МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна графіка і Web-дизайн»

Група: 4КГ-05

Дипломний проект

здобувача освіти денної форми навчання
КГ.05.20.000.ДП

Романової Катерини Андріївни

м. Одеса
2022 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Комп'ютерна графіка і Web-дизайн»**

Група: **4КГ-05**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Розробка системи контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту

Проектний матеріал складається з пояснювальної записки на __1____ сторінках та графічного (презентаційного) матеріалу на 11 аркушах (слайдах).

Дипломник _____ (Романова К.А.)

Керівник _____ (Шевцов Ю.С.)

Консультанти:

з економічної частини _____ (Копайгородська Т.Г.)

з охорони праці_____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Скорнякова О.В.)

До захисту допущений

Голова циклової комісії _____ (Скорнякова О.В.)

Завідувач відділення _____ (Суліма Ю.Ю.)

Захист «____»_____ 2022 р. Протокол ДКК №_____

Оцінка ДКК _____

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНАХТ»

Відділення **комп'ютерних систем** Комісія **КТ та ІІІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Комп'ютерна графіка і Web-дизайн»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР_____

_____

"_____"_____2022 р.

З А В Д А Н Н Я

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти **Романовій Катерині Андріївні**

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи): **Розробка системи контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту**

затверджена наказом по коледжу від "**30**" **січня** 202**1** р. № **306-А2-ОД**

2. Термін здачі закінченого проекту (роботи) _____

3. Вихідні данні до проекту (роботи): **Управління ІТ-бізнесом. Оцінка ІТ ризиків. Кібербезпека. Політика інформаційної безпеки ІТ-компанії. Virtual Privat Network. CRC-суми. ІТ-ресурси. ІТ-аудит. Внутрішній ІТ-аудит. Зовнішній ІТ-аудит. Алгоритм проведення аудиторскої перевірки. ІТ-середовище. СВ-ІТ-аудиту. COBIT. ISO 20000x.**

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

ВСТУП.

1. **ТЕХНОЛОГІЧНИЙ РОЗДІЛ**
2. **ЕКОНОМІЧНИЙ РОЗДІЛ**
3. **ОХОРОНА ПРАЦІ**
4. **ВИСНОВКИ**

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Створення презентаційного матеріалу, кількість слайдів не менше 10

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Вступ, 1	Шевцов Ю.С.		
2	Копайгородська Т.Г.		
3	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7. Дата видачі завдання _____

Керівник _____

(підпис)

Завдання прийняв до виконання _____

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	Огляд літератури. Огляд існуючих рішень.		
2.	Формування кінцевого завдання на розробку. Вступна частина дипломного проекту.		
3.	Технологічний розділ. Складники контролю роботи IT-компанії.		
4.	Технологічний розділ. Політика безпеки IT-компанії.		
5.	Технологічний розділ. Розробка системи контролю роботи IT-компанії за допомогою аудиту.		
6.	Економічний розділ.		
7.	Виконання розділу «Охорона праці».		
8.	Підготовка доповіді та презентації для захисту		
9.	Підготовка до попереднього захисту, підготовка до захисту		
10.	Отримання рецензії, відповіді на зауваження рецензента		
11.	Захист роботи		

Дипломник _____

(підпис)

Керівник _____

(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КГ.05.20.000.ДП	Дипломний проект		
А4			КГ.05.20.000.ДП. ПЗ	Пояснювальна записка	1	
				Презентація		

Ізм.	Арк.	№ докум.	Підпис	Дата	КГ.05.20.000.ДП		
Розробив		Романова К.А.			Розробка системи контролю роботи IT-компанії за допомогою внутрішнього та зовнішнього аудиту	Літ.	Аркуш 3 / Ар-
Перевірив		Шевцов Ю.С.				Н Д П	
Н. Контр.		Петрашова В.І.				ВСП ОТФК ОНТУ	
Затверд.		Скорнякова					

АНОТАЦІЯ

Метою даної роботи є розробка системи контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту.

В даній випускній роботі молодшого спеціаліста розглянуто внутрішній і зовнішній аудит на підприємстві, захист конфіденційної інформації в ІТ компанії. Були визначені цілі, завдання та елементи внутрішнього контролю підприємства. В роботі був розроблений алгоритм проведення аудиторської перевірки. В рамках розробки системи контролю роботи ІТ-компанії, були проаналізовані складники контролю за допомогою внутрішнього та зовнішнього аудиту. Був розроблений варіант контролю готовності до інновацій за допомогою аудиту інформаційних технологій та розроблена система контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту.

ЗМІСТ

ВСТУП

Чим масштабнішим стає бізнес, тим складніше стає його контролювати. Якщо на початку тримати все під контролем може його власник чи директор, то з його розвитком одній особі стає складно якісно організовувати всі процеси. Що потрібно запроваджувати на підприємстві та які акценти варто розставляти в процесах контролю, розкриємо у цій публікації.

Будь-який бізнес – це сукупність певних ресурсів. До цих ресурсів належать ті, що мають матеріальне вираження: нерухоме майно, обладнання, корпоративні права, так і ті, що виражені у нематеріальні формі: інформація щодо діяльності підприємства, її комерційні таємниці. Одним із ключових ресурсів є люди – топменеджмент та інші працівники компанії. За якісно сформованими процесами лежить ключ до успіху будь-якої компанії. У XXI столітті важливо не стільки вартість нерухомого майна, яке належить підприємству, скільки захист інформації, яка обробляться ним. Втрата певних відомостей може призвести до різних негативних наслідків. Від витоку клієнтської бази, яку недобросовісні конкуренти можуть використати на власний розсуд, до протиправного заволодіння інформаційним майном підприємства.

Сучасний період розвитку ринкової економіки засвідчує ситуацію, у якій все більшої уваги серед вітчизняних суб’єктів господарювання набуває інтерес до ІТ-середовища. Як показує практика, ІТ-середовище виступає джерелом людських, технічних, інформаційних та програмних ресурсів, що необхідні для забезпечення розвитку підприємства. Однак, для ефективного їх використання в діяльності підприємства необхідно регулярно здійснювати перевірку їх застосування, тобто ІТ-аудит.

РОЗДІЛ 1. СКЛАДНИКИ КОНТРОЛЮ РОБОТИ ІТ-КОМПАНІЇ

Управління ІТ-бізнесом – це складний процес, що потребує уваги, системного підходу та найвищого рівня контролю і безпеки. Чим більше компанія, тим складніше вибудовується система менеджменту, і тим важче налагодити процес звітності та рівнів відповідальності.

