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

студентки ***Копач Вікторії Владиславівни***

академічної групи ***125-20-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка політики безпеки при використанні ERP-системи для компанії «Фінансовий Консалтинг»***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ас. Олішевський І.Г.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студентці ***Копач Вікторії Владиславівні*** **академічної групи** ***125-20-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка політики безпеки при використанні ERP-системи для компанії «Фінансовий Консалтинг»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.24 р. № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Розглянути стан питання актуальності та безпеки ERP-систем, обстежити інформаційно-комунікаційне та інформаційне середовища компанії «Фінансовий Консалтинг», обрати профіль захищеності ІКС	15.03.2024
Розділ 2	Проаналізувати профіль захищеності ІКС компанії, оцінити відповідність ERP-систем вимогам безпеки, розробити політику інформаційної безпеки	10.05.2024
Розділ 3	Економічно обґрунтувати доцільність розробки та впровадження політики безпеки при використанні ERP-системи у компанії	11.06.2024

Завдання видано _____ Ілля ОЛІШЕВСЬКИЙ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Вікторія КОПАЧ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 83 с., 4 рис., 5 табл., 4 додатка, 14 джерел.

Об’єкт дослідження: ERP-системи, розглядувані для потенційного впровадження в компанії «Фінансовий Консалтинг».

Предмет розробки: політика безпеки інформації ERP-системи для компанії «Фінансовий Консалтинг».

Мета роботи: підвищити рівень захищеності обраної ERP-системи в компанії «Фінансовий Консалтинг».

У першому розділі було піднято питання актуальності використання ERP-систем. Окрім того, було проаналізовано типові вразливості ERP-систем та методи їхнього усунення. На завершення, було ознайомлено зі структурою компанії «Фінансовий Консалтинг» та обрано профіль захищеності її ІКС.

У другому розділі було проведено аналіз реалізації послуг обраного профілю захищеності та оцінено відповідність кожної з розглядуваних ERP-систем до загальних вимог безпеки та потреб компанії. В результаті оцінки було узагальнено яка ERP-система найбільше відповідає цим критеріям, після чого було розроблено політику безпеки для її подальшого використання.

У третьому розділі було розраховано капітальні та поточні витрати на впровадження політики безпеки та подальшого функціонування системи підприємства. Також було розраховано потенційні фінансові ризики та період окупності витрат на впровадження політики безпеки для обраної ERP-системи.

Практична цінність дослідження полягає у підвищенні безпеки та оптимізації бізнес-процесів у компанії «Фінансовий Консалтинг». Розроблена політика безпеки допоможе ефективно управляти ризиками, пов'язаними з використанням ERP-системи.

КІБЕРБЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, ПОЛІТИКА БЕЗПЕКИ, СТРАТЕГІЯ БЕЗПЕКИ, ТИПОВІ ВРАЗЛИВОСТІ ERP-СИСТЕМ, УПРАВЛІННЯ РИЗИКАМИ.

ABSTRACT

Explanatory note: 83 pp., 4 pic., 5 table, 4 app, 14 sources.

Object of the study: ERP systems considered for potential implementation in the "Financial Consulting" company.

Subject of the development: ERP system information security policy for the "Financial Consulting" company.

The aim of the study: to increase the level of security of the selected ERP system in the "Financial Consulting" company.

In the first section, the issue of the relevance of ERP systems was raised. In addition, typical vulnerabilities of ERP systems and methods of their addressing were analysed. Finally, the structure of the "Financial Consulting" company was described and the security profile of its ICS was selected.

In the second section, it was analysed the implementation of services of the selected security profile and assessed the compliance of each of the ERP systems under consideration with the general security requirements and needs of the company. As a result of the assessment, it was summarised which ERP system best meets these criteria, and then it was developed a relevant information security policy for its further use.

In the third section, it was calculated the capital and current costs of implementing the security policy and further functioning of the enterprise system. The potential financial risks and payback period for the implementation of the security policy for the selected ERP system were also calculated.

The practical value of the study is to improve security and optimise business processes in the "Financial Consulting" company. The developed security policy will help to effectively manage the risks associated with the use of the ERP system.

CYBERSECURITY, THREAT MODEL, SECURITY POLICY, SECURITY STRATEGY, TYPICAL VULNERABILITIES OF ERP SYSTEMS, RISK MANAGEMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ERP	–	Enterprise Resource Planning;
Д	–	доступність;
ІКС	–	інформаційно-комунікаційна система;
К	–	конфіденційність;
КЗЗ	–	комплекс засобів захисту;
КС	–	комп’ютерна система;
ОС	–	операційна система;
ПЗ	–	програмне забезпечення;
ПК	–	персональний комп’ютер;
С	–	спостережність;
СУБД	–	система управління базами даних;
Ц	–	цілісність.

ЗМІСТ

с.

ВСТУП

З кожним роком кількість кіберзагроз зростає, тому важливим фактором у протидії їм є регулярний перегляд та оновлення політики безпеки підприємства. Цей крок дозволяє запобігти багатьом проблемам, попереджуючи порушення основних характеристик інформаційної безпеки та подальшого витоку критичних даних.

Особливого захисту потребує ERP-система, що останніми роками почала активно поширюватись у малі та великі бізнеси, стаючи головним провідником оптимізації доступу до даних та автоматизації процесів. Такий зріст спричинений активним розвитком технологічного ринку та пандемією COVID-19, що кинула нові виклики для бізнесу та змусила перейти на дистанційний формат роботи. В Україні цю ситуацію ще загострила російсько-українська війна, через що постало питання ефективного управління даними та процесами навіть в нестабільних умовах.

Таким чином, актуальність даної роботи зумовлена необхідністю адаптації бізнес-процесів до сучасних умов. Розробка політики безпеки інформації при використанні ERP-системи стане вагомим внеском у забезпеченні безпеки функціонування компанії «Фінансовий Консалтинг», збереженні її конфіденційних даних та зменшенні ризиків кібератак.

Об’єктом кваліфікаційної роботи є ERP-системи, розглядувані для потенційного впровадження в компанії «Фінансовий Консалтинг».

Предметом кваліфікаційної роботи є політика безпеки інформації ERP-системи для компанії «Фінансовий Консалтинг».

Метою даної роботи є підвищення рівня захищеності обраної ERP-системи в компанії «Фінансовий Консалтинг» задля забезпечення конфіденційності, цілісності та доступності циркулюючих корпоративних даних та процесів.

Завдання роботи включають:

1. Розглянути важливість використання ERP-системи з точки зору безпеки.

2. Проаналізувати типові вразливості та атаки на ERP-системи.

3. Детально ознайомитись з обчислювальним та інформаційним середовищем компанії.

4. Обрати та обґрунтувати вибір профілю захищеності.

5. Сформулювати критерії оцінки ERP-систем, враховуючи міжнародні та українські стандарти безпеки.

6. Оцінити загальний рівень безпеки та відповідності кожної з ERP-систем згідно з потребами компанії.

7. Розробити політику безпеки інформації при використанні обраної ERP-системи.

8. Провести економічні підрахунки доцільності впровадження розробленої політики безпеки.

Отже, практична цінність цієї кваліфікаційної роботи полягає у підвищенні безпеки та оптимізації бізнес-процесів у компанії «Фінансовий Консалтинг», враховуючи ріст кіберзагроз та непередбачуваність геополітичної ситуації. Розроблена політика безпеки допоможе ефективно управляти ризиками, пов'язаними з використанням ERP-системи.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Важливість політики безпеки

Щороку кількість кіберзагроз у цифровому світі зростає, і це ставить бізнес-сектор перед необхідністю звернути особливу увагу на вдосконалення безпеки. Недостатній рівень захищеності може призвести до серйозних наслідків у компанії, зокрема до фінансових збитків, втрати довіри клієнтів, порушення репутації та розладу в управлінні бізнесом. Окрім того, згідно з Законом України «Про захист інформації в інформаційно-комунікаційних системах» [1], у разі порушення захисту інформації у системах підприємства, власник компанії повинен понести юридичну відповідальність. Тому, щоб запобігти потенційним загрозам, вагомий внесок у безпеку діяльності бізнес-організацій становить розробка та впровадження політики безпеки.

Політика безпеки являє собою набір правил, процедур та стандартів, які формуються організацією для захисту її інформації та процесів. За допомогою неї визначаються стратегії управління ризиками та забезпечення безпеки даних. Зазвичай вона включає в себе правила доступу до даних і захисту від кіберзагроз, ґрунтуючись на основі тріади КЦД. Також в ній описуються процедури реагування на інциденти, що допомагає персоналу компанії зрозуміти послідовність дій у разі виникнення критичних ситуації та мінімізувати потенційні збитки.

Існує три види політики інформаційної безпеки:

– організаційна – цей вид політики безпеки визначається на рівні управління організацією, тому включає в себе загальний план положень про безпеку, зазначення правил та процедур, механізми аудиту безпеки;

– системна – ця категорія стосується інформаційних систем, мереж та технологічних платформ і переважно містить в собі зазначення аспектів захисту від несанкціонованого доступу, включаючи механізми автентифікації, авторизації та контролю доступу;

– направлена на вирішення конкретної проблеми – така політика безпеки характеризується своєю тимчасовістю, оскільки будь-яка проблема або інцидент з часом втрачають свою актуальність і на заміну їм приходять інші проблеми та рішення.

Проте незважаючи на свою класифікацію, політика безпеки має слідувати чинному законодавству та відповідати міжнародним стандартам. Одними з таких стандартів є ДСТУ ISO/IEC 27001:2023 [2] та ДСТУ ISO/IEC 27002:2023 [3]. В них наводяться загальні вимоги та рекомендації щодо управління інформаційною безпекою. Завдяки цим стандартам, компанії можуть розробити ефективну політику безпеки, що забезпечить надійний захист даних.

Окрім того, політика інформаційної безпеки має враховувати всі індивідуальні потреби компанії, розпочинаючи від галузі та розміру компанії і закінчуючи технологічними тенденціями і особливостями її інфраструктури. При цьому, для персоналу компанії обов'язково повинні бути проведені регулярні навчання, які допоможуть зрозуміти необхідність політики безпеки та її окремі особливості.

Врахування вищезазначених факторів сприяє створенню надійного рівня захищеності всередині бізнес-організації, а розроблена політика інформаційної безпеки стає придатною для користування.

1.2 Поняття ERP-системи, її класифікації та актуальність

В даній кваліфікацій роботі розглядається розробка саме системної політики безпеки. Така потреба з'явилась завдяки рішенню керівництва компанії перейти на використання ERP-системи замість ведення обліку даних в електронних таблицях та використання окремих програмних застосунків для деяких складних областей.

Останніми роками популярність ERP-систем різко зросла, і це не дивно, оскільки, перш за все, у сучасному світі це чи не одне з найкращих рішень для підприємства завдяки їх здатності інтегрувати бізнес-процеси в єдину систему. ERP-система допомагає поєднати та автоматизувати декілька спектрів операцій, такі як управління фінансами, проєктами та взаємодією з клієнтами. Окрім того,

вона дозволяє централізовано зберігати дані, що забезпечує актуальність та точність циркулюючої інформації.

Для деяких підприємств використання ERP-систем стало вимушеним кроком через нові для багатьох умови праці, які запровадила пандемія COVID-19. З 2020 року в компаніях прискорився перехід на віддалену роботу, тому потрібно було знайти технологію, що допомогла б використовувати та управляти даними на відстані. Завдяки тому, що ERP-система вдало виконує ці функції, вона стала ключовим елементом у полегшенні адаптації підприємств до змін на ринку та у світі. Підтвердженням цього є статистика використання ERP-систем підприємствами деяких європейських країн на прикладі 2019 та 2023 років, що зображена на рис. 1.

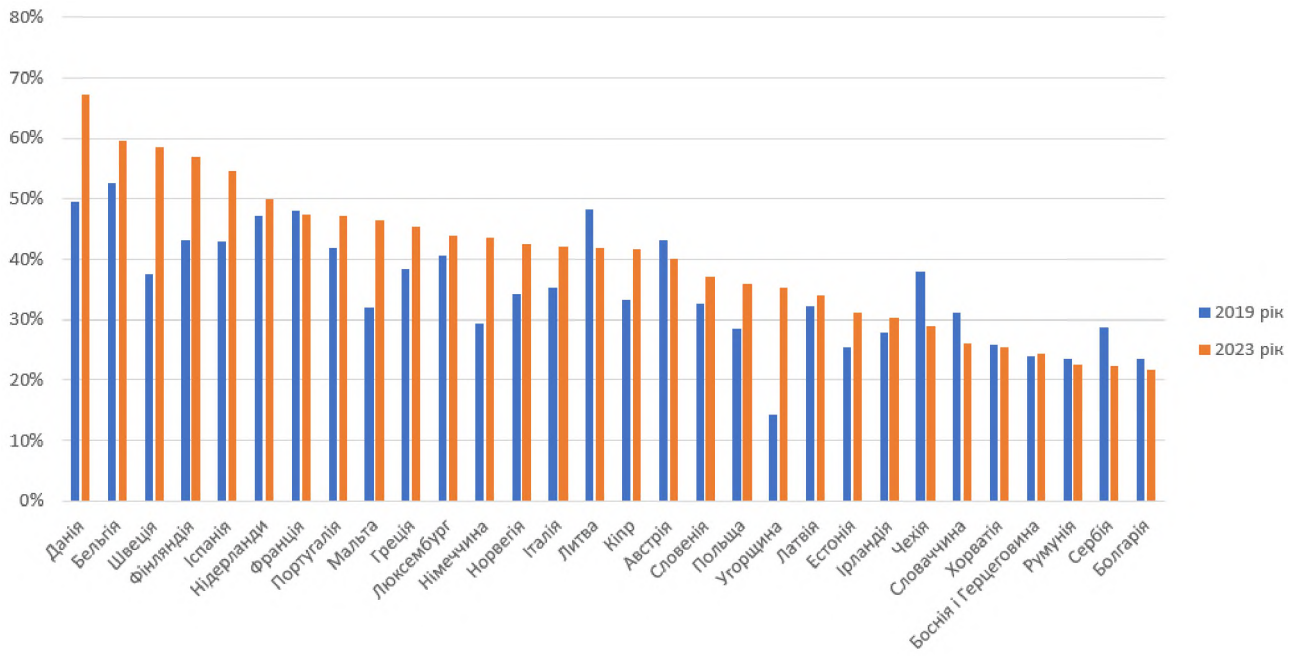

Рисунок 1.1 – Статистика використання ERP-систем у 2019 та 2023 роках підприємствами європейських країн

Примітки:

1 Створено на основі даних Eurostat [4].

2 У статистику не включені країни, по котрим відсутні деякі дані, зокрема це Албанія, Україна, Ісландія, Велика Британія та інші.

Можна побачити, що за 4 роки кількість використання ERP-систем на підприємствах здебільшого зросла, особливо слід виокремити Данію, Бельгію, Швецію, Фінляндію та Іспанію, у яких процентний рівень використання ERP-систем підприємствами перевищує 50%. Це безумно говорить про перевагу ERP-систем над альтернативними їм рішеннями. Звісно, на гістограмі також присутні країни, чиї показники суттєво зменшилися, наприклад, Литва, Чехія та Сербія. Такі дані, скоріше за все, свідчать про вірогідні економічні труднощі або відсутність підтримки підприємств державою. Проте варто зауважити, що загалом країн, в яких зафіксований ріст використання ERP-рішень, приблизно у 2,5 рази більше ніж країн, в яких стався спад. Отже, загалом ERP-системи в дійсності поширюються у сферу бізнесу, підтверджуючи власну важливість для ефективного управління підприємствами та їхнього подальшого розвитку.

