НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»
В.о. завідувача кафедри

_____ М.В.Грайворонський
(підпис)

“_____”_____2019 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

на тему: Ризик-орієнтований аналіз ERP систем

Виконав: студент 4 курсу, групи ФБ-52

_____Радченко Родіон Олегович_____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник_____доктор технічних наук, професор Архипов О.Є._____ _____
(посада, науковийступінь, вченезвання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назварозділу) (посада, вченезвання, науковийступінь, прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковийступінь, вченезвання, науковийступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 рік

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

_____
(прізвище, ім'я, по батькові)

1. Тема роботи «Ризик-орієнтований аналіз ERP систем»_____
_____
_____,
науковий керівник роботи
доктор технічних наук, професор Архипов О.Є._____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від « » 2019 р. №

2. Термін подання студентом роботи червня 2019

3. Вихідні дані до роботи_____
_____

4. Зміст роботи_____
_____
_____
_____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

_____
_____
_____

6. Дата видачі завдання_____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник роботи _____ _____
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Робота об’ємом 63 сторінок, яка містить 4 ілюстрацій, 8 таблиць, 20 джерел за переліком посилань.

Актуальність роботи визначається потребою аналізу та визначення обсягу інвестицій в безпеку інформації організації, що з огляду на необхідність проведення низки економічних досліджень та розрахунків обумовлює можливу доцільність залучення до їх виконання ERP-системи організації.

Мета роботи дослідження та аналіз ефективності інвестицій в інформаційну безпеку організації шляхом залучення до аналізу ERP-системи.

Об’єкт дослідження застосування ризик-орієнтованого підходу для розрахунку інвестицій в інформаційну безпеку організації.

Предмет дослідження методологія розрахунку інвестицій в інформаційну безпеку організації та доведення доцільності застосування у розрахунках ERP-системи.

Методи дослідження є оброблення інформаційних джерел, стандартів за даною темою, практик ризик-орієнтованого аналізу.

Практичне значення одержаних результатів є одержані результати можуть бути використані при плануванні інвестицій в інформаційну безпеку на підприємствах.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ERP-СИСТЕМА, ОЦІНКА РИЗИКІВ, РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД.

ABSTRACT

Work in volume of 63 pages, which contains 4 illustrations, 7 tables, 20 sources under the list of links.

Actuality of work: is determined by the need to analyze investment in the safety of information in the production by putting into operation the ERP system to determine its efficiency in terms of risk-oriented approach.

Purpose: to research and analyze the effectiveness of investments in information security of the enterprise by putting into operation of the ERP system.

Object of research: methodology of calculation of investments in ERP system for review of risk-oriented approach.

Subject of research: methodology for calculating investment in the ERP system.

Object of research: methodology of investing in the ERR system in terms of a risk-oriented approach.

Method of research: processing of information sources, standards on the given topic, practices of risk-oriented analysis.

The practical value of the results obtained: the results obtained can be used to plan investments in information security at enterprises.

Key words: INFORMATION SECURITY, ERP SYSTEM, EVALUATION OF RISKS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ERP система (англ. Enterprise Resource Planning System) — система планування ресурсів підприємства

KPI (англ. Key Performance Indicators) — ключові індикатори ефективності

BPR — реінжиніринг бізнес-процесів

ERP проект — проект по розробці та розгортанню ERP системи

ОУП — офіс управління проектами

ВСТУП

З розвитком інформаційних технологій, автоматизацією бізнес-процесів та переходом до електронного документообігу на підприємствах цінність інформації, що зберігається в електронному вигляді, зростає і тому питання інвестицій в технології захисту інформації стає все гострішим. Для аналізу доцільності інвестицій в ті чи інші технології доцільно використовувати ризик-орієнтований підхід, що дає чітку картину раціональності для кожного підприємства з урахуванням його специфіки.

Актуальність роботи: визначається потребою аналізу та визначення обсягу інвестицій в безпеку інформації організації, що з огляду на необхідність проведення низки економічних досліджень та розрахунків обумовлює можливу доцільність залучення до їх виконання ERP-системи організації.

Мета роботи: дослідження та аналіз ефективності інвестицій в інформаційну безпеку організації шляхом залучення до аналізу ERP-системи.

Завдання роботи:

- Виконати огляд загальних підходів ризик-орієнтованого управління інформаційною безпекою
- Дослідити існуючі методики управління ризиками в проектах ERP
- Розробити методику оцінки ризиків в ERP проектах
- Розрахувати доцільність інвестування в ERP систему для підприємства з огляду на ризик-орієнтований підхід та провести ризик-орієнтований аналіз ERP системи
- Зробити висновки про доцільність використання ERP систем для підприємства на підставі отриманих результатів

Об’єкт дослідження: застосування ризик-орієнтованого підходу для розрахунку інвестицій в інформаційну безпеку організації.

Предмет дослідження: методологія розрахунку інвестицій в інформаційну безпеку організації та доведення доцільності застосування у розрахунках

ERP-системи.

Метод дослідження: оброблення інформаційних джерел, стандартів за даною темою, практик ризик-орієнтованого аналізу.

Наукова новизна: проведено ризик-орієнтований аналіз ERP системи для підприємства та проаналізовано ризики при розгортанні та експлуатації на основі дійсних міжнародних стандартів управління ризиками ІБ.

Практичне значення одержаних результатів: одержані результати можуть бути використані при плануванні інвестицій в інформаційну безпеку на підприємствах.

1 ОГЛЯД РИЗИК-ОРІЄНТОВАНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Поняття ризику

Зростання кількості чутливих даних, що збираються та обробляються державними та приватними організаціями, значно підвищило пріоритет інформаційної безпеки. Порушення безпеки та пошкодження системи, пов'язані з конфіденційними даними можуть призвести до витрат на відновлення даних і переконання, що вони не використовуються для незаконних цілей. Крім того, суб'єкти державного та приватного секторів можуть постраждати від втрати суспільної довіри, що може призвести до фінансових втрат у зв'язку з рішеннями про зайняття бізнесом в інших країнах, а також загальними репутаційними проблемами.

Це збільшення кількості конфіденційних даних, у поєднанні з низкою незручних та шкідливих прогалин безпеки як у державному, так і в приватному секторі, призвело до прийняття стандартів на міжнародному рівні, спрямованих на вирішення проблеми зберігання конфіденційних даних. Незважаючи на те, що ці закони забезпечують управління та мінімальні стандарти для державних і приватних суб'єктів господарювання, яких слід дотримуватися у забезпеченні своїх систем, вони також додають підвищений управлінський та фінансовий тягар. Впровадження додаткового контролю безпеки також збільшує витрати, пов'язані з управлінням системами та досягненням бізнес-цілей. Задача керівництва полягає в тому, щоб запровадити систему контролю, яка захищає конфіденційні дані економічно ефективно, зіставляючи рівень ризику, пов'язаного з системою, та її дані з витратами на управління. Оскільки організації намагаються покращити безпеку та привести свої системи у відповідність до нового законодавства та інших вимог, інструменти оцінки ризику, взяті з управління

проектами, є цінними для забезпечення того, щоб ці проекти досягали своїх цілей[1].

Ризики для інформаційної безпеки можна розділити на зовнішні загрози, які надходять ззовні організації, і внутрішні загрози, що походять зсередини організації. Зовнішні загрози включають, наприклад, віруси та інші шкідливі програми, що вводиться в мережу організації за допомогою електронної пошти або веб-перегляду, хакерських атак та соціальної інженерії сторонніми особами. Внутрішні загрози включають саботаж або шахрайство, що впливають на інформаційні системи працівниками, продавцями або підрядниками компанії, а також помилки та недбалість, включаючи невиконання встановлених процедур. У дослідженні «Комп'ютерна злочинність і безпека» 2007 року Інститут комп'ютерної безпеки у співпраці з Федеральним бюро розслідувань виявив, що 37% респондентів пов'язують більше 20% фінансових втрат їхніх організацій з інцидентами, пов'язаними з безпекою [2]. Опитування CSI повідомило про загальну суму 66 930 950 дол. США у 2007 році з 194 респондентів. Фінансові шахрайства були категорією з найбільшою втратою долара ($ 21 124 750), за якою йшла зараження вірусом ($ 8 391 800). Найбільш поширеними категоріями інцидентів серед 436 респондентів були зловживання доступом до Інтернету інсайдерами (59% респондентів, які повідомляли про такі інциденти), інциденти з вірусами (52%) та крадіжка мобільних пристроїв, включаючи портативні комп'ютери (50%) [2].

1.2 Огляд законодавства

Європейський Союз та Сполучені Штати прийняли різні підходи до законодавства про конфіденційність та безпеку інформації. Сполучені Штати віддавали перевагу прийняттю законодавства дещо реагуючим у відповідь на

конкретні проблеми або кризи. Це призвело до того, що законодавство, яке намагається захистити безпеку певних видів інформації. Приватному сектору в значній мірі дозволяється регулювати себе відповідно до ринкових проблем і прибутковості. Більшість законодавчих актів, що видаються урядом, та інструкції з інформаційної безпеки стосуються, головним чином, державних установ[3].

На відміну від юридичної мішанини, яку Сполучені Штати запровадили для здійснення зусиль з інформаційної безпеки, законодавчий підхід Європейського Союзу до інформаційної безпеки базується на єдиній директиві, «Директива 95/46 / ЄС про захист осіб». Європейський Союз видав цю директиву у 1995 році у відповідь на збільшення кількості зібраних даних і напередодні подальшого збільшення, а також на необхідність транспортування цих даних через національні кордони в межах Європейського Союзу та за його межами з метою досягнення прогресу в науковому та діловому світах. Директива 95/46 / ЄС прагне забезпечити мінімально прийнятний стандарт для забезпечення безпеки даних. Потім держави-члени несуть відповідальність за прийняття та виконання національних законів, які відповідають або перевищують ці стандарти[2].

Закон Грамм-Ліч-Блілі був призначений насамперед для модернізації фінансових послуг через скасування та розслаблення регуляторних обмежень на об'єднання комерційних банків, фондових брокерів та страхових послуг в рамках однієї компанії. Також було частково розширено занепокоєння з боку Європейського Союзу щодо ризиків, пов'язаних з обміном даних між державами-членами з компаніями Сполучених Штатів, які можуть мати більш слабкі процедури безпеки відповідно до нормативно-правової бази США. GLBA застосовується лише до фінансових установ, тобто до підприємств, які займаються банківською справою, страхуванням, акціями та облігаціями, фінансовими консультаціями та інвестуванням [4].

GLBA висуває три основні вимоги, пов'язані з безпекою. Вимоги стосуються лише розкриття інформації та обміну інформацією про

споживачів. Вони не поширюються на інформацію, що стосується інших підприємств. Вимоги:

Фінансові установи повинні зберігати особисті фінансові дані в безпеці.

Фінансові установи повинні надавати сповіщення споживачам перед тим, як поширювати фінансову інформацію з будь-якою неприєднаною стороною або бізнесом, а також надавати можливість відмовитися.

Фінансові установи повинні розкривати свою політику конфіденційності споживачам [5].