Істотну роль у системі контролю роботи ІТ-бізнесу відіграють наступні заходи:

- Розробка політик конфіденційності, які повинні бути доведені до відома всіх працівників.
- Підписання договорів про конфіденційність із чіткими вимогами щодо фіксування наслідків витоку інформації.
- Використання ліцензованого програмного забезпечення для роботи із операційними завданнями бізнесу.
- Формування практик зберігання операційних документів у «хмарних середовищах».
- Запровадження електронного документообігу.
- Інші заходи у сфері ІТ, що спрямовані на попередження витоків інформації та хакерських атак на підприємство.

За підтримки ІТ-підрозділу компанії необхідно формувати належну технічну базу, яка убезпечить конфіденційність усього документообігу підприємства. Тоді як юридичний департамент та департамент з управління персоналом повинні розробити політики поводження із конфіденційною інформацією, правила користування технікою компанії та підготувати договори про конфіденційність.

1.1 Захист конфіденційної інформації в ІТ компанії

Конфіденційність інформації - обов'язкова для виконання особою, яка отримала доступ до певної інформації, вимога не передавати таку інформацію третім особам без згоди її власника. У діяльності ІТ компаній поняття «конфіденційність» може мати багато граней, а тому питання захисту

конфіденційності також є багатогранним. В процесі діяльності компанії важливо не допустити розголошення унікальної клієнтської бази або злому серверів, може виникнути необхідність зберігати в таємниці інформацію про проект, який тільки розробляється, але який підірве ринок і т.д. Тому розуміння шляхів і способів захисту конфіденційної інформації компанії є одним з запорук її успішної діяльності.

Збереження внутрішньої інформації IT компанії в таємниці вигідно для кожного бізнесу через декілька досить очевидних причин:

- Конкурентна перевага: ще Ротшильди сказали: «Що той, хто володіє інформацією – володіє світом». Якщо у нас з'явилася ідея революційного проекту або неймовірного технологічного рішення, ми точно не захочемо, щоб про нього дізналися наші конкуренти. Зберігати в таємниці інформацію про проекти, корпоративну культуру, методики підбору персоналу і т.д. – означає завжди мати туза в рукаві.
- Цінність конфіденційної інформації: особливо у випадку з IT компаніями, вартість інформації або даних, якими вони володіють (клієнтська база, унікальний софт, алгоритми роботи і т.д.) може у багато разів перевищувати вартість їх матеріальних активів (офісне приміщення, обладнання, техніка і т.д.). У разі розголошення клієнтської бази або інформації про проект втрати компанії в моменти можуть бути колосальними, не кажучи про втрати в перспективі.
- Робота з іноземними клієнтами: в своїй більшості, клієнти вітчизняних IT компаній знаходяться за кордоном – США, Європа, Великобританія і т.д. З одного боку, зарубіжні контрагенти цінують, коли бізнес ведеться чітко, правильно, надійно і в повній відповідності з законом (що включає в себе налагоджені механізми захисту інформації). З іншого боку, при роботі з іноземними клієнтами ми отримуємо в розпорядження їх секрети, їх інформацію, а тому стаємо відповідальними вже не тільки перед самими собою, а й перед клієнтами. Тому для спокійного сну вночі потрібно мати надійну систему захисту.

- Вимоги законодавства: банальна, але через це не менш важлива причина. Законодавство кожної країни встановлює свої власні, але незмінно жорсткі та конкретні зобов'язання щодо захисту конфіденційної інформації і персональних даних. Якщо наша компанія не буде їх дотримуватися – ми легко можете потрапити до суду, де зустрітись як з представниками держорганів, так і з клієнтом / замовником, з конфіденційною інформацією якого трапилася неприємність.

Перш за все, слід визначити, що ж в компанії є саме цією конфіденційною інформацією. У кожній компанії є як стандартні категорії такої інформації (наприклад, розмір заробітної плати, умови роботи, побудова бізнес-процесів), так і спеціальні категорії, які залежать від діяльності компанії (наприклад, для тих, хто орендує приміщення – система паролів та доступів).

Як тільки визначено перелік інформації яка є конфіденційною, потрібно описати види захисту.

Перший вид захисту – документальний. Він полягає в необхідності закріпити всі принципи, рішення, правила, способи захисту і т.д. на папері. Це повинно включати в себе наступні дії:

- Складання і підписання угоди про нерозголошення конфіденційної інформації (NDA) з кожним із співробітників, клієнтів, інвесторів, постачальників, підрядників, контрагентів і т.д. Для душевного спокою, NDA варто підписувати навіть зі стажерами і відвідувачами, так як вони теж можуть, випадково чи ні, отримати доступ до конфіденційної інформації.
- Складання Положення компанії про захист конфіденційності. Вимога до наявності такого документа найчастіше встановлюється законодавством для компаній, які працюють зі співробітниками за трудовими договорами. У той же час, для компаній, які працюють за схемою договорів з підрядниками, складання такого документа також може бути вигідним.

- З кожного співробітника має бути письмове зобов’язання, в якому співробітник вказує, що ознайомився з текстом Положення і зобов’язується не порушувати його норми.
- Складання внутрішніх процедур поводження з конфіденційною інформацією. Ці документи будуть суто внутрішніми документами ІТ компанії. Вони повинні регламентувати порядок і правила доступу до конфіденційної інформації; її пересилання; доступу до неї третіх осіб; перелік співробітників, яким дозволено доступ до тієї чи іншої інформації; алгоритм дії в разі порушення захисту конфіденційної інформації і т.д. Для складання цих документів ІТ компанії слід звернутися до профільної юридичній фірмі, яка б проконсультувала компанію з цього питання, провела аналіз її рівня захисти конфіденційної інформації і склала необхідні документи.

Другий вид захисту – технічний. Він полягає в необхідності реалізувати на ділі всі наші рішення і плани. Це повинно включати в себе наступні дії:

- Визначити, хто має доступ до конфіденційної інформації на даний момент. Це дозволить зрозуміти, в якому масштабі потрібно впроваджувати захисні алгоритми, які місця в питанні захисту є найбільш уразливими і т.д. Одним з найпоширеніших підходів є рішення не давати повного доступу до конфіденційної інформації нікому, в тому числі – ІТ-фахівцям.
- Завжди важлива не тільки оцінка ризиків, але і подальший моніторинг. Тому після аналізу ситуації з доступом до конфіденційної інформації необхідно контролювати, хто і як користується, пересилає, змінює, доповнює, видаляє, переглядає і т.д. цю інформацію. Також, у разі будь-якого порушення системи захисту така інформація і аналітика буде на вагу золота.
- Внутрішня система для роботи і спілкування співробітників. Створення корпоративної чат-системи між співробітниками добре тим, що, по-перше, це дозволяє на 99% забезпечити оборот і передачу конфіденційної інформації тільки всередині таких корпоративних систем, а не через відкриті джерела (наприклад,

Telegram, Facebook і т.д.), а по-друге, збирати дані про будь-які операції з конфіденційною інформацією на випадок можливого порушення її захисту.