Що стосується України, то тут також відбувається розквіт ERP-систем у бізнес-секторі. Окрім того, що українські компанії, як і весь світ, спіткала пандемія COVID-19, великою загрозою ще стала російсько-українська війна. Через це бізнесу знадобилось рішення, завдяки якому можна було б знайти стабільність та безпеку навіть у складних умовах. За даними Statista [5] очікується, що у 2024 році дохід на українському ринку ERP-систем складе 254,50 мільйонів доларів США, що у два рази більше ніж отриманий дохід за 2022 рік. Це підтверджує активний перехід українських підприємців на більш сучасні технології.

Враховуючи тенденцію розвитку ERP-рішень, варто детальніше дослідити цю систему та її складові, щоб отримати глибше розуміння її внутрішнього функціонування.

ERP-система – це комплексне програмне забезпечення, яке допомагає бізнесу в автоматизації та інтегруванні робочих процесів в компанії. Така система має типову структуру: фундамент у вигляді платформи, що в свою чергу складається з ядра, базових функцій та системи керування даними, та модулі. Якщо стосовно платформи все зрозуміло – вона має незмінну структуру і забезпечує коректну обробку та зберігання даних, то модулі є більш гнучкими –

їх може бути різна кількість з різним призначенням та вони можуть бути додані або вилучені з системи за потреби. Відповідними прикладами можуть бути модулі щодо управління проєктами, відносинами з клієнтами, працівниками, виробництвом, фінансами, активами підприємства, тощо.

ERP-система може бути впроваджена у будь-який бізнес, проте особливою увагою користуються сектори виробництва, інформаційних технологій та професійних, зокрема фінансових, послуг. Відповідну статистику можна побачити на рис. 2.

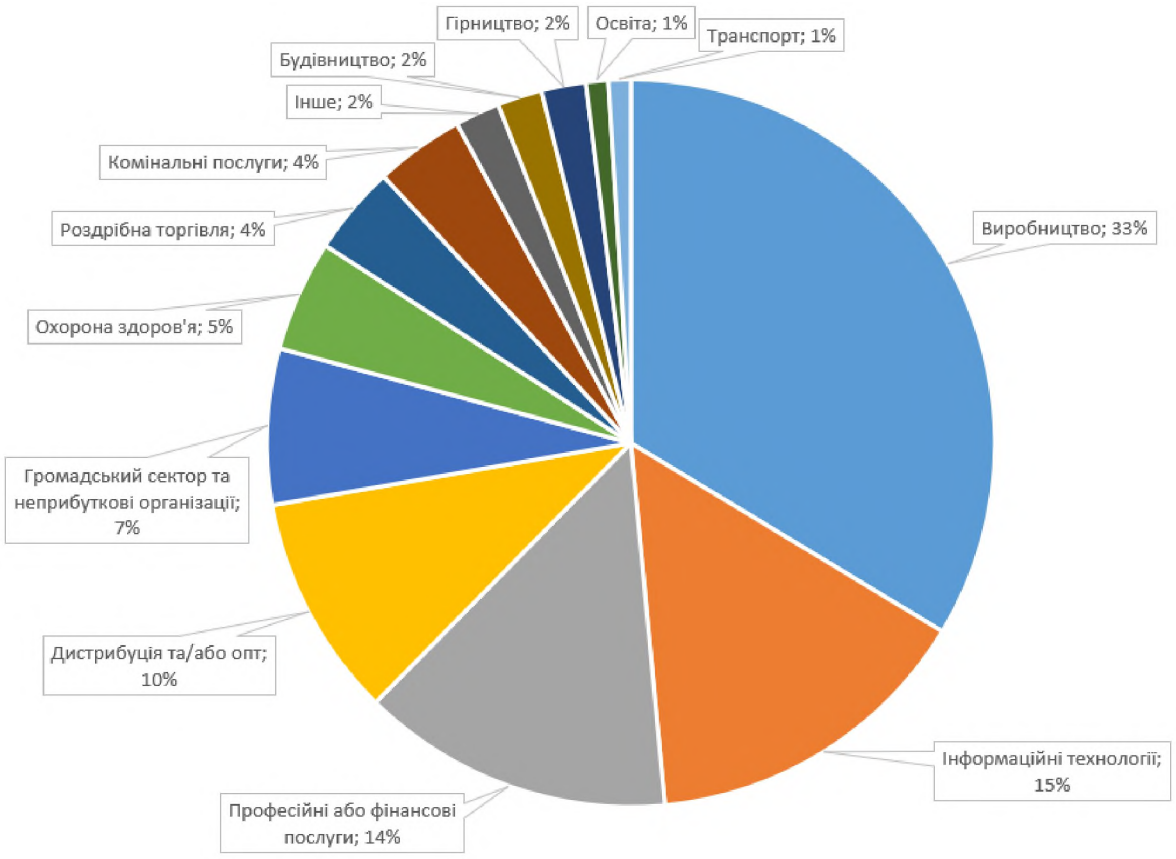

Рисунок 1.2 – Статистика користування ERP-системами згідно з галуззю підприємств

Примітка. Створено на основі даних TechReport [6]

Задовільнити власні потреби, підприємства можуть за допомогою широко популярних ERP-рішень, наприклад таких як Oracle ERP Cloud, Microsoft Dynamics 365, SAP ERP, Odoo, Sage ERP та інших. Українською альтернативою є

IT-Enterprise, що не менш поширена на національному IT-ринку. Окрім того, компанія може розробити власну ERP-систему. Це має значні переваги щодо побудови власної комфортної структури системи, відповідних модулів та загального управління, але в такому випадку слід розуміти, що без професійної команди програмістів та фінансової підтримки не впоратись.

Окрім різновиду постачальника послуг, ще існують різні класифікації ERP-систем, але найбільше слід акцентувати увагу на розподіленнях:

– за архітектурою;
– за типом організації;
– за типом розгортання.

Для подальшого коректного вибору ERP-системи, слід ознайомитися з кожним зазначеним видом окремо.

Архітектура ERP-системи має велике значення в доступності даних, адже неправильно підібраний вид системи може ускладнити процес користування інформацією. Існує два розподіли ERP-систем за їхньою архітектурою: єдині та модульні. Єдина архітектура передбачає відсутність окремих модулів – замість цього всі необхідні функції поєднані в єдину систему та мають між собою тісний зв'язок. Така система є більш простою у використані, але тягне за собою значні витрати на впровадження та обслуговування. Модульна ж архітектура логічно поділена на модулі, кожен з яких відповідає за конкретну функцію підприємства. Такий підхід дозволяє більш легко оновлювати та розширювати систему. Окрім того, існує можливість обирати лише ті модулі, якими компанія або деякі працівники будуть користуватись – це допомагає зосередитись на потрібних процесах та обмежити доступ до важливої інформації.

Наступний вид ERP-систем визначається за типом їхньої організації. Він включає в себе публічні, приватні та гібридні системи. Публічні системи є досить доступними: вони зазвичай розташовані на хмарних сервісах та є недорогими, оскільки оплата за таку послугу здійснюється на основі підписки. Проте є багато питань щодо безпеки таких систем – не можна гарантувати, що дані на платформі будуть повністю конфіденційними через те, що уся інформація у таких системах

зберігається на сторонніх серверах. На відміну від публічної ERP-системи, приватні є значно безпечнішими завдяки тому, що всі дані зберігаються на власних серверах компанії, але цьому є й відповідний наслідок – вартість підтримки такої системи буде значно відрізнятись і може виявитись завеликою, особливо для маленьких підприємств. Гібридна ж система поєднує в собі переваги публічних та приватних систем – вона є фінансово доступною та дозволяє частину даних, зокрема критичних, зберігати на власному сервері, а іншу інформацію оброблювати на хмарних сервісах.

Остання, найбільш поширена, класифікація ERP-систем – за типом розгортання. Вона містить в собі системи з локальним, хмарним та гібридним розгортанням. Локальне розгортання передбачає встановлення ERP-системи на сервери підприємства, хмарне розгортання – використання хмарних технологій, а гібридна – комбінацію цих двох видів. Опис цієї класифікації схожий з описом попередньої, за типом організації, проте вони мають суттєву різницю у підґрунті. Тип розгортання вказує на місце розташування технічної інфраструктури системи в той час, як тип організації – на те, яким чином організована та як контролюється система. Це грає рішучу роль у визначенні доступності та безпеки даних в ERP-системі.

Незалежно від класифікації ERP-системи, вкрай необхідно розуміти механізми захисту та безпеки – це є критичним при виборі системи. Зазвичай використовуються такі механізми як автентифікація та авторизація, аудит подій, шифрування та резервне копіювання даних, використання брандмауерів, тощо. Застосування цих механізмів дозволяє підприємству досягти багаторівневого захисту та підтримувати високий рівень безпеки навіть у разі виникнення потенційних загроз.

1.3 Наслідки використання ERP-системи

Впровадження ERP-системи може стати вирішальним кроком у подальшому розвитку бізнесу. Дана система може поліпшити процес роботи та підвищити фінальну якість послуги чи продукту. Проте важливо пам’ятати, що так стається не завжди.

За даними TechReport [6], половина початкових спроб впровадити ERP-систему закінчується невдало. Сам процес впровадження ERP-системи є доволі складним, і під час його виконання можна спіткнутись з численними викликами. У багатьох первинне налаштування ERP-системи викликає складнощі, здебільшого це пов'язано з процесом її інтеграції з базою даних, програмними застосунками чи іншими існуючими системами підприємства. Усі ці елементи повинні узгоджено та безперебійно працювати, вільно взаємодіяти один з одним. Ще складнішим процес налаштування стає у випадку, коли інші системи підприємства використовують відмінні від ERP-системи технології та платформи або мають інших формат збереження даних. Такі аспекти обов'язково повинні враховуватись при конфігурації системи задля запобігання конфліктів між різними програмними середовищами.

Досить часто компанії недооцінюють тривалість впровадження ERP-системи, внаслідок чого реалізація проєкту відстрочується, що тягне за собою додаткові витрати. До речі, фінансові розрахунки щодо тих самих ERP-системи також залишаються недооціненими, через що доводиться значно підвищувати бюджет проєкту. У підтвердження того, TechReport [6] повідомляє, що кожний третій раз терміни впровадження ERP-системи подовжуються, а загальна сума витрат часто перевищує початкові прогнози у 3-4 рази. Такі наслідки можуть залишити свій відбиток на фінансовому становищі компанії, циркулюючих процесах та загальному настрої команди.

Значні ризики можуть бути пов'язані і з недостатньою підготовкою персоналу, оскільки працівники компаній часто чинять опір подібним змінам та демонструють незацікавленість у нововведеннях. Це може спричинити додаткові витрати на навчання, а також тимчасове зниження продуктивності.

Після впровадження ж, ERP-система має регулярно оновлюватись та отримувати достатній рівень технічного обслуговування. Несправності та помилки, що залишаються без уваги під час роботи, особливо у період знайомства з системою, здатні призвести до втрати даних та порушення безпеки системи загалом.

І не менш важливий аспект уваги необхідно приділити саме безпеці ERP-системи та даних і процесів, що оброблюються нею. Забезпечення належного рівня захисту інформації є критичним для будь-якої системи, але оскільки ERP-системи оброблюють величезний об'єм даних та нерідко пов'язані з іншими застосунками, то недбале ставлення до такої системи може спричинити витік інформації та порушення загальної безпеки компанії. Відсутність спеціаліста, що міг би контролювати захищеність такої системи та належним чином аналізувати її вразливості, негативно вплине на безпечність інформаційно-комунікаційної системи компанії та навіть може привернути увагу хакерів.

1.4 Типові вразливості та атаки на ERP-системи

Будь-яка система, на жаль, має свої слабкі місця, але найголовнішим є зменшення кількості таких слабкостей та запобігання витоку інформації через ці місця. Саме тому варто окремо розглянути найбільш критичні вразливості у ERP-системах. Їх можна поділити на такі групи:

– технічні – вони безпосередньо пов'язані з помилками у програмному та апаратному забезпечені, мережевих компонентах;

– організаційні – такі вразливості виникають внаслідок проблем з управлінням безпекою та недосконалістю політики безпеки;

– людські – це вразливості, що стосуються, насамперед, працівників та людського фактору у процесі роботи.

Кожна з таких вразливостей здатна суттєво вплинути на безпеку ERP-системи та компанії в цілому, тому слід детально розглянути кожну з груп.

Технічні вразливості передусім включають у себе типові недоліки програмного забезпечення, такі як помилки у коді, особливо якщо ERP-система є індивідуальною розробкою компанії. Крім того, доволі примітивною, але поширеною є проблема автентифікації – слабкі паролі, які легко вгадати або підібрати за допомогою словників, можуть стати причиною несанкціонованого доступу до системи. Ненадійні алгоритми шифрування, такі як DES, 3DES, MD5, SHA-1 та інші, можуть призвести до розшифровки конфіденційної інформації. Неналежний контроль введених даних у систему створює ризик впровадження у

базу даних SQL-ін'єкцій. Погано захищені компоненти мережі нерідко є головною причиною DDoS-атак, а відсутність регулярних оновлень може додатково посилити вразливість системи до загроз. Також до технічних вразливостей варто віднести неправильні налаштування брандмауерів та антивірусного програмного забезпечення – наслідком цього може стати поява шкідливого коду.

Під організаційними вразливостями зазвичай маються на увазі такі слабкості як неправильне управління доступом – якщо деякий працівник має занадто широкі, як для своїх потреб, права користувача, то це може спричинити використання доступних привілей у корисливих цілях або може привернути увагу хакерів. З цього також витікає відсутність гідного рівня аудиту та моніторингу безпеки – без цих важливих процесів компанія може навіть не помітити підозрілу активність користувачів у системі. Ще одним яскравим прикладом організаційних вразливостей є політика безпеки, оскільки недостатня увага розробці і дотриманню політик безпеки (як організаційної, так і системних), а також нерозуміння її положень працівниками компанії можуть спричинити порушення безпеки.

Але найбільш поширеними є саме людські вразливості – три чверті успішних кібератак беруть свій початок від людини. Це зумовлено тим, що людський фактор відіграє ключову роль у функціонуванні будь-якої системи, зокрема й ERP. Неналежна підготовка персоналу здатна призвести до недосконалого розуміння та виконання правил безпеки компанії. Часто працівники не усвідомлюють потенційні ризики та загрози для їхніх даних, тому можуть нехтувати встановленими процедурами, тим самим наражаючи компанію на небезпеку. Такі працівники є особливо привабливою мішенню, оскільки необізнана людина більш вірогідно попадеться на гачок зловмисників. Фішинг та соціальна інженерія є найбільш яскравими прикладами наслідків людської вразливості. Ці атаки допомагають вводити людей в оману та отримувати бажане – від конфіденційної інформації до повноцінного доступу до облікових записів.

Комбінація декількох з перелічених вразливостей створює більш комфортне для зловмисників середовище. Вразливості можуть взаємодіяти, посилюючи загальні ризики для компанії. Нерідко наслідками такої кооперації є шкідливе програмне забезпечення, яке ще називають Malware, та програми-вимагачі Ransomware. Ключова ціль таких атак полягає у доступі до конфіденційних даних або їхньому блокуванні. Ці атаки можуть мати катастрофічні наслідки – такі програми здатні уразити усю систему та навіть знищити її.

Підтвердженням небезпек вразливостей є статистика від World Metrics [7] – за їхніми даними, за останні 10 років близько 60% підприємств постраждали від витоку даних у ERP-системах. Більш того, під час впровадження ERP-системи у 85% випадків підприємства переживають хоча б один кіберінцидент. Це безперечно говорить про недостатню підготовку та усвідомлення масштабів важливості захисту інформації у ERP-системах.