Хоча Сарбейнс-Окслі частково підживлює великий інтерес до управління інформаційними технологіями та аудитом інформаційних технологій після його прийняття, закон фактично не дає ніяких конкретних вимог, пов'язаних з інформаційною безпекою. Розділ 404 SOX вимагає, щоб щорічний звіт компанії включав у себе звіт про відповідальність керівництва за встановлення та підтримку адекватної системи внутрішнього контролю для фінансової звітності, а також “містить оцінку ефективності структури та процедур внутрішнього контролю емітента для фінансових операцій[4]. Правила, оприлюднені Радою з нагляду за бухгалтерським обліком державних компаній, також вимагають від аудиторів врахування впливу контролю інформаційних технологій на загальну адекватність структури внутрішнього контролю над фінансовою звітністю. Проте, конкретні директиви щодо контролю, які мають бути реалізовані, залишаються на розсуд аудитора після консультації з керівництвом[5].

Закон про управління федеральними інформаційними системами був прийнятий у 2002 році. Закон встановив вимоги щодо впровадження контролю за інформаційною безпекою на основі оцінки ризиків для систем, які управляються федеральними установами, та для федеральних програм. Закон також вимагає щорічних оцінок ефективності контролів безпеки, а директорам агентств - звітувати про результати своїх оцінок директору Управління та бюджету (ОМБ) для систем, які не класифікуються як системи національної безпеки. . Звіти повинні бути видані директору Центрального

розвідувального управління або міністру оборони для систем національної безпеки. FISMA також вимагає від федеральних відомств дотримуватися Національного інституту стандартів та технологій, включаючи процес сертифікації та акредитації [4].

Директива 95/46 / ЄС, що є основою підходу Європейського Союзу до інформаційної безпеки, надає приватності як особливе право громадянам Європейського Союзу і прагне забезпечити мінімально прийнятний стандарт для забезпечення безпеки даних. Вона визначає декілька прав фізичних осіб щодо їхніх особистих даних, а також відповідальність за суб'єкти, які збирають та обробляють їх. Директива вимагає, щоб суб'єкти, які збирають та обробляють персональні дані, роблять це тільки для визначених і законних цілей, повинні вживати заходів для забезпечення достовірності даних і повинні зберігати ці дані[5].

У 2000 році Європейський Союз ухвалив Рішення 2000/520 / ЕД для вирішення занепокоєння щодо різних і, загалом, слабших стандартів безпеки у Сполучених Штатах. Оскільки держави-члени Європейського Союзу можуть передавати дані лише країні, що не входить до Європейського Союзу, якщо ця країна має вжиті заходи безпеки для забезпечення того ж рівня захисту даних, як у Європейському Союзі, Європейський Союз був стурбований тим, що вимоги Директиви 95/46 / ЕС може завдати шкоди торгівлі між Європою та США. Рішення передбачає, що американські компанії, які дотримуються її положень, можуть розглядатися як безпечна гавань для передачі даних з країн-членів Європейського Союзу[4].

Директива 2002/58 / ЄС Європейського Парламенту побудована на 95/46 / ЕС для роз'яснення прав захисту даних, пов'язаних з обробкою персональних даних та захисту приватного життя в секторі електронних комунікацій. Директива вимагає від держав-членів забороняти збір та збереження даних про місцезнаходження або трафік, пов'язаних з комунікаціями електронними засобами, що дозволить визначити осіб, які беруть участь у комунікаціях[4].

1.3 Підхід до інформаційної безпеки на основі ризиків

Державні та приватні організації можуть нести обов'язки виконувати численні закони та правила. Крім того, вони можуть мати або юридичні або прагматичні зобов'язання для забезпечення того, щоб їхні ділові партнери та підрядники відповідали вимогам безпеки, що стосуються одного або більше законів і правил. Витрати, пов'язані зі слабкою безпекою, можуть бути досить високими, коли настає проміжок, через витрати на реагування на порушення, дотримання нормативних вимог щодо розкриття та звітування про порушення, втрату репутації та довіри між клієнтами або складовими, а також втрату бізнесу. Реалізація ефективної програми безпеки може бути дуже дорогою, особливо для великих організацій, через необхідність придбання апаратного та програмного забезпечення для реалізації технічних заходів безпеки, а також персоналу для управління адміністративними та технічними аспектами безпеки. Завдання управління безпекою, таким чином, полягає в дотриманні відповідного балансу між вартістю впровадженого контролю безпеки та ризиками, пов'язаними з захищеними даними та системами. Щоб забезпечити відповідний баланс, програми безпеки повинні бути розроблені на основі оцінки ризику[1].

Перш ніж обговорювати, як проводити оцінку ризику, необхідно зрозуміти, що означає ризик. Посібник до знань з управління проектами визначає ризик як «невизначена подія або умова, що, якщо це відбувається, має позитивний або негативний вплив на цілі проекту» [1]. Хоча це визначення лише наближається до того, що потрібно для мети нашої роботи, це не зовсім точно.

Використання оцінки ризику в плануванні аудиту викладає загальноприйняту структуру для розгляду ризику при проведенні аудиту. Ці рамки розділяють ризик на три компоненти, дві з яких є корисними для поточної дискусії. Перший тип ризику - це невід'ємний ризик. Відповідно до Керівництва з

аудиту, невід'ємним ризиком є «сприйнятливість до помилок, які можуть бути істотними, окремо або в поєднанні з іншими помилками, припускаючи, що не було пов'язаних внутрішніх контролів»[7]. Щоб надати кілька прикладів, щоб зробити цю концепцію зрозумілішою, інформаційна система, що містить адреси, номери банківських рахунків і медичні записи для декількох мільйонів клієнтів, вважатиметься високим рівнем ризику. Тобто, якщо б система була порушена, наслідки були б серйозними. Єдина база даних користувачів, яка містить контактні дані телефону та електронної пошти для декількох сотень ділових контактів для виконавчої влади, матиме значно нижчий рівень ризику[8].

Другим типом ризику, визначеного в Рекомендаціях з аудиту, є ризик контролю. Керівництво визначає ризик контролю як "ризик того, що помилка, яка може виникнути, і яка може бути матеріальною, індивідуально або в поєднанні з іншими помилками, не буде попереджена або виявлена і виправлена належним чином системи внутрішнього контролю[7]. По суті, ризик контролю, пов'язаний з інформаційною безпекою, є функцією якості ваших процесів безпеки. Наприклад, система, яка дозволяє користувачам з'єднуватися без користувача унікального ідентифікатора користувача або пароля, не робить записів про з'єднання та доступна з терміналів у неконтрольованих громадських місцях, вважається, що має надзвичайно високий рівень ризику контролю . Система з можливістю входу в систему тільки з визначених терміналів, які фізично захищені системою керованого доступу, що вимагає входу з унікальним ідентифікатором користувача, складним паролем, який потрібно змінювати кожні 45 днів, і який створює журнали всіх спроб доступу, які регулярно переглядаються вважається, що вони мають низький рівень ризику контролю, припускаючи, що інші контролі також були сильними.

Більш інтуїтивне пояснення ризику походить від Інституту стандартів внутрішніх аудиторів для професійної практики внутрішнього аудиту. ICBA визначає ризик як “можливість виникнення події, що вплине на досягнення

цілей. Ризик оцінюється з точки зору впливу та ймовірності »[5]. Це також можна просто виразити у вигляді формули:

$$R = P * Z$$

де R – ризик; P – ймовірність втрати; Z – збитки.

Хоча ймовірності та наслідки часто не можуть бути легко виражені в кількісному вираженні, щоб дозволити фактичний розрахунок формули, це забезпечує корисну основу для розгляду концепції ризику, оскільки вона пов'язана з оцінкою ризику безпеки.

Перший крок у проведенні оцінки ризику полягає у визначенні всіх даних у зоні відповідальності організації. У організаціях з централізованими операціями з інформаційними системами і з мінімумом послуг на аутсорсингу це може бути простим завданням. В інших випадках, коли відповідальність за управління інформаційними технологіями або бізнес-функціями передається постачальникам, або окремі відомства несуть повну або часткову відповідальність за розробку та управління власними системами, завдання може стати набагато складнішим. Команді з оцінки ризиків може знадобитися запит управління інформаційними системами та управління бізнес-функціями. Огляд існуючих документів може також надати цінну інформацію про наявні системи. У випадках, коли послуги були укладені контрактним шляхом, здатність суб'єкта господарювання впливати на контроль безпеки буде більш обмеженою, і вона повинна бути виконана насамперед шляхом написання вимог безпеки в контракті, а також процесу моніторингу дотримання договірних вимог[8].

Оцінка впливу збитку, якщо відбулося порушення: цей крок по суті відповідає визначенню рівня власного ризику, пов'язаного з кожною системою або набором даних. В ідеалі хотілося б виразити вплив збитку в доларах або іншої грошової одиниці заради порівнянності. Тим не менш, грошова цифра може бути важко досягти, і насправді може неправильно вказати фактичні збитки, пов'язані з фактичною невдачею безпеки. Під час оцінки рівня ризику, пов'язаного з набором даних або системою, необхідно

враховувати наслідки стихійних лих, пов'язаних із зв'язками з громадськістю, та час, який вони витрачають на реагування на них, а також негативний вплив на складові, якщо втрачені дані отримані та використані для кримінальної діяльності. Часто адекватним є суб'єктивне визначення рівня ризику як високого, середнього або низького[8].

Оцінка загроз і вразливостей: за визначенням Інституту стандартів і технологій, загрозою є «потенціал для того, щоб джерело загроз здійснювало (випадково запускати чи навмисно експлуатувати) певну вразливість»[5]. Простіше кажучи, загроза - це те, що може завдати шкоди системі або бізнес-функції, яку вона підтримує, включаючи несанкціонований доступ до даних. Вразливість - це "недолік або слабкість в системах безпеки, розробці, реалізації або внутрішньому контролі, які можуть бути здійснені (випадково викликані або навмисно використані) і призводять до порушення безпеки або порушення політики безпеки системи"[5]. Іншими словами, вразливість - це слабкість в засобах безпеки, що дозволяє загрозі завдати шкоди. Цей термін приблизно еквівалентний визначенню ризику контролю.

Створення переліку загроз і вразливостей для кожної системи та пов'язаний з нею рівень ризику контролю слід здійснювати у співпраці з управлінням безпекою, управлінням інформаційними системами та управлінням бізнес-функцій. Також можуть залучатися зовнішні консультанти або аудитори[8].

Визначити залишковий ризик та визначити пріоритети ризиків: залишковий ризик для цілей цієї роботи можна визначити як ризик того, що здійснення загрози призведе до значного негативного впливу на інформаційні системи або бізнес-операції. Залишковий ризик NIST визначається як ризик, який залишається після впровадження контролю[5].