- Паролі. Переконайтеся, що доступ до всього знаходиться під захистом. Криптографічне шифрування ПК, паролі доступу до папок з конфіденційною інформацією, особисті паролі доступу в корпоративну систему для кожного співробітника і т.д. – все це є очевидно необхідним, а також дозволяє збирати дані про доступ до конфіденційної інформації, які можуть стати в нагоді для аналітики.
- Система захисту від кібератак. Така система базова і може включати в себе превентивні засоби захисту, процедуру резервного копіювання конфіденційної інформації, прописаний алгоритм дії в разі кібератаки або іншого порушення захисту конфіденційної інформації і т.д.

Окремі заходи можуть знадобитись IT компаніям, які знімають великі офіси. Для таких компаній розумним буде встановити обов'язкову рівневу систему доступу до приміщень (вхід-відділи-кабінети), мати систему відеоспостереження, службу охорони, захищену Wi-Fi мережу і т.д.

Загалом, захист конфіденційної інформації – це не питання п'яти хвилин: цим потрібно займатися постійно, методично і з розумом, а навіть найкоротша перерва може призвести якщо не до незворотних наслідків, то до досить серйозних втрат.

Також, не варто забувати, що це повинно бути комплексним процесом. Підписання з усіма співробітниками договору без впровадження реальних механізмів забезпечення конфіденційності або навпаки – розробка та впровадження хорошої системи і алгоритмів захисту інформації, працюючи без документів «під чесне слово» – будь-який з таких варіантів не буде працювати.

1.2 Оцінка IT ризиків

Комп'ютерне обладнання і програмна база, що використовуються в компаніях, вимагають підтримки актуального стану. Інформаційні технології повинні відповідати потребам і завданням бізнесу, для цього необхідний контроль і облік. Експертний аналіз IT дозволяє отримати достовірну інформацію про стан

інформаційно-технологічних ресурсів компанії. Все це можна реалізувати за допомогою IT-аудиту.

Аудит інформаційної безпеки (ІБ) — це розуміння, управління, контроль і зниження ризиків для критично важливих активів компанії. Якщо ми працюєте з даними в мережі, — нам необхідна оцінка ризиків інформаційної безпеки нашої організації.

Аудит кібербезпеки – це можливість уникнути незапланованих ризиків, пов'язаних з відмовою або неправильним використанням IT. На Рис.1.1 наведено ризики кібербезпеки.

Рисунок 1.1 –Ризики кібербезпеки

Кібербезпека — це складне питання, в якому багато чинників і критеріїв мають значення. І це одна з причин, чому багато організацій відкладають рішення забезпечення кібербезпеки в «довгий ящик». На жаль, 100 %- гарантії безпеки не існує, тому важливо застосовувати підхід, що ґрунтується на оцінці IT-ризиків, зосередивши увагу, насамперед, на пріоритетах і ризиках.

Аудит інформаційної безпеки містить докладний опис конкретного фінансового збитку, який IT-ризики можуть нанести організації. Наприклад,

судові витрати, простої в роботі й пов'язані з цим втрати прибутку, а також втрачений бізнес через недовіру клієнтів. Найважливіші питання щодо IT-ризиків представлені Рис.1.2 :

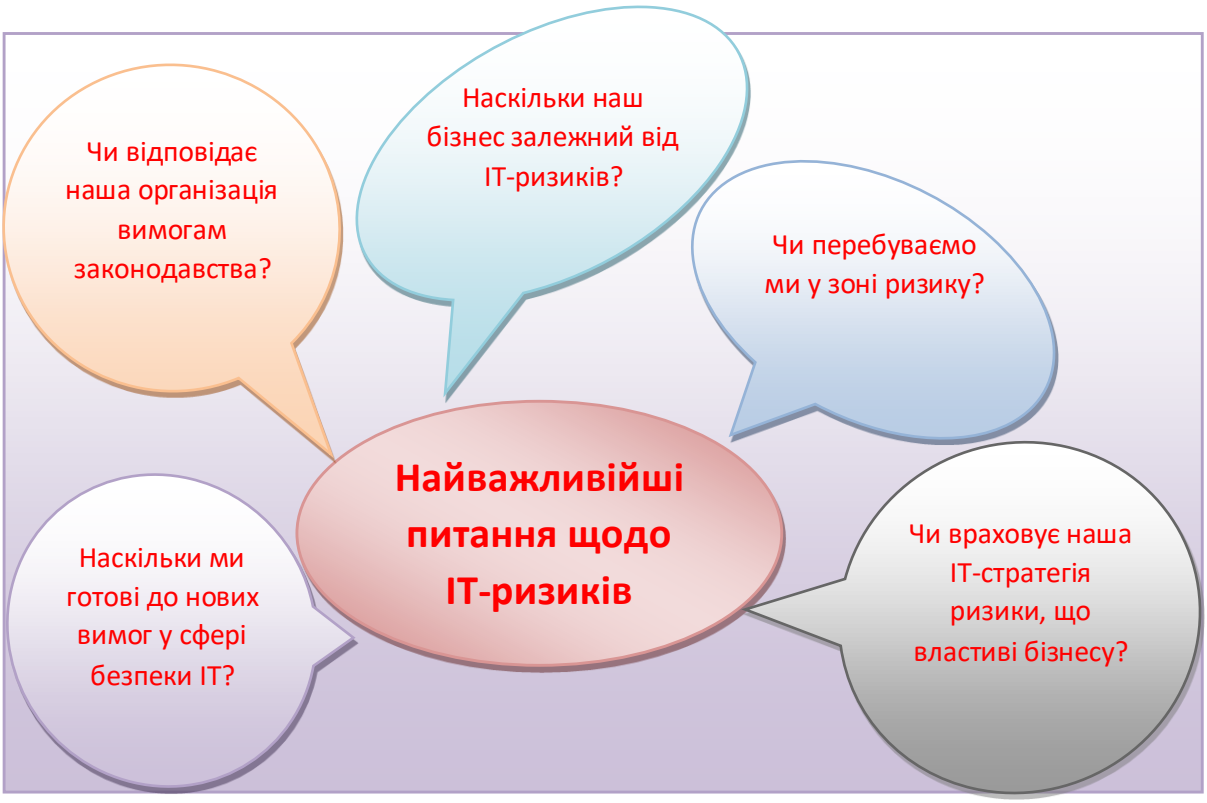

Рисунок 1.2 – Найважливіші питання щодо IT-ризиків

Залишається лише визначити, що є причиною ризиків та від кого необхідно захищатись.