Задля підвищення рівня безпеки програмного забезпечення, у тому числі й ERP-систем, у 2001 році в США було засновано некомерційний фонд Open Web Application Security Project (OWASP). З 2021 року він поширився на країни Європи. Головним фокусом OWASP є ідентифікація та зменшення ризиків безпеки у вебдодатках та програмному забезпеченні. Ця спільнота щорічно організовує освітні конференції з метою обізнаності у галузі кібербезпеки. Також вони розроблюють власні інструменти та ресурси для фахівців з інформаційної безпеки, враховуючи власні стандарти та документи. Одним з таких надбань є список OWASP Top 10 [8]. Даний документ оглядає найкритичніші вразливості та відображає актуальні тенденції сучасних загроз. Деякі зі згаданих вище прикладів вразливостей ERP-систем входять до цього списку, зокрема до найвищих позицій, посідаючи перші три місця: порушення авторизації на рівні об’єкта, порушення автентифікації, порушення авторизації на рівні властивості об’єкта. Такі дані свідчать про критичність вразливостей, що пов'язані з авторизацією та автентифікацією, оскільки вони можуть допустити несанкціонований доступу до даних та подальшу компрометацію ERP-системи.

1.5 Методи запобігання кіберзагроз

На поточний момент кіберспеціалісти не можуть запропонувати універсального рішення, що змогло б гарантувати захищеність ERP та інших систем. Проте існує ряд практик, які мають на меті забезпечення належного рівня безпеки.

Взагалі, до такого питання слід підходити комплексно – перш за все, необхідно окреслити ризики для ERP-системи, визначити методи їхнього функціонування, після чого сформулювати план реагування на кіберінциденти. У цьому допомагає політика інформаційної безпеки – вона здатна значно скоротити величину збитків та попередити загрози.

Наступна практика полягає у регулярному оновлені програмного забезпечення – операційних систем та окремих програмних, таких як ERP. Не дарма поставники ПЗ наполегливо рекомендують встановлювати лише найновіші версії їхнього продукту – це, насамперед, пов'язано зі зменшенням ризиків реалізації загроз.

Особливо важливим пунктом для будь-якої системи є контроль доступу. Завжди потрібно слідувати правилу найменших привілей. Тобто кожний користувач системи повинен бути забезпечений мінімальним набором функцій для якісного виконання власної роботи. Це набагато зменшує вірогідність зловживання доступними можливостями всередині компанії.

Також допомогти у контролі доступу до системи можуть засоби автентифікації та авторизації. Корисним є впровадження багатофакторної автентифікації, оскільки вона забезпечує додатковий рівень захисту. Таким чином замість того, щоб просто ввести пароль, користувач повинен додатково надати фактор володіння або фактор властивості. Авторизація ж має за собою мету підтвердження того, які користувачі мають доступ до яких функцій системи – без цього неможливо забезпечити належний рівень безпеки та контролю.

Крім того, для кожної системи, враховуючи ERP, важливо вести журнал подій. Таким чином легко відслідкувати будь-які підозрілі дії та запобігати несанкціонованому доступу чи атаці. Під час робочого дня таку діяльність

організувати простіше – даний обов'язок можна покласти на системного адміністратора, але для неробочого часу варто мати додаткову автоматизовану систему виявлення аномалій та попередження про них.

Можна відслідковувати не лише події через відповідні журнали, а й трафік мережі за допомогою міжмережевих екранів та системи запобігання вторгнень. Вони працюють у тісному зв'язку – міжмережеві екрани контролюють вхідний та вихідний трафік на основі вказаних правил та блокують підозрілу активність в той час як системи запобігання вторгнень реагують на виявлені загрози в режимі реального часу. Незважаючи на те, що системи запобігання вторгнень глибше аналізують систему, не рекомендується використовувати їх без міжмережевих екранів, оскільки вони є базовим компонентом у фільтрації трафіку та завдяки певним правилам здатні швидко оброблювати велику кількість запитів. Тому комбінація цих двох технології дозволяє надійно захистити систему від складних атак та підвищити рівень захисту, оскільки навіть якщо міжмережевий екран пропустить якусь загрозу, то система запобігання вторгнень допоможе утилізувати її.

Щоб бути впевненими у конфіденційності та цілісності даних, слід шифрувати дані як під час зберігання, так і під час транспортування. Рекомендується використовувати у цьому процесі саме алгоритм AES-256. Його головна перевага, окрім забезпечення вищого рівня захищеності, полягає у стійкості до криптоаналітичних атак та у високій продуктивності, проте він має і деякий недолік – він споживає доволі багато ресурсів та енергії. Також гарними варіантами з точки зору безпечності шифрування даних є AES-128 і AES-192 (той самий AES-256, але з меншою довжиною ключа), RSA та еліптичні криві. Будь-який з цих варіантів здатен надати якісний рівень безпеки.

Проте на випадок непередбачуваних ситуацій, завжди необхідно мати резервні копії системи та даних. Така практика надає можливість оперативно відновити систему у разі кібератаки та продовжити робочі процеси. Найкраще за все, щоб резервне копіювання здійснювалося автоматично. Зберігати резервні копії варто у кількох місцях, включаючи віддалені або хмарні сховища, та, більш

того, важливо регулярно перевіряти цілісність та працездатність резервних копій, виконуючи тестові відновлення.

Кібербезпека ERP-системи та бізнесу загалом залежить на лише від пристроїв та технологій, а й від персоналу підприємства. Тому ще одним методом запобігання загроз є навчання працівників. Завдяки підвищенню рівня їхньої обізнаності, можна вберегти систему від низки загроз, що пов'язані з людськими вразливостями.

1.6 Опис компанії «Фінансовий Консалтинг»

«Фінансовий Консалтинг» – це невелика українська компанія, що надає послуги у сфері фінансового консалтингу. Зокрема компанія надає консультації щодо планування фінансів та податків, інвестиційних стратегій та управління активами, а також допомагає вести бухгалтерський облік та готувати фінансові звіти. Цільовою аудиторією є малі та середні бізнеси.

Режим роботи компанії обмежується з 9 до 18 години з годинною перервою між 13 та 14 годинами. Даний графік діє з понеділка по п'ятницю. Субота та неділя є вихідними днями. Додатково графік може коригуватися в залежності від святкових днів.

Організаційна структура підприємства складається з таких підрозділів: керівництво компанії, відділ фінансових консультацій, відділ бухгалтерського обліку та планування податків, відділ управління проєктами, відділ маркетингу та відділ адміністративної підтримки. Загалом кількість персоналу налічує 30 осіб. Огляд кожного з підрозділів надано нижче.

Керівництво компанії включає в себе генерального та фінансового директорів. Генеральний директор відповідає за стратегічне управління підприємством та загальний розвиток компанії, фінансовий директор – за управлінням бюджетом та контроль за фінансовими операціями.

Відділ фінансових консультацій містить у собі керівника відділу та 4 фінансових консультанти. Керівник організовує роботу у відділі та слідкує за якістю виконання проєктів. Консультанти ж надають консультації клієнтам з приводу фінансових питань, керують відповідними проєктами, фіксуючи там

відповідну інформацію стосовно фінансового стану клієнтів, аналізують фінансові звіти, оцінюють ризики та можливості розвитку клієнтів.

Відділ бухгалтерського обліку та планування податків включає в себе керівника відділу, що організовує та координує роботу відділу, головного бухгалтера, що відповідає за фінансові процеси самої компанії, враховуючи розрахунок та виплату заробітної плати, ведення внутрішньої звітності та забезпечення фінансової стабільності підприємства, з 5 бухгалтерів, що ведуть облік, розрахунки та звітності для клієнтів, передаючи необхідні документи фінансовим консультантам для аналізу, та з 2 податкових консультантів, які виконують розробку податкових стратегій та надають консультації стосовно податкового законодавства.

Відділ управління проєктами складається з керівника відділу та 3 менеджерів проєктів. Керівник відповідає за планування та управління всіма проєктами компанії, зокрема забезпечуючи їх вчасне виконання та дотримання бюджетів. Менеджери проєктів здійснюють моніторинг прогресу реалізації проєктів, вирішують питання, що виникають у процесі роботи над проєктами, та комунікують з клієнтами, звітуючи щодо виконання проєктів.

Відділ маркетингу містить у своєму складі керівника відділу, 3 менеджери та 2 фахівця з маркетингу. Керівник відділу розробляє та впроваджує маркетингові стратегії, організовує роботу команди. Менеджери займаються пошуком нових клієнтів, веденням переговорів, укладенням контрактів та підтримкою стосунків з існуючими клієнтами. Фахівці з маркетингу реалізують рекламні кампанії, проводять аналіз ринку та займаються просуванням бренду.

Відділ адміністративної підтримки складається з офіс-менеджера, 2 асистентів та системного адміністратора. Офіс-менеджер забезпечує організацію роботи офісу та вирішує організаційні питання. Асистенти допомагають в організації зустрічей та веденні документації. Системний адміністратор відповідає за підтримку та обслуговування комп'ютерних систем, мереж, програмного забезпечення, забезпечення кібербезпеки та технічної підтримки.

Щомісяця компанія отримує дохід приблизно у розмірі 1,3 мільйони гривень, а щомісячні витрати сягають суми приблизно у 740 тисяч гривень. Витрати включають у себе оренду офісу та оплату комунальних послуг, виплату заробітної плати всіх працівникам, витрати на канцелярію, ліцензії на програмне забезпечення, консультації з юристом, податки, рекламні кампанії, регулярне навчання персоналу, тощо.

Офіс компанії знаходиться у бізнес-центрі за адресом м. Дніпро, просп. Пилипа Орлика, буд. 11, офіс 402. Загальна площа офісу становить близько 220 м2. Сам офіс складається з кабінету керівників, окремих зон для кожного відділу, кабінету для нарад, серверної кімнати, зони відпочинку та кухні, зони очікування, вбиральні і коридорів.

Забезпечення офісу компанії комунікаціями є типовим: водопостачання та опалення є централізованими, на кожному поверсі бізнес-центру є окрема кімната з електрощитовим обладнанням, а у кожному офісі встановлена своя розподільча панель. Система каналізації підключена до міських мереж. Окрім того, в усіх офісах присутня вентиляційна система з механічною подачею та витяжкою повітря. В бізнес-центрі проведено високошвидкісний інтернет. В офісі встановлено внутрішню локальну мережу з використанням Ethernet-кабелів та налаштовано традиційну телефонну лінію. Також, для забезпечення більш комфортних умов роботи, офіс обладнано кондиціонером та LED-світильниками.

Що стосується охорони бізнес-центру, де розташовано офіс компанії, на вході знаходиться охоронець, який контролює доступ до будівлі та який регулярно обходить її територію. Всередині бізнес-центру встановлена система відеоспостереження та сигналізації – коридори та всі офіси облаштовані сповіщувачами, які підключені до пульту охорони. Крім того, вся будівля обладнана системою пожежної сигналізації, що включає в себе пожежні димові та точкові ручні магніконтактні сповіщувачі.

Обчислювальна система компанії складається з 30 робочих місць, кожне з яких має системний блок, монітор, бездротові клавіатуру та мишу – загалом 28

місць активно використовуються, а ще 2 є запасними на випадок несправності компонентів системного блоку чи монітору. Генеральний та фінансовий директори мають по ноутбуку. У серверній кімнаті встановлено сервер, головна роль якого – домен-контролер. На ньому створено акаунти для всіх працівників – всі мають права користувачів, окрім системного адміністратора. У кабінеті для нарад знаходиться ноутбук та проєктор. Серед додаткових робочих засобів також є сканер та 2 принтери. По офісу розташовано 2 комутатори, які забезпечують з'єднання всіх комп'ютерів за допомогою дротових кабелів з мережею, а також маршрутизатор, зв'язок інших приладів з яким є бездротовим. В офісі компанії також передбачено використання зовнішніх носіїв інформації – вони призначені лише для корпоративного користування. Серед таких носіїв є 14 флешок. Кожна з них зареєстрована системним адміністратором та використовує цифровий підпис задля забезпечення автентичності та захисту інформації. Флешки марковані та закріплені за кожним структурним відділом компанії.

Графічне зображення обчислювальної системи можна побачити на рис. 3.

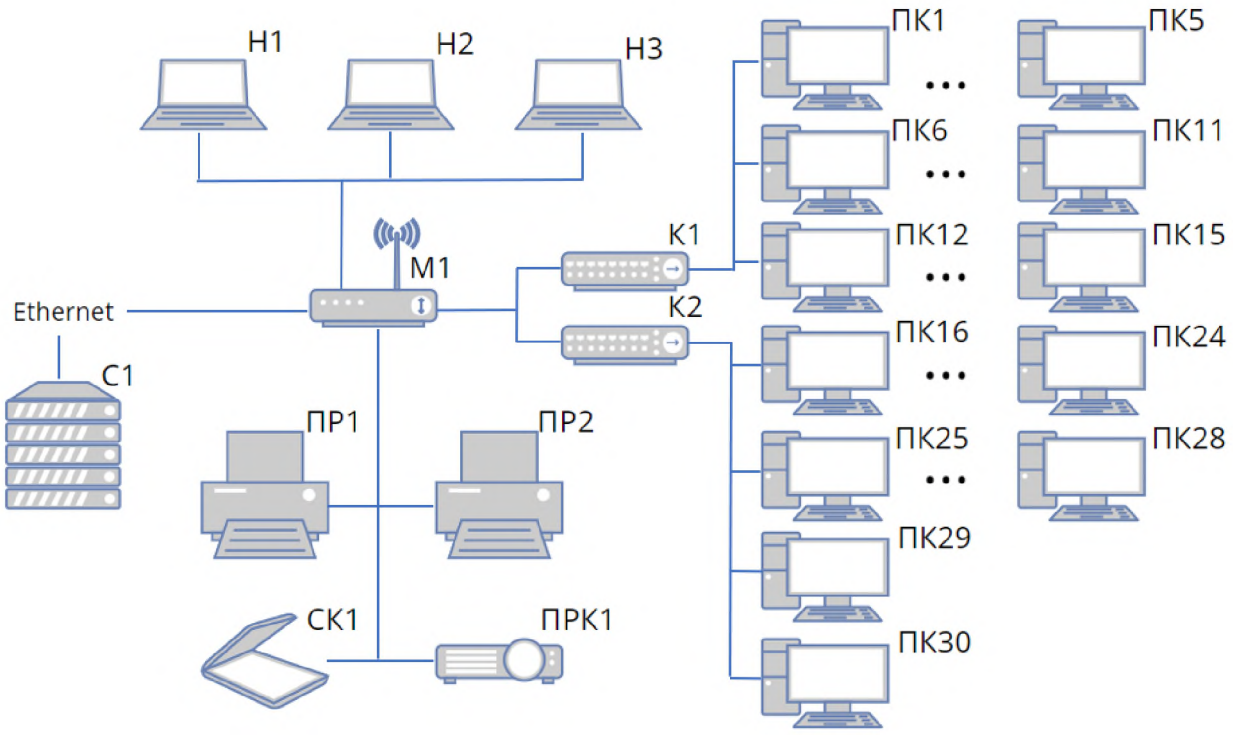

Рисунок 1.3 – Схема ІКС компанії

ПК під номерами від 1 до 5 розташовані у відділі фінансових консультацій. ПК6-ПК11 розташовані у відділі маркетингу. Наступні за номером ПК (від 12 до 15) знаходяться у відділі управління проєктами. ПК16-ПК24 та ПК25-ПК28 встановлені у відділі бухгалтерського обліку та планування податків і відділі адміністративної підтримки відповідно. Резервні ж ПК29 та ПК30 зберігаються у серверній кімнаті. Ноутбуки Н1 та Н2 знаходяться у кабінеті керівництва, а Н3 – у кабінеті для нарад.

Обслуговуванням та адмініструванням обчислювальної системи займається системний адміністратор. Окрім того, ним регулярно оновлюється програмне забезпечення, контролюються права користувачів та відслідковується журнал подій.

Програмне забезпечення, встановлене на робочих місцях, включає Windows 10 Pro, Microsoft Office 365, Google Chrome, Microsoft Edge, M.E.Doc для бухгалтерського обліку, Microsoft Project для управління проєктами, Google Analytics для аналізу даних, Bitdefender GravityZone для забезпечення безпеки комп'ютерної системи, Adobe Acrobat DC для роботи з PDF-документами та Zoom для проведення відеоконференцій. На сервері встановлено операційну систему Windows Server 2019. Більш детальний опис ПЗ можна побачити у табл. 1.1.