Процес визначення залишкових ризиків та визначення пріоритетів ризиків повинен бути практично синонімом визначення системи, на якій організація буде акцентувати увагу при розробці політики та впровадженні контролю. Таблиця 1.1 показує, як залишкові ризики можуть бути віднесені

до систем і ресурсів, спрямованих на поліпшення безпеки, використовуючи просту високу, середню, низьку систему для оцінювання рівнів ризику. Наприклад, якщо система оцінена як така, що має високий рівень власного ризику, і високий рівень ризику контролю, то організація повинна хотіти інвестувати значні ресурси в посилення контролю безпеки цієї системи з метою зниження рівня контроль ризиків шляхом усунення вразливостей. Якщо система оцінена як така, що має низький рівень власного ризику та низький рівень ризику контролю, можливо, не варто вкладати додаткові ресурси для поліпшення безпеки цієї системи. При прийнятті рішень про розподіл ресурсів організація повинна намагатися забезпечити відповідність їх розподілу всім відповідним законам, нормам і вимогам контракту[8].

Таблиця 1.1 - Визначення залишкового ризику

	Невід'ємний ризик			
Контроль-ований ризик		**Високий**	**Середній**	**Низький**
	Високий	**Високий залишковий ризик:** сфокусуйте ресурси тут	**Середній залишковий ризик:** Виділіть ресурси тут	**Низький залишковий ризик:** виділіть тут незначні ресурси
	Середній	**Середній залишковий ризик:** Виділіть ресурси тут	**Середній залишковий ризик:** Виділіть ресурси тут	**Низький залишковий ризик:** виділіть тут незначні ресурси
	Низький	**Низький залишковий ризик:** виділіть тут незначні ресурси	**Низький залишковий ризик:** виділіть тут незначні ресурси	**Низький залишковий ризик:** виділіть тут незначні ресурси

Розробити рамки політики: хоча розробка та передача політик та процедур є важливою складовою ефективної програми безпеки, хоча її часто розглядають як обтяжливу діяльність у створенні документів для аудиторів.

Цінність написання, повної політики та процедур полягає в тому, що якщо ваші користувачі не знають, чого очікується від них, вони, ймовірно, не будуть робити те, що від них очікується. Політики та процедури забезпечують базовий стандарт, на якому будуть налаштовуватися функції безпеки, і надаватимуть користувачам інструкції щодо використання систем[8].

Процедури повинні бути пояснені користувачам, щоб бути ефективними. Вони повинні бути легко доступними для всіх працівників, які несуть відповідальність за дотримання або виконання їх. Треба також розглянути та впровадити навчання з питань політики та процедур безпеки, а також вимагати від працівників письмової сертифікації, що вони прочитали та зрозуміли процедури.

Розробка та впровадження технічних рішень для захисту даних: цей крок передбачає вибір апаратних та програмних рішень, які забезпечують досягнення цілей бізнесу, для яких розроблені системи, і забезпечують адекватні та економічно ефективні засоби досягнення цілей безпеки. Головне полягає в тому, що конкретні технічні рішення повинні бути обрані тільки після того, як була проведена оцінка ризику, щоб гарантувати, що реалізовані рішення відповідають меті безпеки організації[8].

Висновки до розділу 1

У даному розділі було розглянуто загальне поняття ризику, було зроблено огляд законодавства щодо ризику в інформаційній безпеці і його історичної еволюції. Був даний огляд на управління інформаційною безпекою на основі ризику, було класифіковано залишкові ризики в залежності від рівня контрольованого і неконтрольованого ризику.

2 УПРАВЛІННЯ РИЗИКАМИ В ПРОЕКТАХ ERP

2.1 Основні фактори ризику

Як засвідчує кожен, хто коли-небудь брав участь у впровадженні ERP, впровадження системи ERP є ризикованою діяльністю. Невдачі впровадження відбуваються за всілякими причинами, а наслідки невдач можуть варіюватися від відносно доброякісного (наприклад, «низької зручності користування») до загрози для бізнесу («нездатність обробляти транзакції»).

У роботі 2007 року Алоіні, Дульмін і Мініно [3] було проаналізовано 75 опублікованих статей, що стосуються вибору, впровадження та управління ризиками проектів ERP системи. Їх аналіз статей визначив 19 факторів ризику ERP, які сприяли невдачам проекту ERP.

Ми розглянемо чотири фактори ризику, які найбільше впливають на реалізацію ERP, і розглянемо, як ці ризики можна вирішити.

2.2 Неефективне стратегічне мислення та планування

Узгодження цілей проекту ERP з оригінальним обґрунтуванням проекту ERP є одним з перших кроків у забезпеченні успіху проекту. Стратегічні питання бізнесу, які мають вирішуватися системою ERP, зазвичай визначаються, коли розробляється обґрунтування для проекту, але вони повинні бути переглянуті та проаналізовані протягом впровадження, щоб забезпечити синхронізацію бізнес-стратегії та цілей проекту. Підхід до досягнення цього полягає в переведенні бізнес-цілей проекту в очікувані

вигоди, а потім включити огляди і завдання реалізації пільг на кожному етапі плану проекту[3].

Перед запуском: перед тим, як проект буде запущений, очікувані вигоди повинні бути визначені, зареєстровані та перевірені для того, щоб вони були реалістичними та досяжними. Необхідно встановити базові значення для кожного з них, призначити власника і, якщо можливо, досягнення вигоди має бути пов'язане з KPI. Власник повинен бути з ділової сфери, на яку впливає вигода, але бажано не на проектну команду, оскільки це скоріше пов'яже вигоду із загальною організацією, ніж з проектом[9].

Запуск: включення деталей щодо очікуваних переваг у зв'язку з запуском проекту починає процес забезпечення чіткості всієї організації щодо бачення проекту і може бачити, як проект сприяє досягненню загальних бізнес-цілей[9].

Дизайн: надзвичайно важливо, що внаслідок виникнення проекту нової системи на етапі проектування, вигоди знову розглядаються, щоб переконатися, що нові бізнес-процеси пропонують процес для досягнення цих переваг. Якщо на цьому етапі виникають нові переваги, вони також повинні бути захоплені, оцінені та повідомлені власнику. Орієнтація процесу тестування на те, як система надаватиме переваги, сприяє узгодженню цілей проекту та бізнесу[9].

Збірка: протягом етапу побудови процесу, власники вигод підтверджують, що система надасть переваги, беручи участь і підписавшись на приймальних випробуваннях. На цьому етапі розглядається вплив нових процесів на організаційну структуру, а реалізація переваг знову є важливим фактором[9].

Підтримка: переваги, як правило, не повністю реалізуються після того, як команда проекту може більше не існувати. Важливо, щоб був узгоджений план поетапної реалізації пільгових показників з проміжним часом та досягненням цілей, а власникам призначено вимірювати та звітувати про кожну з них. Оскільки керівник проекту більше не буде відповідати,

загальний власник повинен бути призначений для досягнення плану реалізації та забезпечення регулярних формальних перевірок[9].

2.3 Слабкі навички проектної команди

Якщо "слабкі навички проектної команди" є ризиком для проекту ERP, то запитання повинні бути поставлені:

- Як ви можете створити команду з необхідними навичками?
- Які ключові ознаки повинен мати член проекту?
- Що ви можете зробити, щоб визначити неадекватні навички членів команди і запобігти цьому негативно вплинути на роботу команди?

Як можна створити команду з необхідними навичками?

Кожен кандидат на місце в команді проекту принесе свою унікальну комбінацію досвіду, навичок і компетенцій. Ідеально до підбору потрібних кандидатів для проектної команди підходити, як і до будь-якого іншого навчального процесу. Розробити профіль роботи, а бажані критерії задокументувати. Провести інтерв'ю з декількома кандидатами, і, сподіватися, що деякі видатні особи можуть отримати позиції в команді[10]. На жаль, реальний світ взагалі не працює так. Виклики в реальному світі включають:

- Переконувати менеджерів відмовитися від своїх кращих людей протягом певного періоду часу, поки вони відряджаються до проекту.
- Відсутність реального вибору учасників команди (наприклад, лише одного можливого кандидата; вибір кращого з поганих партій; наявність у кого-небудь нав'язування команді, щоб «позбутися від них» у певній формі), що призводить до виникнення невідповідних кандидатів в команді.

Які ключові ознаки повинен мати член проекту?

Є багато різних ролей у команді проекту ERP. Наприклад, внутрішня команда може включати менеджера проекту, менеджера змін, експертів з предметів бізнесу; Бізнес-аналітики / технологічні лідери; Адміністратори бази даних тощо[10]. Точна природа кожної з цих ролей значно відрізняється, але певні характеристики є спільними для всіх членів команди:

Очікується, що кожен член команди матиме відповідний рівень досвіду, щоб ефективно сприяти проекту. Попередня участь у впровадженні ERP є певною перевагою[11].

Всебічне знання бізнес-процесів має важливе значення для експертів з предмету бізнесу та технологічних лідерів, а технічний персонал також повинен бути знайомий з бізнес-процесами та розуміти, як технологія їх підтримує[11].

Кожен член команди повинен як мінімум володіти навичками, необхідними для виконання поставлених перед ними завдань. Вміння працювати з ERP-системами є необхідною умовою, але також важливими є такі навички, як відображення процесів, підготовка навчальної документації та проведення презентацій навчання[11].

Будучи членом команди проекту ERP, це важка робота - часто з довгими днями та періодами напруженого тиску. Члени команди повинні бути працелюбними, цілеспрямованими та стійкими до виконання завдань[11].

Бізнес-аналітики та керівники процесу ефективно представляють свою сферу бізнесу в команді проекту. У результаті вони повинні мати можливість:

Взаємодіяти з користувачами, яких вони представляють, для критики запропонованих нових ідей та процесів.

Взаємодіяти з іншими членами команди, щоб гарантувати, що міжфункціональні процеси мають сенс.

Хороший менеджер проекту повинен знати свою команду і планувати всі слабкі сторони. Психометричні або професійні оцінки можуть бути використані для визначення того, наскільки добре кожен з кандидатів

відповідає вимогам їхньої ролі в команді проекту. Окрім визначення конкретних сильних сторін або позитивних моментів, оцінка може також допомогти виявити слабкі сторони або потенційні проблемні області у порівнянні з відповідними компетенціями[11].

Хоча у вас можуть бути ідеальні кандидати з певних точок зору, вони можуть потребувати тренування або моніторингу стосовно деяких аспектів їхньої діяльності. Ключовим моментом тут є те, що якщо ви заздалегідь знаєте про слабкі місця, ви можете планувати навколо них. За певних обставин вам доведеться подумати про перепризначення обов'язків - але це набагато легше зробити на початку проекту, ніж далі, коли ви зіштовхнетеся з проблемою.

2.4 Недостатній BPR

Хоча наслідки недостатнього BPR, безумовно, є ризиком під час впровадження ERP, корисно зробити крок назад і подивитися на загальну роль BPR у проектах ERP[11].

Багато організацій, які думають про вибір та впровадження нової системи ERP, опиняються в дилемі: вони відчувають, що вони повинні дивитися на реінжиніринг своїх бізнес-процесів, але чи повинні вони це робити перед вибором нової системи, до реалізації або під час впровадження? Більшість експертів погоджується з тим, що БПР має відбуватися до вибору системи, оскільки результати, здійснені в ході BPR, повинні впливати на сферу застосування та функціональні вимоги до проекту відбору ERP. Проте стратегічна мотивація проекту ERP повинна диктувати характер і масштаби вправи BPR[11].