Після визначення цілей управління ІБ слід проаналізувати проблеми, які заважають наблизитися до цільового стану. На цьому рівні процес аналізу ризиків спускається до інформаційної інфраструктури та традиційних понять ІБ – порушників, загроз та вразливостей. Для оцінки ризиків недостатньо ввести стандартну модель порушника, що розділяє всіх порушників на кшталт доступу до активу та знань, про структуру активів. Такий поділ допомагає визначити, які загрози можуть бути спрямовані на актив, але не дає відповіді на питання, чи можуть бути ці загрози в принципі реалізовані. У процесі аналізу ризиків необхідно оцінити вмотивованість порушників під час реалізації загроз. При цьому під

порушником мається на увазі не абстрактний зовнішній хакер або інсайдер, а сторона, яка зацікавлена в отриманні вигоди шляхом порушення безпеки активу.

Початкову інформацію про моделі порушника, як й у випадку з вибором початкових напрямів діяльності із забезпечення ІБ, доцільно отримати у вищого менеджменту, що представляє собі положення організації на ринку, що має відомості про конкурентів і про те, яких методів впливу можна від них очікувати. Відомості, необхідні для розробки моделі порушника, можна отримати зі спеціалізованих досліджень з порушень в області комп'ютерної безпеки у сфері бізнесу, на яку проводиться аналіз ризиків. Правильно опрацьована модель порушника доповнює цілі забезпечення ІБ, визначені в оцінці активів організації.

Розробка моделі загроз та ідентифікація вразливостей нерозривно пов'язані з інвентаризацією оточення інформаційних активів організації. Сама собою інформація не зберігається та не обробляється. Доступ до неї забезпечується за допомогою інформаційної інфраструктури, що автоматизує бізнес-процеси організації. Важливо зрозуміти, як інформаційна інфраструктура та інформаційні активи організації пов'язані між собою.

З позиції управління ІБ значимість інформаційної інфраструктури може бути встановлена лише після визначення зв'язку між інформаційними активами та інфраструктурою. Якщо процеси підтримки та експлуатації інформаційної інфраструктури в організації регламентовані та прозорі, збір інформації, необхідний для ідентифікації загроз та оцінки вразливостей, значно спрощується.

Розробка моделі загроз - робота для професіоналів у галузі ІБ, які добре уявляють собі, яким чином порушник може отримати неавторизований доступ до інформації, порушуючи периметр захисту або діючи методами соціальної інженерії. При розробці моделі загроз можна також говорити про сценарії як послідовні кроки, відповідно до яких можуть бути реалізовані загрози. Дуже рідко трапляється, що загрози реалізуються одним кроком шляхом експлуатації єдиного вразливого місця системи.

У модель загроз слід включити всі загрози, виявлені за наслідками суміжних процесів управління ІБ, таких як управління вразливістю та інцидентами.

Потрібно пам'ятати, що загрози необхідно ранжувати одна щодо одної за рівнем ймовірності їх реалізації.

І тому у процесі розробки моделі загроз, необхідно вказати найбільш значущі чинники, існування яких впливає її реалізацію.

РОЗДІЛ 2. ПОЛІТИКА БЕЗПЕКИ ІТ-КОМПАНІЇ

Політика безпеки будується з урахуванням аналізу ризиків, які визнаються реальними для інформаційної системи організації. Коли ризики проаналізовано та стратегію захисту визначено, складається програма забезпечення інформаційної безпеки. Під цю програму виділяються ресурси, призначаються відповідальні, визначається порядок контролю за виконанням програми тощо.

У широкому сенсі політика безпеки визначається як система документованих управлінських рішень щодо забезпечення безпеки організації. У вузькому розумінні під політикою безпеки зазвичай розуміють локальний нормативний документ, що визначає вимоги безпеки, систему заходів, або порядок дій, а також відповідальність співробітників організації та механізми контролю для певної галузі безпеки. Перед тим, як почати формувати саму політику інформаційної безпеки, необхідно розібратися в основних поняттях, якими ми оперуватимемо.

2.1 Політика інформаційної безпеки ІТ-компанії

Інформація – відомості (повідомлення, дані) незалежно від форми їх подання.

Інформаційна безпека (ІБ) – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання та розвиток на користь громадян, організацій, держав.

Поняття "інформація" сьогодні використовується досить широко та різнобічно.

Забезпечення безпеки інформації може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні та реалізації найбільш раціональних методів, способів та шляхів удосконалення та розвитку системи захисту, безперервному контролі її стану, виявлення її слабких місць та протиправних дій.

Безпека інформації може бути забезпечена лише при комплексному використанні всього асортименту наявних засобів захисту у всіх структурних

елементах виробничої системи та на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі використовувані засоби, методи та заходи поєднуються в єдиний цілісний механізм системи захисту інформації. При цьому функціонування системи має контролюватись, оновлюватись та доповнюватись залежно від зміни зовнішніх та внутрішніх умов. Також варто враховувати, що умови можуть змінюватися непередбачено.

Можна назвати такі види вимог до безпеки:

- функціональні: відповідають активному аспекту захисту, що пред'являються до функцій безпеки та механізмів, які їх реалізують;
- вимоги довіри: відповідають пасивному аспекту, що висуваються до технології, процесу розробки та експлуатації.

Дуже важливо, що безпека розглядається не статично, а у прив'язці до життєвого циклу об'єкта оцінки. Виділяються такі етапи:

- визначення призначення, умов застосування, цілей та вимог безпеки;
- проектування та розробка;
- випробування, оцінка та сертифікація;
- використання та експлуатація.