Таблиця 1.1 – Програмне забезпечення обчислювальної системи компанії

Назва	Тип ПЗ	Опис	Тип ліцензії	Де встановлено
Windows 10 Pro	Системне	Операційна система для ПК	Client Access License	ПК1-ПК30, Н1-Н3
Windows Server 2019		Серверна операційна система		С1

Продовження таблиці 1.1

Назва	Тип ПЗ	Опис	Тип ліцензії	Де встановлено
Microsoft Office 365	Прикладне	Набір офісних додатків та сервісів	Subscription License	ПК1-ПК30, Н1-Н3
Google Chrome		Браузер	Freeware	
Microsoft Edge				
M.E.Doc		Програма для електронного документообігу	Proprietary License	ПК16-ПК24
Microsoft Project		Програма для управління проєктами	Subscription License	ПК12-ПК15
Google Analytics	Вебсервіс	Інструмент для аналізу вебтрафіку та поведінки користувачів	Freeware	ПК6-ПК11
Bitdefender GravityZone	Прикладне	Антивірусний пакет	Proprietary License	ПК1-ПК30, Н1-Н3
Adobe Acrobat DC		Програма для роботи з PDF-документами	Subscription License	
Zoom		Інструмент для відеоконференцій	Freeware	Н1-Н3

Продовження таблиці 1.1

Назва	Тип ПЗ	Опис	Тип ліцензії	Де встановлено
PeaZip	Прикладне	Архіватор	GNU Lesser General Public License	ПК28

У компанії циркулює відкрита інформація та інформація з обмеженим доступом. Нижче наведено опис цієї інформації.

Контактна інформація підприємства – під цією інформацією мається на увазі фізична адреса офісу компанії, телефонні номери, електронна пошта, вебсайт та посилання на сторінки у соціальних мережах.

Організаційно-розпорядча інформація – ця інформація включає в себе дані, що стосуються внутрішньої організації та управління компанією. Наприклад, інформація про структуру компанії, політики та регламенти компанії, рангову систему працівників, опис робочих процесів та відповідні інструкції для працівників всіх відділів.

Фінансова інформація – під цією інформацією мається на увазі вся фінансова діяльність підприємства, що включає в себе фінансові та податкові звіти, розподіл бюджету, контроль витрат та аналіз фінансових індикаторів.

Юридична інформація – така інформація містить у собі реєстраційний дані, ліцензії та дозволи на надання послуг, документи, що регулюють нерозголошення конфіденційної інформації.

Маркетингова інформація – прикладами такої інформації служать маркетингові стратегії підприємства, аналіз цільових ринків, дані про ефективність рекламних кампанії.

Персональна дані працівників – прикладами даного типу інформації є ПІБ, дата народження, телефонний номер, адреси проживання, посилання на

соціальні мережі, посада, трудовий стаж, резюме, дані про освіту та/або сертифікати пов’язані з підвищення кваліфікації, банківські реквізити.

Персональні дані клієнтів – у цьому пункті дані поділяються на додаткові групи такі як загальні (ПІБ, контактна інформація, дані про структуру компанії, реєстраційні дані), фінансові (доходи та витрати, активи та пасиви, фінансова історія, наявність акцій чи облігацій), податкові (податкові декларації та номери, податкові зобов'язання, історія перевірок), бухгалтерські (інформація про надходження та витрати, банківські виписки, фінансові звіти, враховуючи планування бюджету).

Інформація про підписані угоди – цей вид даних включає в себе всі деталі та документи, пов'язані з укладеними договорами між компанією та її клієнтами, зокрема опис послуг, фінансові та юридичні умови договору, термін їхньої дії.

Інформація про проєкти – ця інформація включає в себе опис проєкту, дані про команду, завдання та етапи їхнього виконання, бюджет, статус поточного стану проєкту, оцінка потенційних проблем та ризиків, пов'язаних з реалізацією проєкту.

Інформація про реалізовану послугу – така інформація має на увазі деталі щодо наданих послуг, включаючи документацію, фінансові та юридичні аспекти, результати та зворотний зв’язок.

Інформація про конкурентів – цей тип інформації містить в собі інформацію про послуги конкурентів, контактні дані, цінову політику конкурентів, рекламні кампанії, аналіз діяльності конкурентів.

До кожної інформація доступ можна отримати різними способами. Здебільшого, дані зберігаються у сховищі OneDrive. Інформація про проєкти ведеться та зберігається у програмі Microsoft Project. Що стосується фінансових звітів компанії та клієнтів, цим займається програмний застосунок M.E.Doc.

Деталі стосовно характеристики інформації можна побачити у табл. 1.2.

Таблиця 1.2 – Характеристика циркулюючої інформації у компанії

Найменування	Рівень доступу	Правовий режим	Вимоги до захисту		
			К	Ц	Д
Контактна інформація підприємства	Відкрита	Відкрита	1	2	3
Організаційно-розпорядча інформація	З обмеженим доступом	Конфіденційна	3	3	2
Фінансова інформація			4	4	3
Юридична інформація			4	3	2
Маркетингова інформація			2	3	2
Персональна дані працівників			4	3	3
Персональні дані клієнтів			4	4	3
Інформація про підписані угоди			4	4	3
Інформація про проєкти			3	3	3
Інформація про реалізовану послугу			3	3	3
Персональна дані працівників			2	2	2

Примітка. Рівні конфіденційності, цілісності та доступності інформації визначені від 1 до 4, де 1 – не має особливих вимог до захисту та не потребує додаткових заходів безпеки, а 4 – вимагає особливого контролю та обмеження, оскільки порушення КЦД такої інформації може мати серйозні наслідки.

Оскільки кожний різновид інформації має специфічні права доступу, варто окремо розглянути розмежування цих прав для кожного з відділів компанії. Даний опис можна побачити у табл. 1.3.

Таблиця 1.3 – Розмежування доступу до інформації

Найменування	Керівництво	Відділ				
		ФК	БОПП	УП	М	АП
Контактна інформація підприємства	RWMDP	R	R	R	RW MP	RW MP
Організаційно-розпорядча інформація	RWMDP	-	-	-	-	RW MP
Фінансова інформація	RWMDP	RP	RW MDP	-	-	-
Юридична інформація	RWMDP	-	RP	-	-	-
Маркетингова інформація	RP	-	-	-	RW MD PS	-
Персональна дані працівників	RWMDP	-	-	-	-	RW MDP
Персональні дані клієнтів	RP	RW MD PS	RW MD PS	-	-	-
Інформація про підписані угоди	RWMDP	RP	-	RWP	-	-
Інформація про проєкти	RWMDP	RP	RP	RW MD PS	RP	-
Інформація про реалізовану послугу	RP	RW MD PS	RWP	-	-	-

Продовження таблиці 1.3

Найменування	Керівництво	Відділ				
		ФК	БОПП	УП	М	АП
Інформація про конкурентів	RP	-	-	-	RW MD PS	-

Примітки:

1 Поясненнями позначень є R – читання, W – запис, M – модифікація, D – видалення, P – друк, S – сканування.

2 Назви відділів компанії у підзаголовку графу скорочено, відповідними названими для кожної абревіатури є ФК – фінансових консультацій, БОПП – бухгалтерського обліку та планування податків, УП – управління проєктами , М – маркетингу, АП – адміністративної підтримки.

3 Відділ АП має деякі уточнення, зокрема системний адміністратор має доступ на читання усієї циркулюючої інформації, а асистенти не мають доступу на модифікацію та видалення доступної для відділу інформації.

Згідно з НД ТЗІ 2.5-005-99 [11] та базуючись на вимогах підприємства до захисту ІКС та конфіденційної інформації, можна стверджувати, що найбільш підходящим профілем захищеності такої АС є 3.КЦД.2. Він вказує на те, що АС відноситься до «3» класу та має підвищені вимоги до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації. Даний профіль захищеності реалізує такі послуги:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2,
ЦД-1, ЦА-2, ЦО-1, ЦВ-2,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Коротке пояснення позначень кожної послуги надано нижче.

Послуги, що відповідають за конфіденційність:

– КД-2 – Базова довірча конфіденційність;

– КА-2 – Базова адміністративна конфіденційність;
– КО-1 – Повторне використання об'єктів;
– КВ-2 – Базова конфіденційність при обміні.

Послуги, що відповідають за цілісність:

– ЦД-1 – Мінімальна довірча цілісність;
– ЦА-2 – Базова адміністративна цілісність;
– ЦО-1 – Обмежений відкат;
– ЦВ-2 – Базова цілісність при обміні.

Послуги, що відповідають за доступність:

– ДР-1 – Квоти;
– ДВ-1 – Ручне відновлення.

Послуги, що відповідають за спостережність:

– НР-2 – Захищений журнал;
– НИ-2 – Одиночна ідентифікація і автентифікація;
– НК-1 – Однонаправлений достовірний канал;
– НО-2 – Розподіл обов'язків адміністраторів;
– НЦ-2 – КЗЗ з гарантованою цілісністю;
– НТ-2 – Самотестування при старті;
– НВ-1 – Автентифікація вузла.

Висновок до першого розділу

У першому розділі даної кваліфікаційної роботи було розглянуто поняття ERP-системи та її класифікації, також було оглянуто актуальність даних систем на основі поточних статистичних даних їхнього використання. Ці дані підтвердили зростання популярності використання бізнесом ERP-систем, особливо північними країнами Європи.

Далі було розглянуто питання безпеки ERP-систем, зокрема їхні типові вразливості, і основні методи підвищення їхньої захищеності, завдяки яким було отримано краще розуміння деяких механізмів захисту від потенційних кібератак.

На останок було ознайомлено з компанією «Фінансовий Консалтинг», де було коротко описано організаційну структуру, інформаційно-комунікаційну

систему, циркулюючу інформацію та розмежування доступу до неї. Такий огляд надав краще розуміння внутрішнього устрою компанії, зокрема було окреслено, що в компанії циркулює достатня кількість конфіденційної інформації, для якої важливо забезпечити основні критерії безпеки. Тому після цього було профіль захищеності

Отже, на основі піднятих питань, у наступному розділі можна приступити до аналізу реалізації послуг обраного профілю захищеності та огляду задовільності потенційних для впровадження у компанію ERP-систем даному профілю та загальним принципам безпеки.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Аналіз послуг профілю захищеності

Оскільки у першому розділі кваліфікаційної роботи було обґрунтовано вибір стандартного профілю захищеності 3.КЦД.2 для ІКС компанії «Фінансовий Консалтинг», то тепер необхідно розглянути чи реалізовані усі послуги даного профілю захищеності завдяки детальному аналізу відповідності зі стандартом НД ТЗІ 2.5-004-99 [12], в якому детально надано опис усіх послуг.

КД-2. Базова довірча конфіденційність. Реалізована. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Прикладом реалізації цієї послуги є можливість користувачів КС у властивостях документів та/або папок, налаштовувати правила доступу до них. Таки чином, керівник відділу маркетингу може налаштувати доступ маркетологів до власної папки, що зберігає звіти проаналізованих даних цільових ринків, а інші користувачі доступу до його папки не матимуть.

КО-1. Повторне використання об'єктів. Реалізована. Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Прикладом реалізації даної послуги є буфер обміну – при виході з акаунту одного користувача і перед входом до акаунту іншого, буфер обміну має бути очищений для того, щоб він міг використовуватись іншим користувачем, та при цьому не порушувалась конфіденційність даних попереднього користувача КС.

КА-2. Базова адміністративна конфіденційність. Реалізована. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати

потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

Приклад реалізації цієї послуги схожий на приклад реалізації послуги КД-2 і відрізняється лише тим, що тепер не звичайний користувач, а саме адміністратор або користувач з правами адміністратора у властивостях документу та/або папки має змогу налаштовувати правила доступу. Також відмінне і те, що якщо у послузі КД-2 користувач міг налаштувати доступ лише до власних папок та файлів, то у даному випадку адміністратор або уповноважена такими правами особа може зробити це відносно будь-яких елементів КС для будь-якого користувача або групи користувачів.

КВ-2. Базова конфіденційність при обміні. Реалізована. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Прикладом реалізації даної послуги служить шифрування даних при передачі у Інтернеті та при передачі через флешку. У першому випадку у збереженні конфіденційності допомагають криптографічні протоколи SSL/TLS, а у другому випадку вирішальну роль відіграє алгоритм шифрування AES-128.

ЦД-1. Мінімальна довірча цілісність. Реалізована. Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Прикладом реалізації цієї послуги служить можливість кожного користувача КС мати певні права на модифікацію даних, тобто податковий консультант може редагувати та вносити корективи у податкові звіти, а фінансовий консультант такого права не має і може лише переглядати дані у таких документах.

ЦА-2. Базова адміністративна цілісність. Не реалізована. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати

потоками інформації від користувачів до захищених об’єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

У адміністратора розглядуваної ІКС є не має можливості розмежувати доступ процесів до об'єктів, наприклад наразі не можна заборонити деякій програмі відкривати та/або модифікувати вказані файли.

ЦО-1. Обмежений відкат. Реалізована. Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об’єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Прикладом реалізації даної послуги є можливість у програмних застосунках відмінити певну кількість виконаних операцій над файлом, зокрема в офісних додатках Microsoft Office 365, ПЗ Adobe Acrobat DC.

ЦВ-2. Базова цілісність при обміні. Ця послуга дозволяє забезпечити захист об’єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Прикладом реалізації даної послуги служить використання хеш-функції при обміні даними через флешку. В такому випадку цілісність забезпечується порівнянням контрольної суми вихідного файлу з контрольної сумою файлу після його передачі. Якщо вони збігаються, то це означає, що файл не було змінено або пошкоджено під час передачі.

ДР-1. Квоти. Реалізована. Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Прикладом реалізації цієї послуги служить можливість адміністратора або іншої уповноваженої особи налаштовувати квоти для користувачів, що будуть фіксувати обсяг даних, які вони можуть займати на дисках C: чи D:.

ДВ-1. Ручне відновлення. Реалізована. Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування.

Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

ДВ-1. Ручне відновлення. Реалізована. Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

Прикладом реалізації даної послуги служить створення образу системи, який можна повторно інсталювати у випадку відмови КС. Створити образ диску можна через функцію «Диск відновлення» у засобах адміністрування ОС Windows.

НР-2. Захищений журнал. Реалізована. Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Прикладом реалізації цієї послуги служить журнал подій, в якому можна перевірити події, що стосуються безпеки системи, роботи застосунків та системи загалом.

НИ-2. Одиночна ідентифікація і автентифікація. Реалізована. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Прикладом реалізації даної послуги є отримання доступу до системи або програмного забезпечення за допомогою унікального для кожного користувача логіну та відповідного йому паролю.

НК-1. Однонаправлений достовірний канал. Реалізована. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Прикладом реалізації цієї послуги служить механізм CAPTCHA у браузері Google Chrome – це використовується для того, щоб сервіс міг запевнитись у тому, що зв'язок зініційовано саме користувачем, тобто реальною людиною.

НО-2. Розподіл обов'язків адміністраторів. Не реалізована. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

У розглядуваної ІКС є лише один адміністратор, тому дана послуга не є реалізованою через невиконання основної умови – обов'язкова наявність системного адміністратора та адміністратора безпеки.

У розглядуваної ІКС є лише один адміністратор, тому дана послуга не є реалізованою через невиконання основної умови – обов'язкова наявність системного адміністратора та адміністратора безпеки.

НЦ-2. КЗЗ з гарантованою цілісністю. Реалізована Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Прикладом є можливість КЗЗ, що включає антивірусне ПЗ Bitdefender GravityZone та вбудований у операційну систему антивірус Microsoft Defender, перевіряти цілісність не тільки не тільки файлів та програм у системі, а й цілісність самого себе.