Для проектів, де впровадження ERP-рішення є частиною великої ініціативи з трансформації бізнесу або процесу гармонізації, очевидно,

вимагається комплексний BPR. Розуміння того, яким чином бізнес-плани роботи будуть працювати в майбутньому, є фундаментальним для вибору правильного рішення та встановлення сфери та завдань для реалізації[12].

З іншого боку, заміна застарілої системи, ймовірно, передбачає певний елемент змін, але ймовірно, що рівень необхідних змін буде менш фундаментальним, ніж у описаних раніше сценаріях[12]. Одним із способів вирішення ситуації, подібної до цього, є думка, що ідеальні процеси будуть розроблені і впроваджені в тих сферах, де організація вважає, що певна конкурентоспроможна або комерційна перевага може бути отримана від реінжинірингу існуючих процесів. Деяким існуючим процесам може знадобитися незначні зміни, і в цьому випадку завданням буде пристосувати систему до існуючого процесу. Інші процеси можуть змінюватися більш радикально. Для інших (більш загальних) процесів вони будуть використовувати процеси передового досвіду або попередньо налаштовані шаблони, що надаються як частина рішення ERP (якщо вони підходять природно). Ця частина BPR повинна відбуватися до вибору ERP і повинна інформувати про обсяги та функціональні вимоги до проекту відбору. Основна відмінність, однак, полягає в тому, що в багатьох випадках така робота по реінжинірингу початкового процесу буде на високому рівні, і детальна реінжиніринг процесу буде фактично відбуватися під час впровадження ERP[11].

Такий підхід:

- Допомагає зменшити загальні зусилля БНР.
- Використовує стандартні практики та шаблони процесів, що підтримуються рішенням ERP.
- Допомагає звести до мінімуму прогалини між бажаними процесами, що підлягають, та функціональністю ERP-системи, доступної з коробки.
- Допомагає зменшити або усунути необхідний рівень налаштування.

Очевидно, що існує багато інших можливих сценаріїв, ніж три, описані тут, але в цілому ризик для реалізації буде значно зменшений шляхом проведення BPR вперед до вибору ERP з результатами виконання BPR, керуючи функціональними вимогами. Хоча цей підхід допоможе не повністю виключити ризик прогалин у новому розумінні процесу, оскільки на практиці багато деталей стосовно нових процесів розробляється лише на етапі проектування впровадження ERP. Важливо також, щоб робота з реінжинірингу бізнес-процесів узгоджувалася з роботою, що проводиться з реалізації.

2.5 Неадекватне управління змінами

Одна абсолютна впевненість в тому, що введення нової системи ERP означає, що все зміниться. Бізнес-процеси та процедури будуть змінюватися. Потрібно оновити визначення роботи / ролі (деякі ролі можуть припинити існування). Користувачі можуть боятися того, що для них означають зміни. Дуже важливо, щоб змінам вдалося впоратися з мінімізацією впливу пов'язаних з цим ризиків[13].

Під час управління організаційними змінами під час впровадження ERP потрібно враховувати п'ять сфер:

1. Переваги реалізації
2. Перехід робочої сили
3. Ефективність навчання
4. Очікування зацікавлених сторін
5. Проектний зв'язок

У проекті ERP все вищезазначене має свої власні проекти, пов'язані з загальним планом. Складність в кожній області має бути розглянута з самого

початку і визначена стратегія управління змінами. Потім може бути визначено відповідний рівень зусиль.

В ідеалі буде призначений спеціальний менеджер з питань змін, але менші реалізації, як правило, не можуть бути пристосованими для цього або дозволити це, і часто менеджер проекту бере на себе відповідальність за управління організаційними змінами[13].

Реалізація переваг

Забезпечення того, щоб визначити переваги проекту та запровадити структури та процеси для забезпечення цих переваг, є основною частиною управління змінами. Більш детальну інформацію про це можна знайти в розділі[13].

Перехід робочої сили

Це передбачає визначення областей проекту, які матимуть вплив на ролі та обов'язки робочої сили та керувати організацією через процес змін[13].

Впровадження нових бізнес-процесів або зміна поточних процесів можуть вплинути на організацію по-різному. У деяких випадках завдання можуть зникнути або бути необхідними для перепризначення. Деякі ролі більше не можуть бути релевантними або можуть різко змінитися. Також можуть знадобитися нові ролі. Необхідно провести детальний аналіз впливу на роботу, і необхідно запровадити план переходу до робочої сили. Навіть якщо немає значних змін у процесах та організації, поточні ролі повинні бути зіставлені з новими ролями в системі та відповідними призначеними профілями безпеки[13].

Ефективність навчання

Це стосується визначення потреб у навчанні, розробки навчальних планів і навчальних матеріалів і ефективного навчання[13].

Перед початком проекту необхідно визначити підхід до навчання. Чи буде вся підготовка здійснюватися постачальником або зовнішніми консультантами, чи буде підхід «навчати тренера»? Які матеріали потрібні і

хто буде розробляти ці матеріали? Ці питання та багато інших треба вирішувати і включати в план навчання високого рівня. Пізніше, як тільки завершиться перехід робочої сили та визначено нові ролі та обов'язки, може бути проведений аналіз потреб у навчанні, щоб вирішити, кому треба навчатись і яку підготовку вони повинні отримати. Потім може бути розроблена детальна навчальна програма і графік[13].

Очікування зацікавлених сторін

Визначення ключових зацікавлених сторін проекту або груп зацікавлених сторін та зосередження уваги на вирішенні питань, які можуть зменшити рівень підтримки проекту, є ще однією важливою сферою управління організаційними змінами.

Після того, як зацікавлені сторони будуть ідентифіковані, проведення дослідження для оцінки їхньої взаємодії з проектом сприяє висвітленню будь-яких проблем. Потім вони можуть бути розкриті під час запланованих інтерв'ю, а дії можуть бути узгоджені та відстежені. Це ітеративний процес і до тих пір, поки менеджер змін постійно контактує з зацікавленими сторонами, ризик виникнення будь-яких несподіваних проблем і впливу на масштаб і графік проекту мінімізується[14].

Проектний зв'язок

Наявність структурованого процесу передачі ключової інформації проекту зацікавленим сторонам або групам зацікавлених сторін є ще одним ключовим фактором у забезпеченні успішності впровадження проекту ERP. Це зберігає проект, пов'язаний з організацією[13].

Важливо визначити, яка інформація потрібна зацікавленим сторонам і коли і як вони отримуватимуть оновлення. Комунікаційні завдання починаються з підготовки до запуску проекту і продовжуються до реалізації. Окрім надання інформації про стан проекту, комунікаційний план повинен також забезпечити, щоб організація, що знаходиться поза межами безпосередньої команди проекту, була проінформована про будь-які зміни в процесі або нові проекти процесу. Це гарантує, що розглядається широкий

спектр вхідних даних та будь-які потенційні проблеми розглядаються на початку проекту. Це також відкриває шлях для легшого прийняття нових процесів після впровадження[12].

2.6 Методологія управління ризиками

Проект, за своєю природою, призводить до змін, і це призводить до невизначеності і, отже, до ризику. Для успішного управління ризиками в проекті необхідна методологія, а методи, запропоновані PRINCE 2, дуже застосовні в ситуації впровадження ERP [15].

Класифікація та ідентифікація ризиків

Перш за все, ризики класифікуються в PRINCE 2 у рамках бізнес-ризиків або ризиків проекту[15]. Це допомагає визначити, хто несе відповідальність за управління ризиками. Ризики бізнесу, тобто ті ризики, які пов'язані з наслідками, що не впливають на вигоду, зазвичай управляються Радою / Керуючою групою проекту. Ризики, пов'язані з проектом, є тими, які впливають на управління проектом і зазвичай керуються менеджером проекту. Ризики проекту широко класифікуються як питання постачальників (залежні від третьої сторони), організаційні фактори (пов'язані з людьми, культурою тощо), а також спеціалізовані питання (що стосуються типу проекту, що реалізується). Крім визначення того, хто володіє управлінням ризиком, ці категорії корисні на етапі ідентифікації ризику[15].

Чотири описані вище ризики класифіковані в за даною методикою в таблиці 2.1:

Таблиця 2.1 - Класифікація ризиків за PRINCE 2

Ризик	**Тип**	**Категорія**
Неефективне стратегічне мислення та планування	Бізнес	-
Слабкі навички проектної команди	Проект	Організаційний
Неадекватний BPR	Проект	Спеціалізований
Неадекватне управління змінами	Проект	Організаційний

Керівник проекту несе відповідальність за забезпечення ідентифікації, реєстрації та регулярного перегляду ризиків. Правління / Керівна група проекту повинна переконатися, що менеджер проекту повідомляється про будь-які зовнішні ризики для проекту і повинен приймати рішення щодо рекомендованих менеджером проекту реакцій на ризик, досягнення балансу між рівнем ризику та потенційними вигодами, які можуть бути досягнуто.

Дві дисципліни, описані PRINCE2, що управляють ризиком під час проекту[15]:

1. Аналіз ризиків (ідентифікація та оцінка ризиків; виявлення та вибір відповідної реакції)

2. Управління ризиками (планування, моніторинг, контроль і ресурси для усунення виявлених ризиків)

Аналіз ризиків:

Аналіз ризиків включає чотири основні напрямки діяльності[15]:

- Визначення потенційних ризиків, з якими може зіткнутися.
- Оцінка важливості кожного ризику на основі ймовірності його виникнення та його потенційного впливу.
- Виявлення можливих відповідей для кожного ризику.
- Вибір необхідних дій.

Існує п'ять можливих відповідей для кожного ризику, хоча можливо, що для кожного окремого ризику можуть знадобитися декілька дій[15]:

- Профілактика

Саме тут вживаються заходи для запобігання виникненню ризику або будь-якого впливу, якщо воно відбудеться.

- Скорочення

Зменшити ймовірність або вплив ризику.

- Передача

Передати ризик на іншу частину (наприклад, страховий поліс або пеню).

- Непередбачені обставини

Планування заходів, які необхідно вжити, якщо ризик виникне.

- Прийняття

Саме тут ризик фактично ігнорується на підставі того, що це або дуже малоймовірно, або занадто дорого для реалізації контрзаходів.

Результати аналізу ризиків відображають в журналі ризиків. Основний аналіз ризиків має бути проведений на початку проекту, але методологія PRINCE2 підкреслює, що подальший аналіз повинен проводитися безперервно в міру розробки проекту та отримання нової інформації[15].

Управління ризиками:

Управління ризиками передбачає управління планування та виконання різних дій, визначених як частина аналізу ризиків. Вона включає чотири основні заходи, всі з яких є стандартною діяльністю з управління проектами і проілюстровано на рисунку 2.1:

- Планування
- Ресурсне забезпечення
- Моніторинг
- Контроль

Рисунок 2.1 - Цикл управління ризиками (Адаптовано автором на основі [15])

Стратегія управління ризиками повинна бути узгоджена на початку проекту. Методологія PRINCE2 визначає численні пункти в проекті, де необхідно здійснювати управління ризиками, але конкретний підхід та використовувані методи будуть відрізнятися від проекту до проекту, залежно від характеру проекту та рівня ризику для бізнесу[15].