Отже, докладніше зупинимося на функціональних вимогах безпеки. Вони включають:

- захист даних користувача;
- захист функцій безпеки (вимоги відносяться до цілісності і контролю даних сервісів безпеки та реалізують їх механізми);
- управління безпекою (вимоги цього класу відносяться до управління атрибутами та параметрами безпеки);
- аудит безпеки (виявлення, реєстрація, зберігання, аналіз даних, що стосуються безпеки об'єкта оцінки, реагування на можливе порушення безпеки);
- приватність (захист користувача від розкриття та несанкціонованог використання його ідентифікаційних даних);

- використання ресурсів (вимоги до доступності інформації);
- зв'язок (аутентифікація сторін);
- довірений маршрут/канал (для зв'язку із сервісами безпеки).

Відповідно до цих вимог потрібно формувати систему інформаційної безпеки організації.

Система інформаційної безпеки організації включає напрямки:

- нормативні;
- організаційні (адміністративні);
- технічні;
- програмні;

Для повної оцінки ситуації на підприємстві за всіма напрямами забезпечення безпеки, необхідна розробка концепції інформаційної безпеки. Яка б встановлювала системний підхід до проблеми безпеки інформаційних ресурсів і була систематизованим викладом цілей, завдань, принципів проектування та комплексу заходів щодо забезпечення інформаційної безпеки на підприємстві.

В основі системи інформаційного контролю ІТ-компанії повинні лежати наступні принципи Рис.2.1:

- забезпечення захисту існуючої інформаційної інфраструктури підприємства від втручання зловмисників;
- забезпечення умов для локалізації та мінімізації можливої шкоди;
- виключення появи на стадії причин виникнення джерел загроз;
- забезпечення захисту інформації за трьома основними видами загроз (доступність, цілісність, конфіденційність).

Рисунок 2.1 – Система інформаційного контролю IT-компанії

Розв'язання вищезгаданих завдань досягається шляхом:

- регламентація дій користувачів роботи з інформаційною системою;
- регламентація дій користувачів роботи з базою даних;
- єдині вимоги до надійності технічних засобів та програмного забезпечення;
- процедури контролю роботи інформаційної системи (протоколювання подій, аналіз протоколів, аналіз мережевого трафіку, аналіз роботи технічних засобів);

Політика інформаційної безпеки включає основний документ – «Політика безпеки».

У ньому в цілому описана політика безпеки організації, загальні становища, а як і з усіма аспектами політики зазначені відповідні документи:

- інструкція щодо регламентації роботи користувачів;
- посадова інструкція адміністратора локальної мережі;

- посадова інструкція адміністратора бази даних;
- інструкція щодо роботи з ресурсами Інтернет;
- інструкція щодо організації парольного захисту;
- інструкція з організації антивірусного захисту.

Документ "Політика безпеки" містить основні положення. На основі нього будується програма забезпечення інформаційної безпеки, будуються посадові інструкції та рекомендації.

- Інструкція з регламентації роботи користувачів локальної мережі організації регулює порядок допуску користувачів до роботи у локальній мережі обчислювальної мережі організації, а також правила поводження з інформацією, що захищається, оброблюється, зберігається і передається в організації.
- Посадова інструкція адміністратора локальної мережі визначає обов'язки адміністратора локальної мережі, що стосуються забезпечення інформаційної безпеки.
- Посадова інструкція адміністратора бази даних визначає основні обов'язки, функції та права адміністратора бази даних. У ній дуже докладно описані всі посадові обов'язки та функції адміністратора бази даних, а також права та відповідальність.
- Інструкція по роботі з ресурсами Інтернет відображає основні правила безпечної роботи з мережею інтернет, також містить перелік допустимих недопустимих дій під час роботи з ресурсами інтернет.
- Інструкція з організації антивірусного захисту визначає основні положення, вимоги до антивірусного захисту інформаційної системи організації, всі аспекти пов'язані з роботою антивірусного програмного забезпечення, а також відповідальність у разі порушення антивірусного захисту.
- Інструкція з організації парольного захисту регламентує організаційно-технічне забезпечення процесів генерації, зміни та припинення дії паролів

(видалення облікових записів користувачів). А також регламентовані дії користувачів та обслуговуючого персоналу під час роботи з системою.

Таким чином, основою для організації процесу захисту є політика безпеки, існуюча для того, щоб визначити, від яких загроз і яким чином захищається інформація в інформаційній системі.

Під політикою безпеки розуміється набір правових, організаційних і технічних заходів захисту інформації, прийнятий у конкретній організації. Тобто політика безпеки містить у собі безліч умов, за яких користувачі отримують доступ до ресурсів системи без втрати якості інформаційної безпеки цієї системи. Завдання забезпечення інформаційної безпеки має вирішуватися системно. Це означає, що різні засоби захисту (апаратні, програмні, фізичні, організаційні тощо) повинні застосовуватися одночасно під централізованим управлінням.

Політика інформаційної безпеки є пакет документів, що регламентує роботу працівників, описує основні правила роботи з інформацією, інформаційною системою, базами даних, локальною мережею та ресурсами інтернету. Важливо розуміти, яке місце політика інформаційної безпеки займає у спільній системі управління організацією.

Нижче наведено загальні організаційні заходи, пов'язані з політикою безпеки. На процедурному рівні можна виділити такі класи заходів:

- управління персоналом;
- фізичний захист;
- підтримання працездатності
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

Управління персоналом починається з прийому працівників, проте ще до цього слід визначити комп'ютерні привілеї, пов'язані з посадою. Існує два загальних принципу, які слід мати на увазі:

- розподіл обов'язків;
- мінімізація привілеїв.

Принцип поділу обов'язків наказує як розподіляти ролі та відповідальність, щоб одна людина не могла порушити критично важливий для організації процес. Наприклад, небажана ситуація, коли великі платежі від імені організації виконує одна людина. Надійніше доручити одному співробітнику оформлення заявок на подібні платежі, а іншому – завіряти ці заявки. Інший приклад – процедурні обмеження дій суперкористувача. Можна штучно розщепити пароль суперкористувача, повідомивши першу його частину одному співробітнику, а другу - іншому. Тоді критично важливі дії щодо адміністрування інформаційної системи вони зможуть виконати лише вдвох, що знижує ймовірність помилок та зловживань.

Принцип мінімізації привілеїв наказує виділяти користувачам ті права доступу, які необхідні їм до виконання службових обов'язків. Призначення цього принципу очевидне – зменшити збитки від випадкових чи навмисних некоректних дій. Попереднє складання опису посади дозволяє оцінити її критичність та спланувати процедуру перевірки та відбору кандидатів. Чим відповідальніша посада, тим ретельніше потрібно перевіряти кандидатів: навести про них довідки, можливо поговорити з колишніми товаришами по службі тощо. Подібна процедура може бути тривалою та дорогою, тому немає сенсу додатково ускладнювати її. У той же час, нерозумно і зовсім відмовлятися від попередньої перевірки, аби випадково не прийняти на роботу людину із кримінальним минулим чи психічним захворюванням.