НТ-2. Самотестування при старті. Реалізована. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Прикладом реалізації цієї послуги служить самоперевірка КС при запуску ПК на цілісність та справність своїх компонентів.

НВ-1: Автентифікація вузла. Реалізована. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і

забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Прикладом реалізації даної послуги є підтвердження ідентичності під час автоматичного оновлення програмного забезпечення – оскільки щоб знайти відповідне оновлення для набору офісних додатків Microsoft Office 365, КЗЗ треба ідентифікувати та автентифікувати місце походження цього ПЗ, тобто офіційного сайту Microsoft.

Для багатьох з послуг потрібна обов'язкова реалізація інших послуг, що не вказані в обраному профілі захищеності, зокрема це послуги НИ-1 та НО-1. Тому варто розглянути їх окремо.

НИ-1. Зовнішня ідентифікація і автентифікація. Реалізована. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Прикладом реалізації цієї послуги служить підключення до робочого столу, що знаходиться на сервері. При вході необхідно зазначити IP-адресу серверу та дані для ідентифікації та автентифікації (логін та пароль).

НО-1. Виділення адміністратора. Реалізована. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Прикладом реалізації цієї послуги є розмежування ролей користувачів у КС, де є один адміністратор та звичайні користувачі.

Серед усіх послуг обраного профілю захищеності, наразі ІКС підприємства не реалізується всього дві послуги – ЦА-2 та НО-2. Для коректного функціонування системи згідно з обраним профілем, необхідно, щоб ці послуги були обов'язково реалізовані. Зробити це можна наступним чином:

Для реалізації послуги ЦА-2 необхідно оновити операційну систему Windows або до 11 версії, або до видання Enterprise. І там, і там є вбудований механізм під назвою Applocker, який дозволяє розмежовувати та контролювати

доступ процесів до об'єктів, та утиліта командного рядка icacls.exe, що дозволяє виконати ті самі дії, що і через Applocker, але ручним способом.

Що стосується послуги НО-2, то її можливо реалізувати за допомогою появи у компанії ще одного адміністратора, проте не системи, а безпеки. Це допоможе розмежувати обов'язки між адміністраторами та запобігти привілейованості поточного єдиного адміністратора, а також таке рішення здатне кращим чином вплинути на захищеність ІКС.

2.2 Критерії оцінки відповідності ERP-систем

Аналіз безпеки ERP-системи є важливою складовою процесу її впровадження у компанію. Без огляду наявних механізмів захисту є ризик несанкціонованого доступу до системи та її даних або навіть витік конфіденційної інформації. Недостатня увага до такого кроку може обернутися порушенням робочого режиму та бізнес-процесів, що, в свою чергу, може спричинити великі матеріальні та нематеріальні збитки для компанії. Тому, задля запобігання негативних наслідків, необхідним є оцінка загального рівня захищеності ERP-системи.

Окрім того, оскільки ІКС підприємства має певні вимоги до захисту, що були визначені профілем захищеності, важливо, щоб обрана ERP-система не тільки гарантувала б гідний рівень безпеки, а й відповідала б та не порушувала б описані у попередньому підрозділі послуги.

Оцінка буде проводитись серед трьох ERP-систем – усі з них є підходящими згідно з процесами та даними, що циркулюють на підприємстві. Також вони задовольняють загальним та фінансовим вимогам компанії, що робить порівняння систем між собою справедливим.

Варто коротко оглянути загальні характеристику цих ERP-систем. Перша система (далі – ERP-1) вироблена у Франції та є локальною. Використовується переважно малими бізнесами з метою налаштування та поліпшення бізнес-процесів. Вона містить різні модулі, що може допомогти краще відокремити доступ користувачів до системи. Друга система (далі – ERP-2) є хмарною розробкою бельгійської компанії та включає в себе базові та просунуті

бухгалтерські та фінансові функції. А третя система (далі – ERP-3) взяла свій початок з Індії, проте стала популярною серед малих підприємств всього світу. Вона, як і попередня система, використовує хмарне рішення. Також вона допомагає легко та просто управляти фінансами та проєктами.

Таким чином, треба сформулювати критерії оцінки безпеки в ERP-системах. Основою для створення критеріїв слугують міжнародні стандарти безпеки, в яких згадується основна концепція безпеки КЦД. Прикладом одного з таких стандартів є ДСТУ ISO/IEC 15408:2023 "Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ" [9, 10] – він охоплює дві серії опису критеріїв оцінювання безпеки в ІТ-продуктах. В першій частині описуються загальні вимоги до безпеки, у тому числі інформуючи про важливість забезпечення КЦД. Друга ж частина, здебільшого, описує методи та підходи для оцінки реалізації функцій безпеки. Разом вони можуть бути використані для повної якісної оцінки безпеки систем або інших технологій.

Ґрунтуючись на згаданому стандарті, можна виокремити такі категорії для критеріїв майбутньої оцінки безпеки ERP-систем: конфіденційність, цілісність, доступність, спостережність. Незважаючи на те, що спостережність не так часто згадується як тріада КЦД, вона все одно відіграє ключову роль у формулюванні загальної безпеки системи. Завдяки спостережності, можливим стає своєчасне виявлення інцидентів безпеки та відновлення після них, а також вона дозволяє проводити аудити, тим самим відстежуючи дії користувачів у системі. Відсутність такого пункту при аналізі захищеності системи може обернутись збільшенням потенційної загрози від внутрішніх та зовнішніх порушників. Що стосується тріади КЦД, то конфіденційність, як відомо, захищає дані від несанкціонованого доступу, цілісність гарантує, що дані залишаються точними та неушкодженими у будь-якому стані, а доступність забезпечує безперебійний доступ до системи та даних у ній.

На основі цих чотирьох категорій, сформульовано критерії, за допомогою яких можна оцінити загальну безпеку розглядуваних ERP-систем. Ці критерії можна побачити на рис. 2.1.

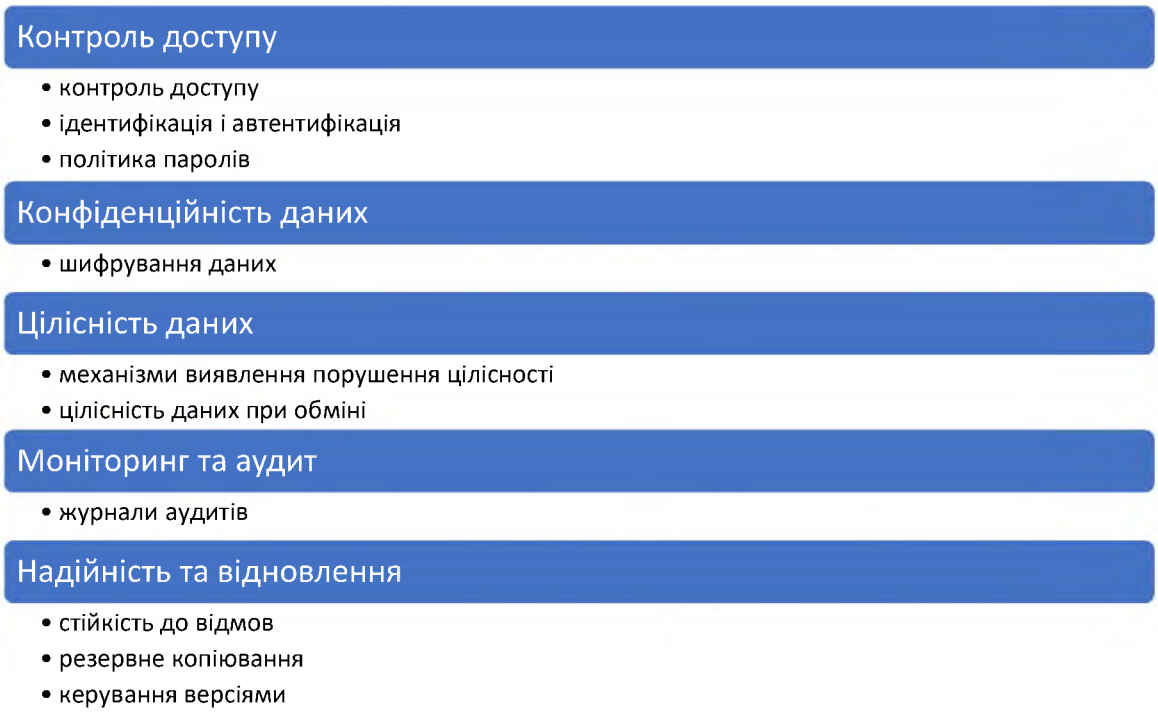

Рисунок 2.1 – Критерії оцінки безпеки у ERP-системах

Варто коротко оглянути кожну категорію та пункт.

Контроль доступу відповідає за захист системи від несанкціонованого доступу. Це включає в себе управління правами доступу користувачів до окремих модулів та функцій системи, ідентифікацію та автентифікацію користувачів, використовуючи логін та пароль, і, безпосередньо, політику паролів, що є окремим відгалуженням від автентифікації. Завдяки даній групі можливо забезпечити конфіденційність, цілісність, доступність та спостережність, а також врахувати ряд послуг профілю захищеності.

Конфіденційність даних гарантує, що циркулююча на підприємстві інформація залишатиметься приватною та невідомою для третіх осіб. Ця категорія включає у себе шифрування даних алгоритмами та їхню відповідність сучасним стандартам безпеки.

Цілісність даних забезпечує достовірність і точність даних незалежно від їхнього стану: чи то зберігання, чи то передача. Достатньо мати механізми виявлення порушення цілісності, що враховує і цілісність даних при обміні – виконання цих критеріїв здатне забезпечити належний рівень цілісності та спостережності.

Моніторинг та аудит дозволяє контролювати активність користувачів у системі. Це забезпечується журналами аудитів. Наявність таких елементів у ERP-системі може поліпшити рівень конфіденційності, цілісності та спостережності.

Надійність та відновлення забезпечують безперервну роботу системи та швидке відновлення навіть у разі технічних збоїв. Це включає у себе стійкість системи до відмов, наявність резервного копіювання та можливість керувати версіями. Комбінація цих механізмів може у певній мірі гарантувати підвищення рівня цілісності, доступності та спостережності.

Реалізація зазначених критеріїв у системах визначається у вигляді коефіцієнту для кожного пункту. Таким чином мінімальна оцінка за окремий критерій є 0, що означає відсутність будь-якої реалізації механізму, а максимальна – 1, що означає ідеальне впровадження механізму захисту. Після аналізу ERP-системи та виставлення оцінки для всіх критеріїв, бали додаються і отримане в результаті число буде вказувати на приблизний рівень захищеності системи.

Отже, оскільки характеристика процесу оцінки надана, можна розпочати огляд кожної з ERP-систем.

2.3 Огляд ERP-1

У налаштуваннях системи наявні механізми обмеження доступу до певних модулів та їхніх функцій. Дана можливість притаманна не лише для окремих користувачів, а і для цілих груп, тобто не потрібно для кожного фінансового консультанта визначати доступ до компонентів системи, а можна додати їх в одну групу, для якої вже визначити окремі правила. Серед наявних функцій у модулях зафіксовані такі базові процедури як читання, запис, створення та видалення записів.

Користувачі ідентифікуються завдяки логіну, а для успішного логування у систему необхідно ввести відповідний пароль – однофакторна автентифікація є стандартною для даної ERP-системи, але альтернативи у вигляді багатофакторної автентифікації вона не пропонує.

За базовими налаштуваннями у системі відсутні особливі вимоги до паролів користувачів, проте адміністратор має повноваження змінити це, встановивши певні правила, яким повинні будуть всі слідувати. Окрім того, адміністратор може налаштувати обов'язкове регулярне оновлення паролю та переглядати історію зміни паролів – це може бути корисним для відслідковування підозрілих дій, оскільки якщо користувач занадто часто змінює паролі, то це може вказувати на атаку зловмисників на акаунт. Єдиним недоліком є те, що усі перераховані функції необхідно самостійно налаштовувати та контролювати.

У ERP-1 є вбудовані механізми виявлення порушення цілісності, зокрема серед них є хешування, проте даний механізм застосовується лише для забезпечення надійного зберігання паролів. Інших механізмів для автоматизованої перевірки цілісності даних у системі не передбачено.

Система має механізм моніторингу безпеки, що включає в себе журнал активності користувачів – там можна побачити коли останній раз відбулась автентифікація користувача, коли був змінений пароль або виконана будь-яка дія стосовно модулів системи.

Дані на хостингу цієї ERP-системи є добре захищеними. Цілісність та конфіденційність даних при обміні забезпечується стандартними протоколами безпеки, такими як TLS 1.2 та TLS 1.3, а зв'язок клієнта з сервером базується на протоколі HTTPS. Інші ж протоколи безпеки можуть бути додані лише через сторонні рішення.

Через свою клієнт-серверну архітектуру ERP-1 є досить стійкою до відмов, оскільки усе навантаження розподіляється рівномірно. Це пов'язано з тим, що ERP-1 зберігає дані у СУБД PostgreSQL, які мають вбудовані механізми відмовостійкості.

Система має базові функції що стосується керування версіями. До неї входить ведення історії дій для всіх модулів, де зберігаються попередні версії даних та документів.

За базовими налаштуваннями резервне копіювання у системі не є автоматизованим процесом, проте адміністратор має змогу налаштувати регулярне створення копій системи через інструменти PostgreSQL.

2.4 Огляд ERP-2

У меню налаштувань є можливість для кожного з користувачів виділити права доступу до модулів та їхніх окремих функцій. Наприклад, можна обрати право доступу до модулю ведення бухгалтерського обліку, і це може бути: бухгалтер, керівник, звичайний користувач або пусте поле, що позначатиме відсутність доступу до даного модулю. Таким чином, можна якісно окреслити видимість модулів та можливості роботи у них згідно з посадами та обов'язками працівників компанії.

Ідентифікація користувачів відбувається завдяки унікальному логіну, для кожного з яких створено відповідний пароль. Проте це не єдиний спосіб автентифікації – також у налаштуваннях системи адміністратор має змогу додати двофакторну автентифікацію, що включає у себе необхідність підтвердження повідомлення на електронній пошті, прив'язаній до акаунту користувача.

За стандартними налаштуваннями лише адміністратор системи може змінити пароль користувачів. Що стосується правил, то у системі відсутні особливі правила створення паролів – єдине правило це довжина паролю від 6 символів, а інші ж вимоги можуть бути за необхідності додані адміністратором.

У модулях системи реалізовано автоматизований механізм перевірки цілісності даних. Його основу створює хеш-функція – у випадку не співпадіння записаних у журнал звітності хешів з фактично порахованими, система позначить перший пошкоджений запис.

ERP-2, як і попередня, також має механізми для моніторингу, враховуючи ведення аудиторських логів. Крім того, для адміністратора присутня можливість налаштування детального моніторингу активності користувачів – ця функція

включає контроль за часом перебування у системі, наприклад про виявлену активність поза робочим часом буде сповіщено адміністратора.

Дані на хостингу цієї ERP-системи також є добре захищеними. Для забезпечення конфіденційності та цілісності даних сервіс використовує TLS 1.2 та протокол HTTPS для безпечного зв'язку між клієнтом та сервером.

Цією системою підтримується автоматизація процесу керування версіями. Таким чином, у кожному відповідному модулі автоматично зберігається історія змін записів або документів.

Стійкість до відмов цієї системи дуже схожа на попередню – обидві мають схожу архітектуру та зберігають дані в СУБД PostgreSQL. Ще однією спільною рисою з ERP-1 є те, що дана система теж має механізм резервного копіювання та відновлення, що пов'язані з використанням однакової СУБД. Проте варто зазначити, що ERP-2 додатково має автоматизований процес створення резервних копій, але він не увімкнений за замовчуванням.