Висновки до розділу 2

У даному розділі було розглянуто основні фактори ризику в проектах ERP. Була розглянута методологія для управління даними ризиками.

Ризик притаманний будь-якому проекту впровадження ERP, тому управління ризиками відіграє важливу роль у забезпеченні досягнення цілей проекту. Визначення ризиків та впровадження відповідних планів пом'якшення повинні бути одним з центральних обов'язків керівника проекту.

Досвідчені менеджери проектів будуть знайомі з ризиками та стратегіями пом'якшення. Вони також матимуть досвід використання методології управління ризиками, як описано вище. Більшість організацій не матимуть практичного досвіду впровадження ERP і можуть мати обмежені можливості управління проектами. Роль менеджера проекту є центральною для успіху впровадження ERP, тому аутсорсинг цієї ролі варто враховувати.

Управління ризиками часто сприймається як уникнення негативних наслідків, але очевидно, що для проекта ERP, який можна назвати успішним, має бути також позитивний результат. Гарне управління проектами має зосереджуватись на досягненні цілей та завдань проекту, а також на реалізації переваг для бізнесу.

3 РОЗРОБКА МЕТОДИКИ ОЦІНКИ РИЗИКІВ В ERP ПРОЕКТАХ

3.1 Загальні засади ERP проектів та ризики зв’язані з ними

Планування ресурсів підприємства розроблено для забезпечення безшовної інтеграції процесів у функціональних областях з поліпшеним робочим процесом, стандартизацією ділової практики та доступом до актуальних даних у реальному часі. Як наслідок, ERP системи є складними, і їх впровадження може бути складним, трудомістким і дорогим проектом для будь-якої компанії. Хоча існує безліч готових ERP-систем, ERP-проекти продовжують вважатися ризикованими для реалізації в комерційних підприємствах, оскільки вони виходять з ладу по різним тісно пов'язаним між собою організаційним і технічним факторам[2]. Насправді, запровадження будь-якої масштабної інтегрованої інформаційної системи (тобто ERP) може призвести до значних змін у процесах, завданнях і проблемах, пов'язаних з людьми. Особливі ризики, пов'язані з проектами ERP, змушують організації розробляти підходи до управління ризиками протягом всього життєвого циклу проекту. Необхідність підходів до управління ризиками виникає через відсутність ефективного керівництва щодо впровадження ERP. Небажання компаній повідомляти про невдачі в реалізації не дозволяє легко дослідникам пропонувати і перевіряти ефективні рамки. До теперішнього часу література з проектів ERP показує, що тільки знання ризиків не є достатнім для компаній, що впроваджують підхід до управління ризиками, і розгортання є нетривіальною задачею[16].

Поточні дослідження в значній мірі базуються на тому припущенні, що управління ризиками працює так як воно і повинно бути в теорії, в відриві від того як насправді процеси протікають в практиці проекту.

3.2 Ризики впровадження ERP

Декілька досліджень стверджують, що серед основних причин невдачі IT-проектів є неправильне розуміння ризиків проекту та неадекватність управління ризиками керівниками проектів. В останні роки кілька дослідників намагалися визначити критичні фактори успіху для впровадження ERP. Вони досліджують чинники, які полегшують або стримують успіх ERP-проектів на основі методології конкретного дослідження, порівнюючи успішне впровадження ERP з невдалою. Вони розкривають декілька ризиків впровадження ERP, серед яких такі: неефективне стратегічне планування та комунікація та недостатні навички команд проекту. Автори роблять висновок, що ключовим фактором успіху є ретельне управління змінами, мережеві відносини та культурна готовність[16].

Вони зосереджують увагу на питаннях, що стоять за процесом впровадження ERP за допомогою методології конкретного дослідження. Ми ж розглянемо бізнес і технічні, а також культурні питання впровадження ERP. Ми підкреслимо необхідність адекватних підходів до комунікації та BPR, а також вдосконалення методів управління проектами та змінами. Варто приділяти увагу необхідності узгодження процесів з певними конфігураціями програмного забезпечення, навчання вищого керівництва та кінцевих користувачів, а також навчання людей прийняттю змін[16].

Було проведено емпіричне дослідження критичних питань, які впливають на успіх впровадження ERP. Воно висвітлює декілька ризиків ERP, таких як невідповідний досвід консалтингових послуг, неадекватний BPR, невідповідний вибір ERP та низькі зобов'язання керівництва. Вони виробляли 10 найчастіших факторів ризику на основі огляду літератури. Автори вказують, що п'ять основних факторів ризику - це неадекватний вибір ERP, неефективне стратегічне мислення та планування, неефективні методи

управління проектами, погана управлінська поведінка та неадекватне управління змінами[16].

Останні дослідження пропонують шість ключових факторів, які можуть призвести до успішної реалізації ERP структури проекту, стратегії реалізації, стратегії перетворення бази даних, техніки переходу, стратегія управління ризиками і стратегія управління змінами. Автори класифікують ризики, пов'язані з впровадженням ERP, з точки зору організації клієнта та експертів. При цьому вони класифікують ризики на шість категорій, пов'язаних з організацією, спеціалізованими навичками, управлінням проектами, системою, користувачами та технологіями[16].

Ризик впровадження ERP можна класифікувати за фазами проекту з урахуванням процесів управління проектами, організаційних перетворень та інформаційних технологій для того, щоб запропонувати пом'якшувальні заходи для кожної категорії (таблиця 3.1).

Таблиця 3.1 - Фактори ризику відповідно до фази проекту та категорії ризику

Фази проекту	**Категорії ризику**		
	Процес управління проектом	**Організаційні перетворення**	**Інформаційні технології**
Планування	Неточний бізнес-кейс Незрозумілі цілі Слабкий підбір команди	Невиконання управлінських\виконавчих зобов'язань та керівництва Нестача синергії між IT стратегією й організаційною стратегією	Нестаток комунікації з кінцевим користувачем Неадекватний план навчання користувачів
Реалізація	Невідповідальне управління Недостатня комунікація між командою інтеграції, провайдером системи і користувачами	Неналежне управління змінами Неналежне управління структурою та культурою	Невірний вибір ERP системи Недоречна інтеграція системи Неточні дані про ефективність Невірне навчання користувачів
Здача, оцінка, експлуатація	Невідповідальне закриття угоди	Неадекватна підготовка організації Опір змінам Недостатня підготовленість користувачів	Недоречне тестування та введення в експлуатацію системи Невірне вимірювання продуктивності і управління

Успішне впровадження ERP-систем може бути результатом ефективного управління цими ризиками, які є дуже загальними, оскільки вони були зібрані з різноманітних проектів ERP в різних галузях.

3.3 Рамки управління ризиками

Подібно до управління ризиками інших проектів, управління ризиками впровадження ERP має здійснюватися у три етапи - фази планування, реалізації та після впровадження[17]. Аналіз ризику на етапі планування ERP тісно пов'язаний з вибором ERP-системи, оскільки попередні дослідження визнають, що впровадження ERP є ризикованою справою. Він використовує комбіновану номінальну групову техніку та модель процесу аналітичної ієрархії для оцінки ERP-систем і розглядає ризик як одну з конструкцій. Барді і Девіс застосували аналітичний мережевий процес і підхід до цільового програмування 0–1 для вибору ERP-системи. Вони використовують цільове програмування 0–1 з кількома критеріями, такими як переваги, апаратне забезпечення, програмне забезпечення та інші витрати, фактори ризику, переваги тих, хто приймає рішення та користувачів, та зобов'язання щодо завершення та часу навчання. Аналітичний ієрархічний підхід на основі процесу з ризиком як одна з конструкцій був прийнятий. Аналіз ризиків на етапі планування вирішує проблему. Існує значна кількість ризиків у будь-якій фазі впровадження ERP через технічну складність та вимоги до організаційних перетворень[16].

Література повідомляє про прийняття загальних методів для управління ризиками впровадження ERP. Відомо про методологію діагностування ризиків, яка складається з аналізу контексту, ідентифікації ризиків, аналізу ризиків, оцінки ризиків, обробки ризиків, моніторингу та перегляду, а також комунікації та консультацій[16]. Інші методики також припускають, що

стратегія управління ризиками складається з двох підходів - перша спрямована на зменшення ризикових обставин, а друга - на лікування ризику після появи ризику. Вони зауважують, що реалізація ERP на декількох ділянках є непростою принаймні на чотирьох різних рівнях - бізнес-стратегії, конфігурації програмного забезпечення, технічній платформі та управлінні. Успішна реалізація ERP на декількох ділянках спрямована на взаємодію і компроміс між чотирма різними рівнями; проте цей підхід є більш концептуальним, ніж практичним[17].

Підсумовуючи, попередні дослідження розробили кілька методів управління ризиками при впровадженні ERP, які є теоретично обґрунтованими і практичними для конкретного випадку. Однак, наша методика розширює цю роботу, надаючи більш цілісний підхід, який враховує ієрархічні ризики (рівні зовнішнього залучення, програми, потоку робіт і робочого пакету) для технічних, планових, операційних, ділових та організаційних факторів.

3.4 Процес управління ризиками впровадження ERP

Процес має наступні етапи: ідентифікувати та класифікувати ризик, аналізувати ризики, визначати підхід до виявленого ризику, відстежувати ризики та зменшувати ризик. Схематично процес наведений на Рисунку 3.1.

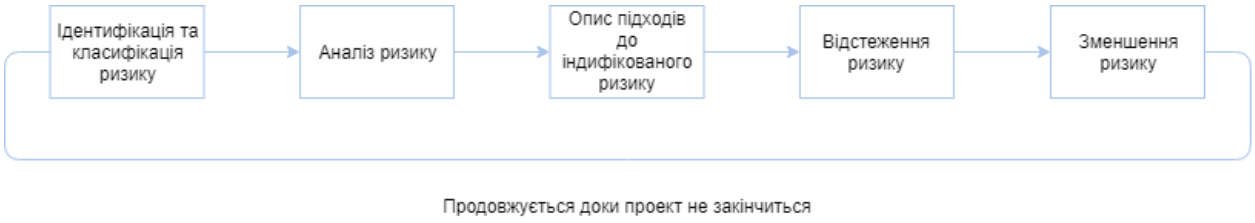

Рисунок 3.1 - Процес управління ризиками (високий рівень).

Процес управління ризиками включає різні зацікавлені сторони - кожен з різними ролями та рівнями повноважень; кожен з них відіграє ключову роль у аналізі ідентичності та контролю ризиків.

Менеджер з управління ризиками «Управління програмами» володіє цим процесом управління ризиками. ОУП повинно створити звіти про оновлення ризиків та вимагати щотижневих оновлень статистики ризиків від менеджерів робочих пакетів про продуктивність програми, які були точно зареєстровані, класифіковані та діють. Дія приймає форму інструкції для менеджерів робочих пакетів або ескалацію до вищого органу - менеджерів областей[18].

Роль менеджера робочого пакету полягає в оцінці ризиків на місці роботи, підвищенні та оновленні двомісячних звітів про оновлення ризиків, а також з інструкціями щодо дій, наданими менеджером з управління ризиками ОУП[18].