Коли кандидата визначено, він повинен пройти навчання; принаймні його слід докладно ознайомити зі службовими обов'язками, а також з нормами та

процедурами інформаційної безпеки. Бажано, щоб заходи безпеки були ним засвоєні до вступу на посаду та до заведення його системного рахунку з вхідним ім'ям, паролем та привілеями.

2.2 Методи забезпечення інформаційної безпеки

На сьогоднішній день існує великий арсенал методів забезпечення інформаційної безпеки:

- засоби ідентифікації та автентифікації користувачів;
- засоби шифрування інформації, що зберігається на комп'ютерах та передається по мережах;
- міжмережеві екрани;
- віртуальні приватні мережі;
- засоби контентної фільтрації;
- інструменти перевірки цілісності вмісту дисків;
- засоби антивірусного захисту;
- системи виявлення вразливостей мереж та аналізатори мережевих атак.

Система аутентифікації (або ідентифікації), авторизації та адміністрування. Ідентифікація та авторизація – це ключові елементи інформаційної безпеки. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування полягає в наділенні користувача певними ідентифікаційними особливостями в рамках цієї мережі та визначенні обсягу допустимих для нього дій.

Системи шифрування дозволяють мінімізувати втрати у разі несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересиланні електронною поштою або передачі мережевими протоколами. Завдання даного засобу захисту – забезпечення конфіденційності. Основні вимоги до систем шифрування - високий рівень криптостійкості та легальність використання на території Україїни або інших держав.

Міжмережевий екран є системою або комбінацією систем, що утворює між двома або більше мережами захисний бар'єр, оберігає від несанкціонованого попадання в мережу або виходу з неї пакетів даних. Основний принцип дії міжмережевих екранів - перевірка кожного пакета даних на відповідність вхідної та вихідної IP-адреси на базі дозволених адрес. Таким чином, міжмережові екрани значно розширюють можливості сегментування інформаційних мереж та контролю за циркулюванням даних.

Говорячи про криптографію та міжмережевих екранів, слід згадати про захищені віртуальні приватні мережі (Virtual Private Network - VPN). Їх використання дозволяє вирішити проблеми конфіденційності та цілісності даних при їх передачі по відкритих комунікаційних каналів. Використання VPN можна звести до вирішення трьох основних завдань:

- захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу);
- захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, що здійснюється через інтернет;
- захист інформаційних потоків між окремими програмами всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється із внутрішніх мереж).

Ефективний засіб захисту від втрати конфіденційної інформації – фільтрація вмісту вхідної та вихідної електронної пошти. Перевірка самих поштових повідомлень та вкладень у них на основі правил встановлених в організації, дозволяє також убезпечити компанії від відповідальності за судовими позовами та захистити їх від спаму. Засоби контентної фільтрації дозволяють перевіряти файли всіх поширених форматів, зокрема стислі та графічні. При цьому пропускна здатність мережі практично не змінюється.Усі зміни на робочій станції або сервері можуть бути відстеженні адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диска (Integrity checking). Це дозволяє виявляти будь-які дії з файлами (зміна, видалення

або просто відкриття) та ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль складає основу аналізу контрольних сум файлів (CRC-сум).

Сучасні антивірусні технології дозволяють виявити практично всі відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворені вірусні програми. Об'єкти, що виявляються, можуть піддаватися лікуванню, ізолюватися (поміщатися в карантин) або видалятися. Захист від вірусів може бути встановлений на робочі станції, файлові та поштові сервери, міжмережні екрани, які працюють практично з будь-якою поширеною операційною системою (Windows, Unix-і Linux-системи, Novell) на процесорах різних типів.

Фільтри спаму значно зменшують непродуктивні трудовитрати, пов'язані з розбором спаму, знижують трафік та завантаження серверів, покращують психологічний фон у колективі та зменшують ризик залучення співробітників компанії до шахрайських операцій. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси (навіть ще не ввійшли до баз антивірусних програм) часто мають ознаки спаму та відфільтровуються. Правда, позитивний ефект від фільтрації спаму може бути перекреслено, якщо фільтр разом зі сміттєвими видаляє або маркує як спам корисні повідомлення, ділові чи особисті.

Величезні збитки компаніям, завдані вірусами та хакерськими атаками – великою мірою наслідок слабких місць у програмному забезпеченні. Визначити їх можна завчасно, не чекаючи реального нападу, за допомогою систем виявлення вразливостей комп'ютерних мереж та аналізаторів атак. Подібні програмні засоби безпечно моделюють поширені атаки та способи вторгнення визначають, що саме хакер може побачити у мережі та як він може використовувати ці ресурси.

Для протидії природним загрозам інформаційної безпеки в компанії повинен бути розроблений та реалізований набір процедур щодо запобігання надзвичайним ситуаціям (наприклад, щодо забезпечення фізичного захисту даних від пожежі) та мінімізації збитків у тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних – резервне копіювання із чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій тощо).

Безпека інформаційної системи залежить від оточення, де вона функціонує. Необхідно вжити заходів для захисту будівель та прилеглої території, підтримуючої інфраструктури, обчислювальної техніки, носіїв даних.

Розглянемо такі напрямки фізичного захисту:

- фізичне управління доступом;
- захист підтримуючої інфраструктури;
- захист мобільних систем.

Заходи фізичного управління доступом, дозволяють контролювати і за необхідності обмежувати вхід та вихід співробітників та відвідувачів. Контролюватися може вся будівля організації, а також окремі приміщення, наприклад, де розташовані сервери, комунікаційна апаратура тощо.

До підтримуючої інфраструктури можна віднести системи електро-, водо- та теплопостачання, кондиціонери та засоби комунікацій. У принципі, до них застосовні ті самі вимоги цілісності і доступності, як і до інформаційних систем. Для забезпечення цілісності необхідно захищати обладнання від крадіжок та пошкоджень. Для підтримки доступності слід вибирати обладнання з максимальним часом напрацювання на відмову, дублювати відповідальні вузли та завжди мати під рукою запчастини.