2.5 Огляд ERP-3

У ERP-3 доступ до елементів системи базується на ролевій моделі, тобто для кожного користувача можна призначити фіксовану роль та визначити права доступу до окремих модулів та їхніх функцій. Чудовим доповненням до такого базового механізму є наявність у системі ієрархії користувачів, що допомагає у визначенні доступу окремих користувачів не лише до власних файлів у системі, а і для прив'язаних по ієрархії нижче. Наприклад, при використанні такого механізму, керівник відділу фінансових консультацій зможе переглядати файли та звітності підпорядкованих йому користувачів, тобто фінансових консультантів.

Ідентифікація та автентифікація відбувається традиційним методом – завдяки логіну та паролю. Проте у системі також можливо налаштувати двофакторну автентифікацію, наприклад, додатково до логування потрібно буде ввести код, що прийде на електрону пошту.

Адміністратор має змогу налаштовувати вимоги до паролів, встановлювати та контролювати періодичність його оновлення. За замовчуванням система

вимагає від паролю дотримання таких правил: довжина паролю від 8 символів, комбінація літер та цифр. Цілісність паролів додатково забезпечується хешуванням. Іншого ж вбудованого механізму виявлення порушення цілісності, наприклад цифрового підпису, у системі не передбачено.

Конфіденційність та цілісність передачі даних, як і для двох попередніх систем, забезпечується завдяки протоколам TLS 1.2, TLS 1.3 та HTTPS.

Моніторинг та аудит в ERP-3 реалізовано за допомогою детальних журналів аудиту та доступу. Вони включають інформацію про всі дії користувачів у системі: час виконання дії, логін користувача, тип дії, а також конкретні зміни, внесені в документи.

Система не є настільки стійкою до відмов через особливості використання СУБД – ERP-3 зберігає дані у MariaDB, що може мати деякі проблеми у реплікації даних. Але ця ERP-система має вбудовані механізми для автоматичного резервного копіювання даних, завдяки яким можливе оперативне відновлення доступу до системи. Крім того, вона також підтримує контроль версій файлів та записів, зберігаючи історію їхніх змін та попередніх версій.

2.6 Узагальнення та вибір системи

За розглянутими характеристиками реалізації визначених критеріїв можна підсумувати, що усі три ERP-системи мають багато спільного, зокрема однакові або схожі механізми захисту та контролю. Проте, так само, кожна з систем має і свої сильні та слабкі сторони. Варто розглянути це окремо.

Отже, однаковим для трьох систем є реалізація критеріїв, що стосуються цілісності даних: механізмів виявлення порушення цілісності та механізми цілісності даних при обміні. Також ідентичною є механізм керування версіями, що складається з історії змін записів та файлів. Спільною проблемою для трьох систем є реалізація механізму виявлення порушення цілісності – незважаючи на те, що у даних ERP-системах активно використовується хеш-функція для перевірки цілісності даних, цього може виявитися недостатньо у реаліях таких масштабних систем.

Безперечно сильною стороною ERP-1 є політика паролів – вона забезпечує високий рівень захисту акаунтів користувачів та системи загалом завдяки існуючим можливостям налаштувань. А однією з вагомих слабкостей системи можна назвати резервне копіювання. Відсутність такої вбудованої функції є значною вразливістю при подальшій роботі, оскільки у випадку збоїв системи або серверу робочий процес може застоюватись, а також існує загроза порушення доступності інформації.

Сильна сторона для ERP-2 та ERP-3 є однаковою – це реалізація ідентифікації та автентифікації користувачів. Через наявність двофакторної автентифікації та налагодженого базового механізму ідентифікації ці системи можуть гарантувати високий рівень безпеки у системі, оскільки більшість загроз беруть свій початок саме від проблем з реалізацією цього критерію.

Слабкості ж для цих двох систем різні. ERP-2 має деякі проблеми з налаштуванням політики паролів та шифруванням даних. Оскільки у системі відсутня можливість зміни паролів, власне, звичайними користувачами, це може призвести до неприємних наслідків. По-перше, такий підхід не є досить доречним, оскільки у разі втрати доступу до акаунту необхідно буде тривожити адміністратора системи, і чим більша компанія, тим гострішою буде ця проблема. По-друге, варто враховувати, що компанія може містити внутрішніх порушників, серед яких може опинитись і системний адміністратор. Стосовно ж шифрування, проблема закладається у тому, що серед протоколів шифрування ERP-2 використовує лише протокол TLS 1.2. У порівнянні з протоколом TLS 1.3, він є менш безпечним, оскільки має в своїй основі застарілі алгоритми, такі як MD5 і SHA-1. У той самий час TLS 1.3 використовує для шифрування алгоритми AES з різною довжиною ключів. Натомість ERP-3 не має таких проблем – вона має вразливість у вигляді зниженого, у порівнянні з іншими двома системами, рівня забезпечення відмовостійкості. Насамперед, це пояснюється особливістю СУБД MariaDB. MariaDB підтримує асинхронну і напівсинхронну реплікації, PostgreSQL, яка використовується ERP-1 та ERP-2, – асинхронну та синхронну реплікації. Різниця між цими типами реплікацій полягає у процесі копіювання

даних: при асинхронній реплікації основний сервер не чекає підтвердження успішності завершення даного процесу, а при синхронній реплікації – це є обов'язковим. Таким чином, відсутність реалізації синхронної реплікації у СУБД PostgreSQL впливає на стійкість до відмов у ERP-3.

Після окремого більш детального розгляду сильних та слабких сторін кожної з розглядуваних систем, можна перейти до оцінки їхньої відповідності з сформульованими раніше критеріями. Дана оцінка наведена у табл. 2.1.

Таблиця 2.1 – Оцінка ERP-систем відповідності сформульованим критеріям

Назва критерію	ERP-1	ERP-2	ERP-3
Контроль доступу	0,8	0,7	0,8
Ідентифікація і автентифікація	0,6	0,9	0,9
Політика паролів	0,8	0,6	0,7
Шифрування даних	0,8	0,6	0,8
Механізми виявлення порушення цілісності	0,5	0,5	0,5
Цілісність даних при обміні	0,8	0,8	0,8
Журнали аудитів	0,7	0,8	0,8
Стійкість до відмов	0,7	0,7	0,5
Резервне копіювання	0,5	0,7	0,7
Керування версіями	0,8	0,8	0,8

Підрахуючи виставлені бали, можна побачити, що ERP-1 набрала 7 балів, ERP-2 – 7,1 балів, а ERP-3 – 7,3 бали. Дані показники свідчать про те, рівень захищеності даних ERP-систем є приблизно однаковим.

Коротке пояснення визначених балів наведено нижче.

У трьох системах однаково реалізований механізм розмежування доступу користувачам на основі їхніх ролей, проте дещо вищі бали для ERP-1 та ERP-3 стоять у зв'язку з наявністю додаткових компонентів, зокрема наявність груп та

ієрархії відповідно. В умовах зростання та розширення компанії розмежування лише на основі ролей може бути завузьким.

Ідентифікація та автентифікація, як вже зазначалось вище, краще реалізовані у ERP-2 та ERP-3 завдяки наявності двофакторної автентифікації.

Політика паролів у деяких моментах для трьох систем є схожою, зокрема у визначенні адміністратором правил та вимог до паролів. Оскільки ERP-1 має розширені можливості щодо управління та налаштування паролів, а ERP-3 має початкові вимоги до паролів більш сильні ніж у ERP-2, оцінка градується відповідним чином.

Критерій шифрування даних було розібрано вище, проте також варто зазначити, що для ERP-1 та ERP-3 не стоїть найвищий показник, тобто 1, навіть незважаючи на використання протоколу TLS 1.3 – це пов'язано з захистом даних лише при передачі, тобто у стані спокою дані ніяк не шифруються, хоча в системах є відповідні можливості для реалізації такої функції.

Механізм виявлення порушення цілісності для усіх систем є найнижчою оцінкою, і здебільшого причиною цього є наявність лише хешування, причому тільки для паролів. Відсутній цифровий підпис документів, що активно циркулюють в підприємстві, та захист цілісності інших даних. Саме тому виставлена оцінка для всіх систем є справедливою.

Дані під час передачі є захищеними у випадку усіх розглядуваних систем, і у цьому значно допомагає протокол передачі даних HTTPS.

Оцінку реалізації критерію журналів аудиту можна обґрунтувати тим, що ERP-2 та ERP-3 мають більш розширені можливість контролю за діями у системі, що також дозволяє якісніше слідкувати за станом безпеки у системі.

Враховуючи описані вище особливості СУБД, що використовуються ERP-системами для зберігання даних, та процесу резервного копіювання, зазначені для них оцінки також є об'єктивними.

Що стосується останнього критерію – керування версіями, то у кожній системі є вбудовані автоматизовані механізми для цього процесу, зокрема

можливість відкату до попередніх версій документів або записів у системах. Цього достатньо для забезпечення належного рівня цілісності.

Таким чином, ERP-3 – система, що має найвищий рівень безпеки у порівнянні з двома іншими та може бути розглянута для впровадження у компанію. Крім того, вона відповідає обраному профілю захищеності ІКС підприємства, оскільки єдину послугу, що вимагає власної обов'язкової реалізації у всіх компонентах КС, вона влучно реалізує. Це послуга КО-1, і повторне використання об'єктів ERP-система реалізує завдяки автоматичному очищенню тимчасових файлів та даних після завершення сесії окремого користувача.

Це все робить ERP-3 гідним варіантом для впровадження у компанію, оскільки така система допоможе не тільки підвищенню якості надання послуг та оптимізації бізнес-процесів, а і забезпечить належний рівень захищеності циркулюючої інформації.

2.7 Розробка політики безпеки

У розробленій політиці безпеці запропоновані ключові пункти забезпечення захищеності ERP-системи, зокрема це включає в себе опис загальних положень, визначення обов'язків користувачів та адміністраторів системи, захист даних, згідно з сформульованими раніше критеріями оцінки безпеки у ERP-системі, опис реагування на інциденти безпеки, план відновлення системи у разі відмов або атак, пункти щодо регулярності перегляду цієї політики безпеки.

У загальних положеннях наведено підпункт «Визначення термінів», які описані згідно з НД ТЗІ 1.1-003-99 [13].

1. Загальні положення

1.1. Мета політики:

Метою цієї політики є забезпечення безпечного та ефективного використання ERP-системи у робочих процесах. Політика встановлює основні положення і вимоги, які повинні дотримуватись усіма співробітниками під час взаємодії з ERP-системою. Основні аспекти політики безпеки включають:

– забезпечення конфіденційності, цілісності та доступності даних у ERP-системі;

– мінімізацію ризиків інформаційних загроз і вразливостей, пов'язаних з використанням ERP-системи;

– забезпечення відповідності до внутрішніх і зовнішніх стандартів безпеки даних і обробки інформації;

– підвищення обізнаності та відповідальності співробітників у питаннях безпеки.

1.2. Область застосування:

Ця політика стосується всіх аспектів використання ERP-системи і охоплює всі бізнес-процеси, де використання ERP-системи є ключовим елементом, зокрема це управління фінансовою діяльністю, управління відносинами з клієнтами, управління проєктами, управління персоналом. Політика безпеки поширюється на всіх співробітників компанії «Фінансовий Консалтинг».

1.3. Визначення термінів:

Автентифікація – це процедура перевірки відповідності пред’явленого ідентифікатора об’єкта ERP-системи на предмет належності його цьому об’єкту; встановлення або підтвердження автентичності.

Авторизація – це надання повноважень; встановлення відповідності між повідомленням (пасивним об’єктом) і його джерелом (створившим його користувачем або процесом).

Адміністратор – користувач, роль якого включає функції керування ERP-системою.

Адміністратор безпеки – адміністратор, відповідальний за дотримання створеної політики безпеки.

Атака – спроба реалізації загрози.

Безпека інформації – це стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Вразливість ERP-системи – нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації та/або нанесення збитків компанії.

Ідентифікація – це процедура присвоєння ідентифікатора об'єкту ERP-системи або встановлення відповідності між об'єктом і його ідентифікатором; впізнання.

Інцидент кібербезпеки – подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої атаки, які становлять загрозу безпеці ERP-системи.

Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Користувач – фізична особа, яка може взаємодіяти з ERP-системою через наданий їй інтерфейс.

Ризик – це функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

2. Ролі та обов'язки

2.1. Користувач ERP-системи зобов'язаний:

– дотримуватись внутрішніх політик безпеки компанії щодо використання ERP-системи;

– використовувати функціонал ERP-системи тільки для бізнес-процесів компанії і уникати особистого використання;

– зберігати конфіденційну інформацію, що збирається і оброблюється в ERP-системі, відповідно до внутрішніх політик компанії;

– забезпечувати точність інформації, що вводиться в ERP-систему, задля уникнення помилок і непорозумінь у роботі з іншими відділами компанії;

– перевіряти інформацію перед виконанням транзакцій або змінами в ERP-системі;

– вчасно здійснювати записи та оновлення даних в ERP-системі;

– використовувати лише авторизовані програмні інструменти для доступу до ERP-системи;

– виконувати інструкції адміністратора щодо регулярного оновлення паролів та інших заходів безпеки;

– повідомляти адміністратора про будь-які технічні або функціональні проблеми, виявлені в ERP-системі.

2.2. Адміністратор ERP-системи зобов'язаний:

– налаштовувати і підтримувати працездатність ERP-системи;

– вирішувати технічні проблеми, які виникають в процесі експлуатації ERP-системи;

– налаштовувати права доступу користувачів до модулів ERP-системи відповідно до їхніх ролей та обов'язків в компанії;

– встановлювати і оновлювати програмне забезпечення ERP-системи, забезпечуючи сумісність із зовнішніми та внутрішніми інтеграціями;

– відслідковувати та аналізувати продуктивність ERP-системи;

– проводити тестування окремих функцій і компонентів ERP-системи;

– забезпечувати резервне копіювання даних;

– надавати підтримку користувачам щодо налаштування і функціонування ERP-системи;

– організовувати і проводити тренінги для співробітників компанії з питань оптимального використання системи.

2.3. Адміністратор безпеки зобов'язаний:

– розробляти, впроваджувати і підтримувати політику інформаційної безпеки компанії, спеціально налаштовану для ERP-системи;

– проводити регулярні аудити безпеки ERP-системи, виявляти слабкі місця і розробляти плани їх усунення;

– відслідковувати та фіксувати безпекові події, що стосуються ERP-системи;

– реагувати на інциденти безпеки та проводити відновлення після інцидентів в ERP-системі;

– надавати консультації користувачам і системному адміністратору щодо політики безпеки використання ERP-системи;

– організовувати навчання з питань інформаційної безпеки для персоналу, що працює з ERP-системою.

3. Контроль доступу

3.1. Визначення прав і ролей

Кожному користувачу ERP-системи призначається певна роль, яка відповідає його посадовим обов'язкам і рівню доступу до даних та функцій системи. На основі ролей визначається доступ до окремих модулів ERP-системи.

У ERP-системі повинна бути зазначена ієрархія користувачів та визначений доступ до даних та документів підпорядкованих співробітників

Права доступу повинні переглядатись адміністратором системи щонайменше раз на півроку та/або після кожної зміни в організаційній структурі організації.

3.2. Автентифікація

Кожний користувач ERP-системи має власний обліковий запис, доступ до якого можна отримати за допомогою унікального логіну та відповідного йому паролю. Використання спільних облікових записів не передбачено.

Адміністратором системи повинна бути забезпечена двофакторна автентифікація.

Для успішного логування у систему користувачу потрібно ввести коректні дані від свого облікового запису (логін та пароль) та надати код, надісланий на корпоративну пошту, що прив'язана до облікового запису.

При втраті паролю його можливо відновити через корпоративну пошту або звернувшись до адміністратора системи.

У випадку невдалої спроби входу деякого користувача адміністратор ERP-системи сповіщається про це системою. Якщо кількість невдалих спроб входу

перевищує 5 разів, то обліковий запис автоматично блокується. Розблокувати обліковий запис може лише адміністратор.