Менеджер з випуску/зони отримує звіт про оновлення ризиків два тижні від менеджера ризику ОУП, проаналізував ризики з менеджерами пакетів робіт, вирішив ризики рівня роботи та вирішив, чи потрібно деяким ризикам перерости до вищого органу - менеджера програми[18].

Менеджер програми надає інструкції керівникам з питань реагування на ризики, ризиків керованого програмного менеджменту, підвищених та оновлених ризиків кожні два тижні, використовуючи звіти, оговоривши зовнішні ризики з Радою Програми. Критичні питання програмного рівня розглядаються на зустрічах з управління програмою, коли присутні клієнти та постачальник[18].

Цикл контролю ризиків розпочинається з виробництва, яке розподіляється кожному учаснику оцінки ризику. Це дозволяє кожній людині внести свій вклад - заповнити кожне обов'язкове поле в документі - або зробити оновлення існуючих ризиків. Менеджер з управління ризиками пов'язаний з кожним учасником опитування для забезпечення того, щоб до консолідації в окремі одиниці повідомлялося правильну інформацію. Зазвичай це відбувається у вигляді телефонного дзвінка або особистої зустрічі для перевірки. Потім збираються консолідовані відгуки, які надають відповідну інформацію про ризик управлінській команді кожного потоку робіт, а також інформацію про ризики, що стосуються інших потоків роботи, і весь проект[18].

Однак, незважаючи на те, що був створений цілеспрямований процес управління ризиками, не має уніфікованого фреймворку для об'єктивного розмежування різних видів ризику в цьому процесі. В результаті цієї роботи можна отримати більш широке знання та побудувати та використовувати рамки аналізу ризиків ERP.

3.5 Аналіз ризиків

Аналіз ризиків включає аналіз потенційного впливу та ймовірності виявлених ризиків з метою спрямування відповідей на ризики (Рисунок 3.2). Цей етап процесу відбувається на спеціальній основі в межах груп, хоча збір та формальний журнал ризиків треба оновлювати періодично (кожні два тижні). Для більш об'єктивної оцінки ризиків для оцінки кожного ризику використовуються стандартизовані оцінки, як показано на Рисунку 3.3; кожен фактор ризику оцінюється таким же чином.

Рівень	Вплив	Опис
1	**Вартість** - <50 т.г. та\або **Графік** - ризик затримки результату	Граничний вплив
2	**Вартість** - <50-199 т.г. та\або **Графік** - ризик затримки результату	Помірний вплив
3	**Вартість** - <200-499 т.г. та\або **Графік** - ризик затримки результату	Середній вплив
4	**Вартість** - <500-999 т.г. та\або **Графік** - ризик затримки до етапу плану 1-го рівня	Високий вплив
5	**Вартість** - >1 м.грн. та\або **Графік** - ризик пропуску дедлайну	Критичний вплив

	5	5	10	15	20	25
	4	4	8	12	16	20
Вплив	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Вирогідність				

Рівень	Вирогідність	Опис
1	<5%	Дуже малоймовірно
2	5-25%	Малоймовірний випадок
3	26-60%	Ймовірний випадок
4	61-85%	Вирогідний випадок
5	>85%	Дуже ймовірний

Рисунок 3.2 - Шкала оцінки ризику: вплив і ймовірність (В, П і Н означають червоний, жовтий і зелений колір відповідно)

Ризики були розподілені відповідно до їх потенційного впливу на проект та ймовірності їх виникнення. Кожна з них оцінюється як "високий" ("В"), "помірний" ("П") або "низький" ("Н") тяжкість ризику для загального проекту впровадження ERP. Вони наведені в таблиці 3.2 і таблиці 3.3, використовуючи "В", "П" і "Н", відповідно, для представлення кожного "впливу" і "ймовірності" [В, Й].

Таблиця 3.2 - Загальні ризики для впровадження ERP

	Рівні			
Категорії	Зовнішнє залучення	Документація	Робочий процес	Робочий пакет
Технічні (апаратне та програмне забезпечення)	Спадкові системні зміни впливають на інтерфейси	Необхідні бізнес-ресурси недоступні - бізнес-ресурс може "перекриватися"	Виконання проекту відхиляється від дизайну / принципів	Не відповідає специфікації IT (апаратне, програмне забезпечення, мережа, система безпеки)
	Кінцеві користувачі проекту не підтримують розгортання	Погане управління загальною архітектурою IT	Недостатня обчислювальна потужність серверів	Очищення даних не відповідає вимогам
		Недостатнє навчання фахівців	IT не вирішує функціональних проблем	
		Не вдається передати знання	Недостатній обсяг бази даних у SAP для обсягу транзакцій, які мігрують з попередніх систем	
		Профілі SAP не відповідають ролі організації	Телекомунікаційні зв'язки з аутсорсинговими партнерами призводять до відсутності доступу офшорної команди SAP	
			Неналежне тестування системи	
			Затримка при закупівлі обладнання	
			Рішення про вибір конфігурації архітектури системи не приймалося вчасно	
			План не може бути досягнутий через багато одночасних заходів	
Розклад	Пізні рішення / підписання	Організація не може прийняти зміни		Нова система не може узгодити ділову інформацію
	Спадкові системи вимагають змін, які могли б затримати проект			
Операційні	Ризик комунікації між проектом і бізнесом	Неспроможність забезпечити вигоди, описані в бізнес-справі	Ніяких заходів з відновлення після аварії	
		Недостатнє оформлення	Системна несправність у фазі після переходу	
		Нова система не надає належної фінансової інформації		
		Інформація, що генерується новою системою, не відповідає Закону про захист даних		
Бізнес	Ризик, що спонсор скасовує проект	Відсутність ресурсів у межах бізнесу для заповнення конкретних ролей		
	Бізнес страждає від перевтоми			
	Бізнес неадекватно готовий прийняти нове рішення			
Організаційні	Інші проекти, що відбуваються паралельно в рамках бізнесу впливають на проект ERP	Необхідні ресурси проекту недоступні, наприклад, для навчання	Команда проекту не працює	Відсутність ресурсів у нових технологічних зонах,що зявляється завдяки їхньому фаховому характеру
				Розворот команди проекту

Таблиця 3.3 - Методика застосовується до ризиків впровадження ERP

	Рівні			
Категорії	Зовнішнє залучення	Документація	Робочий процес	Робочий пакет
Технічні (апаратне та програмне забезпечення)	Спадкові системні зміни впливають на інтерфейси[В,П]	Необхідні бізнес-ресурси недоступні - бізнес-ресурс може "перекриватися" [В,В]	Виконання проекту відхиляється від дизайну / принципів [П,П]	Не відповідає специфікації IT (апаратне, програмне забезпечення, мережа, система безпеки) [В,Н]
	Кінцеві користувачі проекту не підтримують розгортання [Н, П]	Погане управління загальною архітектурою IT [В,В]	Недостатня обчислювальна потужність серверів [В,Н]	Очищення даних не відповідає вимогам [П,В]
		Недостатнє навчання фахівців [В,П]	IT не вирішує функціональних проблем [В,П]	
		Не вдається передати знання [В,Н]	Недостатній обсяг бази даних у SAP для обсягу транзакцій, які мігрують з попередніх систем [В,П]	
		Профілі SAP не відповідають ролі організації [В,Н]	Телекомунікаційні зв'язки з аутсорсинговими партнерами призводять до відсутності доступу офшорної команди SAP [В,Н]	
			Неналежне тестування системи [П, П]	
			Затримка при закупівлі обладнання [В,П]	
			Рішення про вибір конфігурації архітектури системи не приймалося вчасно [П,Н]	
			План не може бути досягнутий через багато одночасних заходів [В,Н]	
Розклад	Пізні рішення / підписання [В,В]	Організація не може прийняти зміни [Н,Н]		Нова система не може узгодити ділову інформацію [П,П]
	Спадкові системи вимагають змін, які могли б затримати проект [В,В]			
Операційні	Ризик комунікації між проектом і бізнесом [П,Н]	Неспроможність забезпечити вигоди, описані в бізнес-справі [П,Н]	Ніяких заходів з відновлення після аварії [В,П]	
		Недостатнє оформлення [В,П]	Системна несправність у фазі після переходу [Н,Н]	
		Нова система не надає належної фінансової інформації [В,Н]		
		Інформація, що генерується новою системою, не відповідає Закону про захист даних [В,Н]		
Бізнес	Ризик, що спонсор скасовує проект [В,Н]	Відсутність ресурсів у межах бізнесу для заповнення конкретних ролей [П,В]		
	Бізнес страждає від перевтоми [Н,В]			
	Бізнес неадекватно готовий прийняти нове рішення [П,Н]			
Організаційні	Інші проекти, що відбуваються паралельно в рамках бізнесу впливають на проект ERP [В,В]	Необхідні ресурси проекту недоступні, наприклад, для навчання [В,П]	Команда проекту не працює [П,П]	Відсутність ресурсів у нових технологічних зонах,що з'являється завдяки їхньому фаховому характеру [В,Н]

Приписуючи витрати кожному ризику - на основі його ймовірності виникнення та його рівня впливу, можна продемонструвати потенційний ризик для всього проекту. Оцінки та пов'язані з ними витрати використовувалися як важливий інструмент прийняття управлінських рішень для прийняття ключових рішень щодо напрямків впровадження ERP. Включення витрат заохочує колектив до розгляду повних наслідків кожного ризику. Важливо зазначити, що початкові оцінки ймовірності та впливу ризику можуть бути неточними. Це означає, що оцінювачі ризику не відчувають спочатку необхідності витрачати час на оцінку впливу без необхідності, оскільки команда з управління ризиками розуміє, що оцінки можуть змінюватися з часом, а також пов'язані з ними витрати.

Решта три етапи процесу управління ризиками (див. Рисунок 3.1) (визначення підходу до виявленого ризику, відстеження ризиків та

зменшення ризику) не обговорюються в даному методі, оскільки вони є конкретними для компанії рішеннями, що представляють менший інтерес для загальної практики. Перші два етапи були представлені, оскільки вони надають загальні принципи аналізу ризиків, використовуючи новий метод для впровадження ERP.

Використовуючи вищезгадану структуру звітності, нову методику і цикл управління ризиками, проект ERP успішно можна ввести в експлуатацію. Він може допомогти успішно досягти цілей проекту, забезпечити системний підхід до визначення економічно ефективних заходів зі зниження ризику, забезпечити систематичний підхід до моніторингу та звітування про прогрес у зниженні ризику, допомогти визначити часові рамки для оцінки дій та результатів, заохочувати постійну, систематичну оцінку та аналіз ризиків, при цьому зосереджуючись на постійному зниженні ризику.

Проекти впровадження ERP по суті є ризикованими. Відповідний вибір ERP-системи може значно зменшити наступні ризики впровадження та операційні ризики. Хоча є певні рамки, які допомагають керувати ризиками в процесі впровадження, вони, як правило, занадто теоретичні; їх використання обмежене, головним чином, через відсутність знань користувачів. Таким чином, був необхідний практичний метод для управління ризиком впровадження ERP.