Загалом кажучи, при виборі засобів фізичного захисту слід проводити аналіз ризиків. Так, приймаючи рішення про закупівлю джерела безперебійного живлення, необхідно врахувати якість електроживлення в будівлі, характер і

тривалість збоїв електроживлення, вартість доступних джерел та можливі втрати від аварій (поломка техніки, призупинення роботи організації тощо)

Розглянемо низку заходів, вкладених у підтримку працездатності інформаційних систем. Саме в цій галузі таїться найбільша небезпека. До втрати працездатності, а саме пошкодження апаратури, руйнування програм та даних можуть призвести ненавмисні помилки системних адміністраторів та користувачів.

Основна проблема багатьох організацій – недооцінка факторів безпеки у повсякденній роботі. Дорогі засоби безпеки втрачають сенс, якщо вони погано документовані, конфліктують з іншим програмним забезпеченням, а пароль системного адміністратора не змінювався з моменту встановлення.

Для повсякденної діяльності, спрямовані на підтримку працездатності інформаційної системи можна назвати такі дії:

- підтримка користувачів;
- підтримка програмного забезпечення;
- конфігураційне управління;
- резервне копіювання;
- керування носіями;
- документування;
- регламентні роботи.

Підтримка користувачів мається на увазі, перш за все, консультування та надання допомоги при вирішенні різноманітних проблем. Дуже важливо у потоці питань уміти виявляти проблеми, пов'язані з інформаційною безпекою. Труднощі користувачів, що працюють на персональних комп'ютерах можуть бути наслідком зараження вірусами. Доцільно фіксувати питання користувачів, щоб виявляти їх типові помилки та випускати пам'ятки із рекомендаціями для поширених ситуацій.

Підтримка програмного забезпечення - один із найважливіших засобів забезпечення цілісності інформації.

Перш за все, слід стежити за тим, яке програмне забезпечення інстальовано на комп'ютерах. Якщо користувачі встановлюватимуть програми на свій розсуд, це може призвести до зараження вірусами, а також появи утиліт, що діють в обхід захисних засобів. Цілком ймовірно також, що "самодіяльність" користувачів поступово призведе до хаосу на їх комп'ютерах, а виправляти ситуацію доведеться системному адміністратору.

Другий аспект підтримки програмного забезпечення – контроль за відсутністю неавторизованої зміни програм та прав доступу до них. Сюди можна віднести підтримку еталонних копій програмних систем. Зазвичай контроль досягається комбінуванням засобів фізичного та логічного управління доступом, а також використанням утиліт перевірки та забезпечення цілісності.

Конфігураційне управління дозволяє контролювати та фіксувати зміни, що вносяться до програмної конфігурації. Насамперед, необхідно застрахуватися від випадкових чи непродуманих модифікацій, вміти як мінімум повертатися до минулої працюючої версії. Фіксація змін дозволить легко відновити поточну версію після аварії.

Найкращий спосіб зменшити кількість помилок у рутинній роботі – максимально автоматизувати її. Автоматизація та безпека залежать один від одного, адже той, хто дбає насамперед про полегшення свого завдання, насправді оптимальним чином формує режим інформаційної безпеки.

Резервне копіювання необхідно для відновлення програм та даних після аварій. І тут доцільно автоматизувати роботу, як мінімум, сформувавши комп'ютерний розклад створення повних та інкрементальних копій, а як максимум – скориставшись відповідними програмними продуктами. Потрібно також налагодити розміщення копій у безпечному місці, захищеному від несанкціонованого доступу, пожеж, протікання, тобто всього, що може призвести до крадіжки або пошкодження носіїв. Доцільно мати кілька екземплярів резервних копій частину з них зберігати поза територією організації, захищаючись таким

чином від великих аварій та аналогічних інцидентів. Іноді в тестових цілях слід перевіряти можливість відновлення інформації з копій.

Керувати носіями необхідно для забезпечення фізичного захисту та обліку дискет, стрічок, друкованих видач тощо. Керування носіями має забезпечувати конфіденційність, цілісність та доступність інформації, що зберігається поза комп'ютерними системами.

Під фізичним захистом тут розуміється як відображення спроб несанкціонованого доступу, а й захист від шкідливих впливів довкілля (спеки, холоду, вологи, магнетизму). Управління носіями має охоплювати весь життєвий цикл – від закупівлі до виведення з експлуатації.

Документування – невід'ємна частина інформаційної безпеки. У вигляді документів оформляється майже все - від безпекової політики до журналу обліку носіїв. Важливо, щоб документація була актуальною, відображала саме поточний стан справ, причому у несуперечливому вигляді.

До зберігання одних документів (що містять, наприклад, аналіз уразливих місць системи та загроз) застосовні вимоги забезпечення конфіденційності, до інших, таких як план відновлення після аварій – вимоги цілісності та доступності (у критичній ситуації план необхідно знайти та прочитати).

Регламентні роботи – дуже серйозна загроза безпеці. Співробітник, який здійснює регламентні роботи, отримує винятковий доступ до системи, і це практично дуже важко проконтролювати, які саме дії він робить. Тут на перший план виходить ступінь довіри до тих, хто виконує роботу.

Політика безпеки, прийнята в організації, має передбачати набір оперативних заходів, спрямованих на виявлення та нейтралізацію порушень режиму інформаційної безпеки.

Важливо, щоб у подібних випадках послідовність дій була спланована заздалегідь, оскільки заходи слід вживати термінових та скоординованих.

Реакція на порушення режиму безпеки має такі головні цілі:

- локалізація інциденту та зменшення шкоди, що завдається;
- запобігання повторних порушень.

Нерідко вимога локалізації інциденту і зменшення шкоди, що завдається, вступає в конфлікт з бажанням виявити порушника. У безпековій політиці організації пріоритети мають бути розставлені заздалегідь. Оскільки, як показує практика, виявити зловмисника дуже складно, насамперед слід дбати про зменшення шкоди. Жодна організація не застрахована від серйозних аварій, спричинених природними причинами, діями зловмисника, недбалістю чи некомпетентністю. У той самий час, кожна організація має функції, які керівництво вважає критично важливими, вони мають виконуватися попри що. Планування відновлювальних робіт дозволяє підготуватися до аварій, зменшити збитки від них та зберегти здатність до функціонування хоча б у мінімальному обсязі. Зазначимо, що заходи інформаційної безпеки можна розділити на три групи, залежно від того спрямовані вони на попередження, виявлення чи ліквідацію наслідків атак. Більшість заходів має запобіжний характер.

Процес планування відновлювальних робіт можна поділити на такі етапи:

- виявлення критично важливих функцій організації; встановлення пріоритетів;
- ідентифікація ресурсів, необхідні виконання критично важливих функцій;
- визначення переліку можливих аварій;
- розробка стратегії відновлювальних робіт;
- підготовка до реалізації обраної стратегії;
- перевірка стратегії.