3.3. Політика паролів

Паролі, що використовуються при вході у ERP-систему повинні складатись щонайменше з 8 символів і містити латинські літери у верхньому та нижньому регістрах, цифри та спеціальні символи.

Паролі обов'язково повинні бути змінені користувачами щонайменше кожні 90 днів. Про необхідність це зробити сповіщає адміністратор системи. Без відповідної команди не рекомендується самостійно змінювати пароль.

Також не рекомендується повторно використовувати паролі. Виключенням є використання минулого паролю 180 або більше днів тому.

3.4. Журнали аудиту та логування

Усі дії користувачів в ERP-системі записуються у журнали. Це включає входи в систему, зміни записів у модулях системи, доступ до особистих даних клієнтів, дії над документами, тощо.

Журнали регулярно повинні переглядатись адміністратором системи для виявлення підозрілої активності та можливих інцидентів безпеки.

Журнали з ERP-системи повинні зберігатись у окремому хмарному сховищі протягом одного року та обов'язково повинні мати щонайменше дві копії, збережені на інших хмарних сервісах або фізично у офісі.

4. Захист даних

4.1. Механізми забезпечення конфіденційності та цілісності даних

Дані, що зберігаються у ERP-системі, повинні додатково шифруватись за допомогою алгоритму шифрування AES-256, AES-192 або AES-128.

Для передачі та обміну даними використовуються захищені протоколи HTTPS та TLS.

Обходити та/або відключати механізми забезпечення конфіденційності та цілісності даних заборонено. Користувачі, які намагаються обійти або відключити такі механізми, можуть бути притягнуті до дисциплінарної

відповідальності, включаючи можливе звільнення та притягнення до юридичної відповідальності відповідно до діючого законодавства України.

4.2. Механізми виявлення порушення цілісності даних

У ERP-системі присутній автоматизований механізм перевірки порушення цілісності даних – хеш-функція. Будь-які зміни в даних виявляються шляхом порівняння хеш-значень початкового та поточного записів.

Рекомендується інтегрувати ERP-систему з іншим механізмом перевірки порушення цілісності даних – цифровим підписом. Такий механізм найбільш доречно використовувати для забезпечення цілісності документів та інфших файлів. Його можна використовувати окремо або у комбінації з хеш-функцією.

У випадку виявлення порушення цілісності записів та/або документів користувач повинен негайно повідомити про це адміністратора системи або безпеки. Відкривати документи та використовувати у робочих процесах пошкоджені записи заборонено.

5. Реагування на інциденти безпеки

5.1. Виявлення інцидентів

Адміністраторами системи та безпеки регулярно аналізуються журнали аудиту та логування. Виявлені аномалії та підозрілі дії повинні бути негайно досліджені для визначення їхньої причини та потенційних загроз для системи.

При виявлені підозрілих дій користувачем системи він негайно повинен сповістити про це адміністратора системи або безпеки.

Для автоматизації процесу виявлення інцидентів безпеки рекомендується інтеграція ERP-система з програмним забезпеченням у вигляді системи виявлення вторгнень.

5.2. Реагування на інциденти

При реагуванні на інциденти безпеки адміністратори повинні дотримуватись розроблених планів та діяти швидко.

У разі підтвердження підозрілих дій, адміністратори системи та безпеки повинні оперативно вжити відповідних заходів, таких як ізоляція окремого користувача або ураженої системи в цілому, заміна паролів.

Всі дії та рішення, прийняті під час реагування на виявлений інцидент безпеки, повинні бути задокументовані для подальшого покращення політики безпеки.

5.3. Повідомлення про інциденти

Після реагування на інцидент безпеки адміністратор безпеки повинен негайно повідомити про дану проблему керівників компанії.

У разі необхідності також необхідно сповістити регуляторні органи та постраждалих сторін про інцидент відповідно до вимог законодавства України.

6. Відновлення системи

6.1. Стійкість системи до відмов

Для підвищення стійкості системи для відмов рекомендується впровадити додаткові механізми для забезпечення безперебійної роботи ERP-системи, такі як резервні сервери.

У такому випадку адміністратори повинні налаштувати автоматичне переключення на резервні сервери у випадку відмови основних.

Крім того, варто розглянути використання кластеризації серверів для розподілу навантаження та підвищення доступності ERP-системи.

6.2. Резервне копіювання даних

Адміністратор системи повинен щотижня створювати резервні копій даних та щомісяця – резервні копії системи.

Зберігати резервні копії необхідно у окремому хмарному сховищі для захисту від фізичних загроз у декількох екземплярах, щонайменше у 5, які повинні знаходитись на декількох різних сервісах. Фізичне зберігання резервних копії заборонено.

6.3. Відновлення даних

Адміністратор системи повинен розробити та регулярно тестувати процедури відновлення даних та системи для забезпечення швидкого відновлення роботи ERP-системи у разі збоїв та/або атак.

Це включає створення та підтримку актуальних резервних копій, проведення регулярних навчань та симуляцій для перевірки готовності персоналу до потенційного відновлення ERP-системи або її окремих даних.

Адміністратор системи також повинен забезпечити документування всіх процедур відновлення та їх регулярне оновлення відповідно до змін в інфраструктурі та вимог безпеки.

7. Навчання персоналу

Усі нові співробітники повинні проходити початковий курс з основ інформаційної безпеки та безпечного використання ERP-системи. Це навчання має охоплювати правила створення та зберігання паролів, розпізнавання фішингових атак, безпечну роботу з корпоративними даними та знайомство з політикою доступу до системи.

Для підтримання високого рівня обізнаності всі співробітники повинні регулярно проходити тренінги з інформаційної безпеки. Ці тренінги повинні бути організовані адміністратором безпеки та включати регулярні семінари стосовно забезпечення безпечної роботи у ERP-системі.

Адміністратор системи та адміністратор безпеки повинні регулярно проходити спеціалізоване навчання для покращення власної обізнаності та кваліфікації.

8. Перегляд та оновлення політики

Перегляд політики безпеки використання ERP-системи у компанії повинен проводитись раз на рік або після кожного виявленого інциденту безпеки. За перегляд та оновлення політики безпеки відповідальний адміністратор безпеки.

Крім того, у політиці безпеці повинні враховуватись усі зміни згідно з діючим законодавством України щодо захисту інформацію в інформаційно-комунікаційних системах.

Після впровадження політики безпеки використання ERP-системи обов'язковим є ведення детальної документації та звітності стосовно поточного стану захищеності ERP-системи та процесу виконання даної політики усіма відділами компанії.

Висновок до другого розділу

У другому розділі даної кваліфікаційної роботи було проаналізовано реалізації послуг обраного у першому розділі профілю захищеності ІКС компанії, в результаті чого було виявлено, що у системі не реалізуються дві послуги, такі як ЦА-2 та НО-2. Тому задля забезпечення повної відповідності профілю було запропоновано методи реалізації цих послуг, які рекомендується впровадити у компанії.

Далі було сформульовано критерії оцінки безпеки відповідних потребам компанії ERP-систем. За результатами оцінки кожної з трьох ERP-системи було виявлено, що їхній рівень захищеності є приблизно однаковим, проте все одно на високому рівні. Даний показник свідчить про те, що постачальники ERP-систем дійсно надають високий рівень безпеки, що може гарантувати надійність виконання основних критеріїв безпеки КДЦС в ІКС компанії.

На останок було розроблено основні положення політики безпеки інформації при використанні обраної ERP-системи, що включає у себе інформацію про обов'язки користувачів та адміністраторів системи та безпеки, ключові пункти забезпечення захисту даних та системи загалом.

Проте відкритим залишається питання економічної доцільності розробки політики безпеки та впровадження ERP-рішення в цілому, тому ці аспекти варто розглянути у наступному розділі.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування витрат на реалізацію політики безпеки

Незважаючи на те, що політика безпеки здатна надати гідний рівень захисту системи компанії або її окремих елементів, важливим чинником також є економічна доцільність її розробки, оскільки, не врахувавши цей фактор, є ризик великих фінансових витрат для компанії, які навіть можуть не виправдати себе.

Тому метою виконання економічного розділу є визначення доцільності впровадження ERP-системи в компанію та обґрунтування ефективності розробки системної політики безпеки при використанні цієї ERP-системи.

У цьому допоможе:

1. Розрахунок капітальних витрат на розробку політики безпеки та її інтеграції у існуючу систему підприємства.
2. Розрахунок річних експлуатаційних витрат на керування ІКС підприємства, враховуючи впровадження ERP-системи.
3. Визначення річного економічного ефекту, враховуючи імовірність атак при використанні впровадженої ERP-системи.
4. Визначення та аналіз показників економічної ефективності, що включає коефіцієнт повернення інвестицій та загальний термін окупності.

3.2 Розрахунок (фіксованих) капітальних витрат

Однією з капітальних витрат на розробку політики безпеки є визначення трудомісткості її розробки. Вона визначається тривалістю кожної робочої операції, починаючи зі складання технічного завдання та закінчуючи оформленням документації. Приклад розрахунку наведено у формулі (3.1).

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}}, \text{ годин} \qquad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку політики безпеки інформації, годин;

$t_в$ – тривалість розробки концепції безпеки інформації у організації, годин;

$t_а$ – тривалість процесу аналізу ризиків, годин;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту, годин;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації, годин;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення безпеки інформації, годин;

$t_д$ – тривалість документального оформлення політики безпеки, годин.

Згідно з цією формулою, отримаємо такий результат:

$$t = 5 + 10 + 15 + 10 + 8 + 12 + 6 = 66 \text{ годин}$$

Ще однією складовою капітальних витрат є витрати на, власне, розробку політики інформаційної безпеки, що визначається формулою (3.2).

$$К_{рп} = З_{зп} + З_{мч}, \text{ грн} \quad (3.2)$$

де $З_{зп}$ – витрати на заробітну плату спеціаліста з інформаційної безпеки, грн;

$З_{мч}$ – витрати машинного часу, що необхідний для розробки політики безпеки, грн.

При чому $З_{зп}$ та $З_{мч}$ можна розрахувати за формулами (3.3) та (3.4) відповідно.

$$З_{зп} = t \cdot З_{іб}, \text{ грн} \quad (3.3)$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Середньогодинна заробітна плата спеціаліста з інформаційної безпеки з практичним досвідом роботи від 2 до 3 років, згідно з даними DOU [14], становить приблизно 270 гривень.

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

де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн/годину.

Для $С_{мч}$ також є окрема формула розрахунку (3.5), яку варто оглянути перш ніж робити розрахунки:

$$С_{мч} = Р \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p}, \text{ грн} \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість машин, на яких розроблюється політика безпеки;

$С_е$ – тариф на електричну енергію, грн/кВт · годину;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

F_p – річний фонд робочого часу, годин;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці, частки одиниці.

За характеристиками виробника, початкова потужність ПК, встановлених у офісі, дорівнює 400 Вт. Від придбання ПК, на якому розробляється політика безпеки, до поточного моменту пройшло два роки, що свідчить про незначне зниження потужності пристрою до 350 Вт через регулярне використання у процесі роботи.

Політика безпеки розроблюється лише на одному ПК.

Поточний тариф на електричну енергію в Україні становить 4,32 грн/кВт · годину.

Враховуючи знос ПК за два роки, його поточну вартість можна оцінити у 20 тисяч гривень. Спираючись на орієнтовний корисний строк служби ПК, що можна оцінити у 5 років, річна норма його амортизації становить приблизно 0,2 частки одиниці.

Програмне забезпечення слугує довше апаратних компонентів – приблизно 8 років, тому річна норма амортизації на ліцензійне програмне забезпечення, відповідно, складає 0,125 частки одиниці.

У середньому, в місяць компанія має 21 робочих день за 8-годинним графіком роботи, тобто річний фонд робочого часу становить 2016 годин.

У таблиці 3.1 наведено ціни ліцензійного програмного забезпечення, загальна вартість якого, згідно підрахункам, складає 19,8 тисяч гривень.

Таблиця 3.1 – Вартість ліцензійного програмного забезпечення у компанії

Назва	Ціна за 1 користувача, грн
Windows 10 Pro	5000
Microsoft Office 365	3000
M.E.Doc	3000
Microsoft Project	3500
Bitdefender GravityZone	800
Adobe Acrobat DC	4500

Отже тепер можна повноцінно порахувати усі необхідні елементи для визначення $К_{рп}$:

$$С_{мч} = 0{,}35 \cdot 1 \cdot 4{,}32 + \frac{20000 \cdot 0{,}2}{2016} + \frac{19800 \cdot 0{,}125}{2016} = 4{,}72 \text{ грн}$$

$$З_{мч} = 66 \cdot 4{,}72 = 311{,}52 \text{ грн}$$

$$З_{зп} = 66 \cdot 270 = 17820 \text{ грн}$$

$$К_{рп} = 311,52 + 17820 = 18131,52 \text{ грн}$$

Таким чином, розробка політики інформаційної безпеки може досягати вартості у 18 тисяч гривень. Проте додатково слід порахувати загальну суму капітальних (фіксованих) витрат, що включатимуть вартість розробки політики безпеки, її впровадження та витрати на встановлення на налагодження обраної ERP-системи. У цьому допоможе формула (3.6).

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{навч} + К_{н}, \text{ тис. грн} \quad (3.6)$$

де $К_{пр}$ – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного та додаткового програмного забезпечення, тис. грн;

$К_{рп}$ – вартість розробки політики безпеки, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Варто трохи детальніше оглянути кожний компонент загальної суми капітальних витрат.

До вартості розробки проєкту інформаційної безпеки входить залучення зовнішніх консультантів – представників компанії-постачальника ERP-системи. Згідно з інформацією на їхньому сайті, вартість години консультації з ними коштує приблизно 100 доларів США. Достатньо буде консультації на 2 години, тому вартість розробки проєкту складе 8 тисяч гривень.

До вартості закупівель ліцензійного програмного забезпечення входить придбання підписки на використання ERP-системи (50 доларів США на місяць), оновлення операційної системи до версії Enterprise (5000 гривень за ліцензію для одного користувача) та додаткові налаштування інтеграції ERP-системи з іншим

програмним забезпеченням (до 1000 гривень), що загалом складе 190 тисяч гривень.

Вартість розробки політики безпеки розрахована вище за формулою (3.2) і становить трохи більше ніж 18 тисяч гривень.

Витрати на навчання включають в себе проведення тренінгів серед усіх співробітників, що стосується безпечного та ефективного використання ERP-системи, та додаткове навчання для адміністратора стосовно управління та адміністрування системи. Всього треба провести 3 тренінги групою по 10 чоловік у кожній, і витрати на кожний такий тренінг сягнуть 15 тисяч гривень. Навчання адміністратора може зайняти один робочий день, а згідно з ціновою політикою, вказаною компанією-постачальником, це коштуватиме 30 тисяч гривень.

Витрати на встановлення обладнання та налагодження системи, здебільшого, стосуються імовірного додаткового налаштування серверу та мережі у офісі, тому можуть досягти суми у 5 тисяч гривень.

Таким чином, можна розрахувати загальні капітальні витрати:

$$К = 8 + 190 + 18{,}132 + 75 + 5 = 296{,}132 \text{ тис. грн}$$

Отже, капітальні (фіксовані) витрати на підприємстві «Фінансовий Консалтинг» складають близько 296 тисяч гривень.

3.3 Розрахунок поточних (експлуатаційних) витрат

Річні поточні (експлуатаційні) витрати на функціонування ERP-системи з урахуванням введення розробленою політики безпеки можна порахувати за формулою (3.7).

$$С_к = С_н + С_а + С_з + С_{єв} + С_е, \text{ грн} \quad (3.7)$$

де $С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів, грн;

$С_а$ – річний фонд амортизаційних відрахувань, грн;

$С_з$ – річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує ERP-систему, грн;

$С_{єв}$ – єдиний внесок на загальнообов'язкове державне соціальне страхування, грн;

$С_е$ – вартість електроенергії, що споживається апаратурою, що використовує ERP-систему протягом року, грн.