Даний метод інтегрує ідентифікацію ризиків, аналіз і контроль, класифікуючи ієрархічно ризик (зовнішнє залучення, програма, робочий потік і робочий пакет), що допомагає розподілити ризики для конкретних зацікавлених сторін для ефективного пом'якшення та управління. Також класифікує ризик як технічний, графік, операційний, діловий або організаційний, що допомагає аналізувати вплив факторів ризику та приймати ефективний контроль за всіма ризиками. Розуміння специфічного характеру ризику допомагає кількісно оцінити вплив і ймовірність та визначити пріоритетність розгортання ресурсів для зменшення ризиків.

Механізм управління ризиками з організаційною ієрархією сприяє правильному управлінню ризиком від первинної ідентифікації до закриття конкретного ризику. Призначення вартості ризику додатково підкреслює його потенційну серйозність, а регулярні циклічні оцінки ризику забезпечують використання останньої інформації.

У процесі управління ризиками фаза ідентифікації ризику може мати більшу значимість у порівнянні з фазами аналізу ризиків і реагування, оскільки, якщо ризики не визначені правильно, будь-які подальші складні методи аналізу або відповіді керівництва навряд чи дадуть бажані ефекти. З іншого боку, відповідна ідентифікація ризиків може полегшити як належний подальший аналіз, так і управління. Наш метод не тільки допомагає зацікавленим сторонам (клієнтові, консультанту або постачальнику ERP) правильно визначити ризики, але й полегшує об'єктивний аналіз і дозволяє відповідне управління цими ризиками.

Огляд літератури показує, що ключовими факторами успіху впровадження ERP є: зобов'язання вищого керівництва, вибір відповідних систем та належне управління його інтеграцією з існуючим бізнесом. інформаційні системи - включаючи реінжиніринг бізнес-процесів. Крім того, цей аналіз показує, що управління процесами проектів ERP, поряд з управлінням інформаційними технологіями та управлінням організаційними перетвореннями, робить успішним впровадження ERP-проектів.

Висновки до розділу 3

В розділі були дані рамки управління ризиками, було розроблено класифікацію і процес аналізу ризиків за даною класифікацією. Було надано перелік основних ризиків впровадження ERP системи та проаналізовано їх за розробленою методикою.

У проактивному підході до управління ризиками всі зацікавлені сторони беруть участь у виявленні та аналізі ризиків для кожної фази проекту, перш ніж приймати рішення щодо змінних проекту (наприклад, розгортання та розподіл ресурсів, вибір методології впровадження, підрядники та вибір постачальників тощо). Успіх впровадження ERP частково пов'язаний з тим, що зацікавлені сторони розуміють і ефективно виконують свої поточні обов'язки в проекті [14]

Проекти ERP є технічно складними, міждисциплінарними, тривалими і капіталомісткими; тому їх можна охарактеризувати як високо ризикові проекти. Іноді важко розробити план проекту на початку через відсутність інформації на початковому етапі; Таким чином, динамічний аналіз ризиків може допомогти покращити знання про проект і забезпечити кращі плани в міру прогресу проекту. Хоча практики управління ризиками збільшують вартість проекту з точки зору розгортання додаткових людських ресурсів та накладних витрат, додаткових ресурсів для зменшення ризику тощо, вигоди (активні підходи до запобігання невдачі) в кінцевому рахунку перевершать витрати. Треба розширити практику управління ризиками до періоду після впровадження. Це допоможе забезпечити стійкість інформаційних систем підприємства.

4 ЕКОНОМІЧНИЙ АНАЛІЗ ERP СИСТЕМИ

На жаль, в нормативно-правових документах традиційно відсутні будь-які формалізовані вказівки щодо обчислення втрат, обумовлених реалізацією інформаційних загроз.

Для виокремлення даних, що становлять цінність для підприємства, і для внутрішньої класифікації цієї інформації за ступенем секретності необхідно використовувати певну міру важливості інформації, яку бажано визначити у кількісному вигляді. Цю міру можливо представити як вартісний еквівалент шкоди, яку буде нанесено внаслідок реалізації тієї чи іншої загрози інформації. Рівень потенційної сукупної шкоди W визначається за формулою 4.1:

$$W = W_{ек} + W_{ін} \quad (4.1)$$

де Wек – показник економічної шкоди, який означає рівень зниження ефективності використання виділених коштів для забезпечення діяльності об'єкта ризику (організації, її підрозділу) внаслідок реалізації загрози інформації; Wін – показник, який характеризує шкоду від інших тяжких наслідків, що не можуть бути обраховані в економічному кількісному чи вартісному вимірі, тому звичайно визначається експертним шляхом і часто має суттєво суб’єктивний характер. В зв’язку з цим стає очевидною важливість об’єктивного обчислення значення показника Wек, яке для організації із достатньо складною структурою може бути успішно реалізовано лише за допомогою ERP- системи, що інтегрує усі необхідні для цього розрахунку відомості про організацію[19].

4.1 Розрахунок інвестицій на розгортання ERP системи

З точки зору економічної рентабельності встановимо вимогу, щоб збитки від реалізації можливих загроз не перевищували витрати на забезпечення інформаційної безпеки. Тому, щоб використання ERP системи було доцільним, необхідно визначити збитки від реалізації можливих загроз і порівняти з витратами на розгортання і використання ERP системи.

Доцільно буде використовувати готові рішення, що поставляються як послуга для підприємств. Експертною оцінкою визначено, що доцільно буде взяти для розрахунків продукт «BAS ERP» компанії TQM Systems.

Введення в експлуатацію системи буде складатися з таких етапів:

- аналіз процесів підприємства;
- доповнення модулів системи;
- тестування.

Для даних етапів нам потрібні такі категорії спеціалістів від підприємства:

- керівник;
- інженер;
- аналітик.

Розрахунок основної заробітної плати наведено в таблиці 4.1.

Таблиця 4.1 – Розрахунок основної заробітної плати робітників при введені в експлуатацію системи

Етап	**Посада**	**Кількість людей**	**Всього трудоднів**	**Оклад, грн**	**ЗП за день**	**Разом**
Аналіз	**Аналітик**	1	5	5000	1000	5000
Доповнення	**Інженер**	2	5	5000	1000	10000
Тестування	**Керівник**	1	10	20000	2000	20000

Всього	4	25	–	–	35000

$З_о$ = 35 000 грн.

Додаткова заробітна плата складає 20 % згідно нормативам встановленим підприємством.

$З_д$ = 7 000 грн.

Норматив встановлений на підприємстві на накладні витрати складає 10 %:

$З_н$ = 3500 грн.

Замість розгортання сервера на виробництві буде доцільним використати послугу віддаленого сервера, на конфігурацію котрого за нормативами підприємства встановлено витрати 20 % від основної заробітної плати:

$З_р$ = 7000

В Таблиці 4.2 розраховано кошторис витрат на реалізацію ERP системи. Прибуток визначаємо у відсотках від суми витрат, він становить 12,3% від загальної суми витрат.

Таблиця 4.2 – Кошторис витрат

Стаття витрат	Сума витрат
Основна заробітна плата	35 000
Додаткова заробітна плата	7 000
Накладні витрати	3500
Розгортання	7000
Всього	52500
Прибуток	58957,5
ПДВ (20 %)	10500
Договірна ціна	703536

4.2 Витрати від реалізації можливих загроз

Розрахунки для ризиків від реалізації можливих атак будуть проводитися наступним чином:

Вхідні дані:

- час простою, $t_п$
- час відновлення, $t_в$
- час повторного введення втраченої інформації, $t_{ві}$
- зарплата персоналу, Zo
- зарплата співробітників атакованого сегмента, Zc
- число обслуговуючого персоналу No
- число співробітників атакованого сегмента, Nc
- обсяг продажу атакованого сегмента, O
- число атакованих сегментів, I
- число атак на рік, n

Втрати від зниження продуктивності робітників на сегменті, що був атакований можна обрахувати як:

$$П_П = \frac{\sum_{N_C} Z_C}{176} \cdot t_П,$$

Витрати на відновлення працездатності атакованого сегмента можна вирахувати як:

$$П_В = П_{ВИ} + П_{ПВ} + П_{Зч},$$

де $П_{ві}$ - вартість повторного введення інформації;

$П_в$ - вартість відновлення вузла;

$$П_{ВИ} = \frac{\sum_{N_C} Z_C}{168} \cdot t_{ВИ}$$

$$П_{ПВ} = \frac{\sum_{N_O} Z_O}{168} \cdot t_В$$

Втрачена вигода від простою атакованого сегмента становить:

$$U = П_П + П_В + V,$$

$$V = \frac{o}{52 \cdot 10 \cdot 8} \cdot (t_П + t_В + t_{ВИ})$$

Отже, загальні збитки від реалізації атаки на сегмент організації складе:

$$ОУ = \sum_{год} \sum_i U$$

Тепер можна розрахувати збитки, нанесені реалізацією можливої атаки на систему:

- $t_п$ = 2 години
- $t_в$ = 2 години
- $t_{ві}$ = 10 годин
- Z_0 = 10000 грн.
- Z_c= 15000 грн./міс.
- N_0 = 1
- N_c = 2
- O = 23 300 000 грн./рік
- i = 1
- n = 7

Розрахуємо втрати від зниження продуктивності співробітників атакованого сегмента:

$П_п$ = 15000/160*2=187,5 грн.

Витрати на повторне введення інформації:

$П_{ві}$ = 15000/160*2=187,5 грн.

Витрати на відновлення вузла:

$П_{пв}$ = 10000/160*2=125 грн.

V = (23 300 000 / 52·10·8) · (2+2+10) = 78 413,46 грн.

Упущена вигода від простою атакованого сегмента становить:

$U = П_п + П_в + V,$

$П_в = N_0 + Z_0$(на годину)* $t_в$ =125 грн.

U = 187,5 + 125 + 78 413,46 = 78 725,96 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$О_у = \sum_{год}\sum_i U =$ 18 149,03*4 = 314 903,84 грн.

Маючи суму збитку від реалізації можливої атаки на сегмент мережі можна порахувати ризики від реалізації атак різних рівнів: аматора, досвідченого хакера, професіонала або спецслужб.

$R=P*О_у$,

де P1 = 0,25; P2 = 0,5; P3 = 0,99[19].

Тоді ризики успішної атаки на даний вузол відповідно дорівнюють:

R1 = 78 725,96 грн.

R2 = 157 451,92 грн.

R3 = 311 754,80 грн.

Витрати на розгортання ERP та собівартість одного машинного часу роботи ERP:

Трудомісткість розгортання ERP системи можна визначити за формулою 4.2:

$$То = Т_р * К_п * К_{ск} * К_м * К_{ст} * К_{ст.п.} \quad (4.2)$$

де $Т_р$ – трудомісткість розробки; $К_п$ – поправочний коефіцієнт; $К_{СК}$ – коефіцієнт на складність вхідної інформації; $К_{СТ}$ – коефіцієнт використання стандартних модулів; $К_{ст.п.}$ - коефіцієнт використання стандартного програмного забезпечення, який дорівнює 1,2–1,6;

Нами було визначено кількість людино-днів на розробку системи: $Т_Р$ = 25 людино-днів. Поправочний коефіцієнт, для даного типу системи можна визначити як: $К_П$ = 0.77. Поправочний коефіцієнт коефіцієнт на

складність вхідної інформації для системи рівний 1: $К_{СК}$ = 1. Для розгортання системи використовуються стандартні модулі, тому коєфіцієнт $К_{ст}$ = 0.7.