Деякі з компонентів C, зокрема $С_з$ та $С_е$, вираховуються за допомогою додаткових формул – (3.8) та (3.9) відповідно.

$$С_з = З_{осн} + З_{дод}, \text{ грн} \quad (3.8)$$

де $З_{осн}$ – основна заробітна плата, грн;

$З_{дод}$ – додаткова заробітна плата, що зазвичай становить близько 10% від основного доходу, грн.

$$С_е = Р \cdot F_р \cdot Ц_е, \text{ грн} \quad (3.9)$$

де Р – встановлена потужність апаратури, що використовує ERP-систему, кВт;

$F_р$ – річний фонд робочого часу ERP-системи, годин;

$Ц_е$ – тариф на електроенергію, грн/кВт · годин.

Розглянемо кожну складову розрахунку річних поточних витрат.

Витрати на навчання адміністративного персоналу та кінцевих користувачів можна оцінити у 195 тисяч гривень. Це зумовлено необхідністю щоквартального проведення тренінгів (також групами по 10 чоловік) та додатковим навчанням системного адміністратора на курсах у провідних IT-компаніях, вартістю у 15 тисяч гривень.

Річний фонд амортизаційних відрахувань можна порахувати, враховуючи, що з усього апаратного забезпечення два ПК придбано півроку тому, п'ять ПК придбано рік тому, вісім ПК придбано 2 роки тому, п'ятнадцять ПК придбано 3

роки тому, два ноутбуки придбано 2 роки тому, один ноутбук придбано 1 тому, сервер, два комутатори та маршрутизатор придбано 3 роки тому, один принтер та один сканер придбано 3 роки тому, один принтер придбано 1 рік тому, проектор придбано 2 роки тому, а більшість меблів служать вже майже 9 років, а офісна техніка, здебільшого, – 4 роки. В офісі встановлено стандартні меблі та техніку: робочі місця (стіл та крісло), середнього розміру комоди та маленькі полички, стіл для нарад та стільці, дивани та м'які місця, чайник, холодильник, мікрохвильова піч. Їхня загальна сума, враховуючи термін використання, становить 300 тисяч гривень. На основі цих даних можна визначити річний фонд амортизаційних відрахувань у порядку перерахування компонентів, помноженим на річну норму амортизації для кожної окремої категорії:

$$C_а = (2 \cdot 28000 + 5 \cdot 24000 + 8 \cdot 20000 + 15 \cdot 18000 + 2 \cdot 16000 + 14000) \cdot 0{,}2 + (35000 + 2 \cdot 4000 + 9000) \cdot 0{,}35 + (8000 + 3000 + 10000 + 30000) \cdot 0{,}15 + 300000 \cdot 0{,}1 = 186250 \text{ грн}$$

Річний фонд заробітної плати персоналу, обслуговуючому ERP-систему, тобто системному адміністратору становить:

$$C_з = (20000 + 2000) \cdot 12 = 264000 \text{ грн}$$

Єдиний внесок на загальнообов'язкове державне соціальне страхування можна розрахувати помноживши загальну суму заробітних плат співробітників компанії на суму соціального та медичного страхування, які на поточний момент складають 5,1% від заробітної плати. Стосовно заробітних плат у компанії: керівництво (генеральний та фінансовий директори) отримує по 40 тисяч гривень на місяць кожний, керівники відділів отримують по 30 тисяч гривень, фінансові консультанти – 20 тисяч гривень, головний бухгалтер – 25 тисяч гривень, бухгалтери – 17 тисяч гривень, податкові консультанти – 21 тисячу гривень, менеджери проєктів – 16 тисяч гривень, менеджери – 15 тисяч гривень, фахівці з маркетингу – 16 тисяч гривень, офіс-менеджер – 18 тисяч гривень, системний адміністратор – 22 тисячі гривень, асистенти – 8 тисяч гривень. Підрахуємо:

$$C_{єв} = (40000 \cdot 2 + 30000 \cdot 4 + 20000 \cdot 4 + 25000 + 17000 \cdot 5 + 21000 \cdot 2 + 16000 \cdot 3 + 15000 \cdot 3 + 16000 \cdot 2 + 18000 + 22000 +$$

$$8000 \cdot 2) \cdot 0{,}051 = 31263 \text{ грн}$$

Тепер вже за відомими даними розрахуємо вартість електроенергії, що споживається перерахованою раніше апаратурою компанії:

$$С_е = (0{,}35 \cdot 30 + 0{,}1 \cdot 3 + 0{,}7 + 0{,}5 \cdot 2 + 0{,}025 + 0{,}25) \cdot 2016 \cdot 4{,}32 =$$
$$= 111260 \text{ грн}$$

Таким чином, можна підрахувати вартість поточних витрат для компанії:

$$С_к = 195000 + 186250 + 264000 + 31263 + 111260 = 787773 \text{ грн}$$

Отже, можна підсумувати, що загальна сума поточних (експлуатаційних) витрат для компанії «Фінансовий Консалтинг» складає майже 788 тисяч гривень.

3.4 Оцінка можливого збитку від атаки

Впровадження ERP-системи може зробити ІКС підприємства більш привабливою ціллю для зловмисників, тому варто оцінити можливі збитки від атаки на сегменти (модулі) ERP-системи. Перш за все слід розрахувати упущену вигоду від простою атакованого сегменту корпоративної системи, і це можна зробити за допомогою формули (3.10).

$$U = П_п + П_в + V, \text{ грн} \quad (3.10)$$

де $П_п$ – оплачувані втрати робочого часу співробітників та простоїв атакованого сегмента корпоративної системи, грн;

$П_в$ – вартість відновлення працездатності сегмента корпоративної системи, грн;

V – втрати від зниження обсягу продажів за час простою атакованого сегмента корпоративної системи, грн.

В свою чергу, усі складові упущеної вигоди можна розрахувати за такими формулами як (3.11), (3.12), (3.13), (3.14) та (3.15).

$$П_п = \frac{\sum З_с}{F} \cdot t_п, \text{ грн} \quad (3.11)$$

де F – місячний фонд робочого часу, годин;

$З_с$ – заробітна плата співробітників атакованого сегменту корпоративної системи, грн на місяць;

$t_п$ – час простою сегменту корпоративної система внаслідок атаки, годин.

$$П_в = П_{ви} + П_{пв}, \text{ грн} \quad (3.12)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення сегмента корпоративної мережі, грн.

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви}, \text{ грн} \quad (3.13)$$

де $З_с$ – заробітна плата співробітників атакованого сегменту корпоративної системи, грн на місяць;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого сегмента корпоративної системи, годин.

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в, \text{ грн} \quad (3.14)$$

де $З_о$ – заробітна плата обслуговуючого персоналу, грн на місяць;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну систему, годин.

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

де О – обсяг продажів атакованого сегмента корпоративної системи, грн;

$F_г$ – річний фонд часу роботи організації, годин.

Отже, враховуючи дані формули, слід послідовно порахувати компоненти упущеної від простою системи вигоди:

$$П_{п} = \frac{613000}{168} \cdot 4 = 14595 \text{ грн}$$

$$П_{ви} = \frac{613000}{168} \cdot 16 = 58381 \text{ грн}$$

$$П_{пв} = \frac{22000}{168} \cdot 8 = 1048 \text{ грн}$$

$$П_{в} = 58381 + 1048 = 59429 \text{ грн}$$

$$V = \frac{1300000}{2016} \cdot (4 + 8 + 16) = 18055 \text{ грн}$$

$$U = 14595 + 59429 + 18055 = 92079 \text{ грн}$$

Після розрахунків, отримаємо загальну суму упущеної вимоги внаслідок простою атакованого сегменту ERP-системи у вигляді 164 тисяч гривень. Після цього також слід визначити загальний збиток від атаки на сегмент ERP-системи, що можна визначити за формулою (3.16).

$$В = \sum_i \sum_n U, \text{ грн} \quad (3.16)$$

де i – число атакованих сегментів корпоративної системи;

n – середнє число атак на рік.

Після підрахунків отримаємо наступне значення:

$$B = \sum_8 \sum_6 92079 = 4419792 \text{ грн}$$

Наостанок слід порахувати загальний ефект від впровадження ERP-системи та політики безпеки її використання у компанії. У цьому допоможе формула (3.17).

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

де B – загальний збиток від атаки на сегмент корпоративної системи, тис. грн;

R – очікувана імовірність атаки на сегмент корпоративної системи, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 4419{,}792 \cdot 0{,}3 - 778{,}773 = 547{,}17 \text{ тис. грн}$$

Таким чином, загальний ефект від впровадження ERP-рішення та відповідної політики безпеки становить близько 547 тисяч гривень.

3.5 Визначення та аналіз показників економічної ефективності

Щоб остаточно оцінити та довести доцільність впровадження ERP-системи та розробки політики безпеки її використання, слід звернутись до коефіцієнту повернення інвестицій. Він вказує на те, скільки гривень додаткового прибутку принесе одна гривня капітальних інвестицій на впровадження ERP-системи та політики інформаційної безпеки у ній. Порахувати даний коефіцієнт можливо за формулою (3.18), наведеною нижче.

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

де E – загальний ефект від впровадження ERP-системи та політики безпеки її використання, тис. грн;

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

Підставивши значення пораховані раніше значення у відповідні місця, отримаємо наступне число:

$$ROSI = \frac{547{,}17}{296{,}132} = 1{,}85$$

Отриманий результат підтверджує економічну доцільність обраного підприємством рішення по впровадженню нового програмного забезпечення.

Період окупності усіх витрат можна знайти за допомогою формули (3.19).

$$\mathrm{T_o} = \frac{1}{ROSI}, \text{ років} \qquad (3.19)$$

$$T_o = \frac{1}{1,85} = 0,54 \text{ року}$$

Таким чином, обернений показник коефіцієнту $ROSI$ вказує на термін окупності капітальних витрат на обране рішення і дорівнює періоду майже у 6 з половиною місяців.

Висновок до третього розділу

У третьому розділі цієї кваліфікаційної роботи було розглянуто питання економічної доцільності впровадження ERP-системи до ІКС компанії та розробки політики безпеки інформації при використанні цієї системи. Крім того, було розраховано капітальні та поточні витрати компанії, на основі яких було оцінено можливі збитки компанії у разі атаки на ERP-систему або її окремий сегмент, після чого визначено коефіцієнт $ROSI$ та термін окупності.

Серед основних результатів розрахунків було отримано, що:

1. Трудомісткість розробки політики безпеки становить близько 66 годин, що складає трохи більше ніж 8 робочих днів, а фінансові витрати на неї можуть зайняти близько 296 тисяч гривень.
2. Поточні (експлуатаційні) витрати на підтримку функціонування ERP-системи та ІКС компанії в цілому складають 788 тисячі гривень.
3. Можливий збиток від атаки на ERP-систему в цілому може завдати шкоди підприємству майже у 4,42 мільйони гривень.
4. Одна гривня капітальних інвестицій на розробку політики безпеки принесе підприємству 1 гривню та 85 копійок додаткового прибутку.
5. Термін окупності усіх витрат становить 197 днів, що є приблизно 6 з половиною місяців.

Ці підрахунки допомогли довести економічну доцільність розробки політики безпеки для захисту обраної для впровадження ERP-системи.

ВИСНОВКИ

В даній кваліфікаційній роботі було досліджено процес вибору та впровадження ERP-системи у компанію «Фінансовий Консалтинг», зокрема розробку політики безпеки інформації при використанні цієї системи.

Аналіз та оцінка показали, що загалом ERP-системи є швидко набираючим популярність рішенням для сучасних бізнес-організацій, але, крім того, вони мають привілеї у вигляді достатньо високого рівня безпеки, який, за необхідності, можна покращити завдяки стороннім рішенням. Як і будь-яка система, ERP має власні вразливості, проте при дотриманні встановлених у компанії процедур та політик, конфіденційність, цілісність та доступність оброблюваної у ERP-системі інформації має досягати належного рівня.

Серед трьох розглядуваних ERP-систем найвищий показник отримала третя система. Вона має високі бали за всі сформульовані у процесі оцінки критерії, окрім двох – механізми перевірки порушення цілісності даних та стійкість до відмов. Проте ці критерії можливо самостійно впровадити за допомогою інтеграції з іншими програмними застосунками.

Наприкінці було оглянуто та обґрунтовано питання економічної доцільності розробки політики безпеки та впровадження ERP-системи, і за отриманими результатами можна підсумувати, що дане рішення для компанії може принести поштовх в компанії для подальшого безпечного розвитку.

Саме тому практична цінність даної кваліфікаційної роботи полягає у підвищенні безпеки та оптимізації бізнес-процесів у компанії «Фінансовий Консалтинг».

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України “Про захист інформації в інформаційно-комунікаційних системах.” https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

2. ДСТУ ISO/IEC 27001:2023 “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”

3. ДСТУ ISO/IEC 27002:2023 “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”

4. Eurostat. (2023). Enterprises using ERP software. https://ec.europa.eu/eurostat/databrowser/bookmark/67bb2880-ffd7-4e5e-8f95-c153342160fd?lang=en

5. Statista. (2023). Revenue in the Enterprise Resource Planning Software segment in Ukraine. https://www.statista.com/outlook/tmo/software/enterprise-software/enterprise-resource-planning-software/ukraine

6. TechReport. (2024). ERP Statistics: Market Share, Implementation, and Benefits. https://techreport.com/statistics/software-web/erp-statistics/

7. World Metrics. “Cybersecurity in the ERP Industry: Statistics.” https://worldmetrics.org/cybersecurity-in-the-erp-industry-statistics/

8. OWASP. (2023). OWASP Top 10:2023

9. ДСТУ ISO/IEC 15408-1:2023 “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель”

10. ДСТУ ISO/IEC 15408-2:2023 “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки”

11. НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”

12. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу”

13. НД ТЗІ 1.1-003-99 “Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу”

14. DOU. (2023). Статистика зарплат програмістів, тестувальників і PM в Україні. https://jobs.dou.ua/salaries

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	2	
5	А4	1 Розділ	26	
6	А4	2 Розділ	27	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

Копач_КР_125_20_1_ДМ.pptx

Копач_КР_125_20_1_ПЗ.docx

Копач_КР_125_20_1_ПЗ.pdf

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку ____ б. («_____»).

Керівник розділу _____ Дар'я ПІЛОВА

(підпис) (ім'я, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка політики безпеки при використанні ERP-системи для компанії «Фінансовий Консалтинг»
студентки групи 125-20-1
Копач Вікторії Владиславівни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 83 сторінках та містить 4 рисунка, 5 таблиці, 14 джерел та 4 додатка.

Метою даної кваліфікаційної роботи є підвищення рівня захищеності обраної ERP-системи в компанії «Фінансовий Консалтинг».

У загальній частині описано загальні відомості про ERP-системи, розглянуто їхню актуальність, вразливості та методи захисту, ознайомлено з організаційною структурою компанії «Фінансовий Консалтинг», її обчислювальною та інформаційною системою, обрано та обґрунтовано профіль захищеності інформаційно-комунікаційної системи компанії.

У спеціальній частині проаналізовано відповідність поточної інформаційно-комунікаційної системи обраному профілю захищеності, сформульовано критерії оцінки та безпосередньо оцінено безпеку ERP-систем, обґрунтовано вибір ERP-системи та розроблено політику безпеки інформації при її використанні.

В економічній частині визначено доцільність впровадження та розробки політики безпеки при використанні обраної ERP-системи, пораховано загальну трудомісткість розробки, капітальні і поточні витрати компанії, термін окупності даної розробки.

Практичне значення роботи полягає у покращенні бізнес-процесів та підвищенні рівня захищеності інформаційно-комунікаційної системи компанії.

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

Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». 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 «відмінно».

Керівник кваліфікаційної роботи:
д.т.н., проф. Валерій КОРНІЄНКО

Керівник спеціального розділу:
ас. Ілля ОЛІШЕВСЬКИЙ