Тоді, за формулою, розраховуємо загальну трудомісткість розробки:

$Т_о$ = 27*0,77*1*1*0,7*1,6 = 23,28 людино-дня.

Витрати на обслуговування можна обчислити як:

$З_{об}$ = 12 * $К_д$ * $К_н$ * $З_{см}$ * $К_з$ * $n_з$,

де $З_{см}$ – місячний оклад обслуговуючого персоналу; $К_д$ - коефіцієнт на додаткову заробітну плату; $К_н$. –коефіцієнт на соціальне страхування; $К_з$ – коефіцієнт на зайнятість персоналу протягом зміни; $n_{зм}$ – кількість змін.

$З_{об}$ = 12*10000*1,2*1,3*0,2 = 37440 грн.

Для розрахунку поточних витрат на утримання віддаленого сервера можна взяти ціни послуги оренди сервера компанії «Freehost» що є середніми для ринку. Беремо по тарифу послуги «ADM Ryzen 5».

$З_у$= 1523,80 грн

Собівартість 1 машино-години дорівнюватиме:

$$C1_{м-г.} = \frac{З_у}{T_г} = \frac{1523,80}{8760} = 17 \text{ коп/год}$$

Сумарні експлуатаційні витрати:

$$З_е = З_{об} + З_у = 37440 + 1523,80 = 38\,963,8 \text{ грн}$$

Розрахунок експлуатаційних витрат

1. Заробітна плата обслуговуючому персоналу:

$$З_о = М_о * \frac{Т_о}{У_м} = \frac{10000 * 1}{21,2} = 471,70 грн.$$

Середньомісячна зарплата обслуговуючого інженера $М_о$ = 10000 грн;

$Т_о$ = 1 люд/день;

Кількість робочих днів у місяць $У_м$ = 21,2 дня.

2. Норматив на додаткову заробітну плату встановлений на підприємстві – 30% від основної:

$$З_д = З_о * \frac{К_д}{100\%} = \frac{471,70 * 30}{100} = 141,50\ грн.$$

3. Норма нарахувань на зарплату становить 22%:

$$З_{нар} = \frac{(З_о + З_д) * К_{нар}}{100\%} = \frac{(471,70 + 141,50) * 22}{100} = 134,90\ грн.$$

4. Для розрахунку поточних витрат на утримання віддаленого сервера можна взяти ціни послуги оренди сервера компанії «Freehost» що є середніми для ринку. Беремо по тарифу послуги «ADM Ryzen 5» $З_с$ = 1523,80 грн\рік.

$$З_у = \frac{Зс}{Тр} = \frac{1523,80}{365} = 4.17 \text{ грн}$$

$Т_р$ = 365 днів;

Кошторис експлуатаційних витрат наведено в Таблиці 4.3.

Таблиця 4.3 – Кошторис експлуатаційних витрат за 1 день

Стаття витрат	**Сума витрат**
$З_о$	471,70
$З_д$	141,50
$З_{нар.}$	134,90
$З_{у.}$	4,17
Всього	752,27

4.3 Оцінювання конкурентоспроможності системи та її ефективності

Знайти коефіцієнт зміни ціни споживання нової ERP системи відносно існуючої можна як:

Визначимо коефіцієнт зміни ціни споживання ($K_{цс}$)нового варіанта, відносно існуючого[21]:

$$K_{цс}=\frac{Ц_{д(н)}+E_{в(н)}*T_{(i)}}{Ц_{д(i)}+E_{в(i)}*T_{(i)}}=\frac{703536+752,27*4*240}{707395+843,29*4*240}=0,9399$$

,

де $Ц_{д(н)}$ - договірна ціна нової системи, $Ц_{д(i)}$ договірна ціна існуючої системи, $E_{в(н)}$ - експлуатаційні витрати нової системи, $E_{в(i)}$ - експлуатаційні витрати старої системи.

Термін служби системи (Т) можна вирахувати через відсоток на амортизацію визначений нормами підприємства:

Т = 100 % / 25% = 4 роки.

- Коефіцієнт конкурентоспроможності

Коефіцієнт конкурентоспроможності можна вирахувати як:

$$K_{кон}=\frac{K_к}{K_{цс}}=\frac{1,33}{0,9399}=1,34.$$

Висновки до розділу 4

В даному розділі було виконано економічний аналіз ERP системи, для цього було розраховано витрати на розгортання системи, втрати від реалізації можливих ризиків і оцінено конкурентоспроможність системи.

Зіставивши суму втрат при успішній реалізації атаки можливої атаки на одному сегменті можна побачити, що інвестиції в впровадження ERP

системи для захисту інформації повністю себе виправдовують. Це легко довести, порівнявши отримані ризики в другому підрозділі та вартості розгортання і впровадження ERP системи і можна побачити, що ризики в 2-4 рази більше ніж інвестиції в ERP систему і це без урахування економічної доцільності використання ERP системи на підприємстві.

ВИСНОВКИ

В даній роботі було зроблено загальний огляд ризик орієнтованого підходу до управління інформаційною безпекою, досліджено ризик-орієнтований підхід до проектів ERP. Було зроблено огляд генезису законодавства в даній сфері й існуючих стандартів сьогодні, розглянуто стандартний процес аналізу й управління ризиками, було наведено класифікацію залишкового ризику.

На основі даного огляду була розроблена методика оцінки ризиків на основі їх збитків та ймовірності, було визначено конкретні ризики для ERP проектів за 5 категоріями на 4 рівнях та оцінено їх за розробленим методом. Також було визначено конкретний процес ризик-орієнтованого аналізу ERP проекту на виробництві з огляду на розроблений метод.

Розроблена методика відрізняє себе від існуючої літератури з управління ризиками ERP, прийнявши більш збалансовану та інтегративну структуру, оскільки демонструє практичний і цілісний підхід до виявлення та управління ризиками при впровадженні ERP. Вона інтегрує ідентифікацію ризиків, аналіз і контроль, класифікуючи ієрархічно ризик (зовнішні зобов'язання, програми, потоки робіт і рівні робочого пакету) по технічних, графічних, операційних, ділових і організаційних категоріях. Це не тільки допомагає розробити пом'якшення ризиків, але й полегшує контроль ризиків через організаційну ієрархію.

Наше дослідження запропонувало таку структуру, яка може сприяти успішному впровадженню проекту ERP. У дослідженні, використовуючи новий метод, ризики класифіковані на зовнішні залучення, управління програмами, рівень потоку робіт і робочий пакет, а також технічні, графічні, операційні, ділові та організаційні категорії. Ризики були проаналізовані за допомогою даного методу, що дозволило нам кількісно оцінити ризик і вплив на високий (В), середній (П) і низький (Н) рейтинг тяжкості. Ці результати можуть допомогти розробити відповіді реакції на кожний ризик та

призначити відповідні витрати. Регулярні цикли контролю ризику допомагають керувати мінливим ризиком в організаційній ієрархії та з часом.

Також на основі розробленого методу було зроблено ризик-орієнтований аналіз проекту ERP в ході чого було розраховано суму інвестицій на розгортання ERP системи, витрати від реалізації можливих загроз, ризики в залежності від рівня джерела загрози і визначено, що ризики набагато більші ніж сума інвестицій. На базі цих розрахунків були оцінені конкурентноспроможність та ефективність системи, за якими дана система має коефіцієнт конкурентноспроможності більше 1 .

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Інститут управління проектами. Посібник з управління проектами: блок знань / Інститут управління проектами., 2000. – 368 с.
2. Аль-Машарі, М., Аль-Мудімі, А і Заїрі, М. Планування ресурсів підприємства: таксономія критичних факторів / Аль-Машарі, М., Аль-Мудімі, А і Заїрі, М.., 2003. – 364 с.
3. Директива Європейського Союзу про конфіденційність даних та міжнародні відносини, 2002. – 734 с.
4. Алоіні Д. Управління ризиками у впровадженні проекту ERP: огляд літератури. Інформація та управління / Д. Алоіні, Р. Думлін, В. Мінінно., 2007. – 623 с.
5. ISO 31000:2018 Risk management -- Guidelines [Електронний ресурс] // ISO. – 2018.
6. Бадрі М. Комплексна 0–1 модель цільового програмування для відбору проектів / М. Бадрі, Д. Девіс, Д. Девіс., 2001. – 302 с.
7. Лоуренс А. Г. Емпіричні дані про детермінанти інвестицій у кібербезпеку у приватному секторі / А. Г. Лоуренс, П. Л. Мартін, Ч. Лей., 2018. – 21 с.
8. Хоускен К. Повернення до інформаційної безпеки інвестицій: ефект альтернативних функцій порушення інформаційної безпеки на оптимальні інвестиції та чутливість до вразливості /, 2006.
9. Мандал Р. Питання впровадження ERP: приклад. / Р. Мандал., 2003. – 357 с.
10. Хуанг С. Оцінка ризиків у проектах ERP: визначення та визначення пріоритетів факторів / С. Хуанг., 2004. – 705 с.
11. Мадсен М. Визначення найважливіших питань у реалізації планування ресурсів підприємства (ERP) / М. Мадсен., 2005. – 638

с.

12. Алойні Д. Управління ризиками у впровадженні проекту ERP: огляд літератури / Девід Алойні., 2007.
13. Вуу Ш. Критичні фактори успіху для впровадження ERP: випадок китайського виробника електроніки / Ш. Вуу., 2007. – 573 с.
14. Нгай Ю. Вивчення критичних факторів успіху при прийнятті планування ресурсів підприємства / Ю. Нгай., 2008. – 615 с. – (Комп'ютери в промисловості).
15. AXELOS. Управління успішними проектами з PRINCE2 / AXELOS., 2017. – (The Stationery Office Ltd).
16. Мєддісон І. Структура для оцінки проектів ERP / І. Мєддісон., 2000. – 313 с. – (Міжнародний журнал виробничих досліджень).
17. В. В. Андрианов С. Л. Зефиров В. Б. Голованов Н. А. Голдуев Обеспечение информационной безопасности бизнеса [Електронний ресурс] режим доступу: https://pqm-online.com/assets/files/lib/books/andrianov.pdf
18. Балашов П. А. Оценка рисков информационной безопасности на основе нечеткой логики / П. А. Балашов, В. П. Безгузиков, Р.И.Кислов // [Електронний ресурс] режим доступу: http://www.nwaktiv.ru/textstat2/index.html
19. Архипов О.Є., Муратов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: монографія / Олександр Євгенійович Архипов, Олексій Євгенович Муратов. – К.: Наук.-вид. відділ Національної академії Служби безпеки України, 2011. – 193 с.
20. Архипов О.Є. РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К ОЦЕНИВАНИЮ «РАЗУМНОГО» ОБЪЕМА ИНВЕСТИЦИЙ В

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ / Архипов О.Є. – НТУУ «КПИ им. Игоря Сикорского»

21. Романов П. С. Интеллектуальные информационные системы в экономике / П. С. Романов – М.:Издательство «Экзамен», 2003 – 496 с