Плануючи відновлювальні роботи, слід усвідомлювати, що повністю зберегти функціонування організації не завжди можливо. Необхідно виявити критично важливі функції, без яких організація втрачає своє обличчя, і навіть серед

критичних функцій розставити пріоритети, щоб як найшвидше мінімальними витратами відновити роботу після аварії.

Ідентифікуючи ресурси, необхідних для виконання критично важливих функцій, слід пам'ятати, частина з них має некомп'ютерний характер. На цьому етапі бажано підключати до роботи спеціалістів різного профілю. Таким чином, існує велика кількість різних методів забезпечення інформаційної безпеки. Найбільш ефективним є застосування всіх даних методів у єдиному комплексі.

Сьогодні сучасний ринок насичений засобами забезпечення інформаційної безпеки. Постійно вивчаючи існуючі пропозиції ринку безпеки, багато компаній бачать неадекватність раніше вкладених коштів у системи інформаційної безпеки, наприклад, через моральне старіння обладнання та програмного забезпечення. Тому вони шукають варіанти вирішення цієї проблеми. Таких варіантів може бути два: з одного боку – це повна заміна системи корпоративного захисту інформації, що вимагатиме великих капіталовкладень, а з іншого – модернізація існуючих систем безпеки.

Останній варіант вирішення цієї проблеми є найменш витратним, але несе нові проблеми, наприклад, вимагає відповіді на такі питання:

Як забезпечити сумісність старих, що залишаються з апаратно – програмних засобів безпеки та нових елементів системи захисту інформації? Як забезпечити централізоване управління різнорідними засобами забезпечення безпеки? Як оцінити, а за необхідності і переоцінити інформаційні ризики компанії?

РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ КОНТРОЛЮ РОБОТИ ІТ-КОМПАНІЇ ЗА ДОПОМОГОЮ АУДИТУ

Світовою практикою визначено, що аудит виступає складовою частиною процесу стратегічного управління підприємством. З року в рік все більшої популярності набуває використання послуг аудиту серед сучасних суб'єктів господарювання. Важливо те, що аудит дозволяє формувати висновки про реальний стан захисту ІТ-ресурсів, а також рівень їх здатності протистояти внутрішнім та зовнішнім загрозам, що виникають у середовищі функціонування. Під ІТ-компанією мається на увазі – компанія яка використовує систему методів і способів збору, передачі, накопичення, опрацювання, зберігання, подання і використання інформації.

Інформаційні технології на підприємствах поділяються на:

- технології автоматизації офісу;
- інформаційні технології обробки даних;
- інформаційні технології управління;
- інформаційні технології підтримки прийняття управлінських рішень;
- інформаційні технології експертних систем

ІТ-аудит (аудит інформаційних технологій) – це незалежна перевірка (експертиза) аудитором (компетентним фахівцем або групою фахівців) ІТсередовища підприємства з метою отримання повної та об'єктивної інформації (достовірних фактів, якісних і кількісних оцінок) про його поточний стан (даної підсистеми підприємства), формування об'єктивного аудиторського висновку, а також надання рекомендацій щодо удосконалення ІТ-середовища.

Отже, ІТ-аудит являє собою процес формування висновків у аудитора та надання їх замовнику (підприємству) стосовно стану тої інформаційної системи, яка виступає об'єктом аудиту. Внаслідок отриманих під час аудиторської перевірки даних формуються рекомендації по удосконаленню ІТ-середовища, у якому функціонує замовник.

Практика показує, що аудит інформаційних систем поділяється на декілька напрямків, зокрема:

- аудит технічного стану (націлений на скорочення витрат, що спричинені збоями);
- аудит інформаційної безпеки (дозволяє сформувати оптимальну систему захисту інформації, що відповідатиме цілям та меті діяльності підприємства);
- оціночний аудит програмного забезпечення (спрямований на встановлення рівня економічної ефективності від упровадження та експлуатації програмного забезпечення);
- оціночний аудит інформаційних систем (передбачає виявлення відхилень фактичних результатів від очікуваних);
- аудит проектів упровадження і реінжинірингу (націлений на оцінку ризиків упровадження чи реінжинірингу інформаційної системи);
- аудит ефективності інформаційної системи (дозволяє оцінити сумарну вартість оволодіння інформаційною системою підприємством та порівняти її з показниками лідерів, що функціонують у цьому конкурентному середовищі).

Окрім того, ІТ-аудит поділяється на внутрішній аудит та зовнішній аудит.

3.1 Внутрішній ІТ-аудит

Внутрішній контроль на підприємстві – це процес, що повинен реалізовуватися постійно повноважними органами управління (починаючи з наглядової ради, менеджерів усіх рівнів) і співробітників підприємства із застосуванням певних процедур і методів контролю на базі доступної інформації. Цілі, завдання та елементи системи внутрішнього контролю можливо представити таким чином Рис. 3.1

Рисунок 3.1. Цілі, завдання та елементи внутрішнього контролю підприємства

Внутрішній ІТ-аудит є одним із видів внутрішньогосподарського (управлінського) контролю організацій і може розглядатись як невід'ємна частина загальної системи управління. Замовником у такому випадку є сама організація (в особі її вищого керівництва), ІТ-середовище яке підлягає аудиту, а виконавцем є спеціальний підрозділ в організації – служба внутрішнього ІТ-аудиту (СВ- ІТ-аудиту). Такий підрозділ повинен мати достатньо незалежний статус в організації

для надання максимально об’єктивних аудиторських висновків вищому керівництву. Внутрішні аудитори не зобов’язані бути сертифікованими для проведення такої діяльності (мати сертифікат аудитора).

Підпорядковуючись вищому керівництву організації, СВ- ІТ-аудиту у своїй діяльності керується внутрішньою політикою, правилами й іншими положеннями щодо виконання своїх обов’язків в організації (зокрема, щодо об’єктів і методів аудиту, звітності тощо), які, як правило, узгоджуються і фіксуються у вигляді внутрішньої угоди довільного зразка.

Внутрішній ІТ-аудит, зазвичай проводиться на постійній основі з метою неперервного удосконалення ІТ-середовища, підвищення зрілості ІТ-процесів, гарантування надійності та ефективності заходів ризик-менеджменту ІТ, а також обґрунтування відповідних інвестицій організації тощо.

Однак він також може виконуватись періодично, наприклад, з метою економії часових й інших ресурсів зовнішнього аудиту, оскільки внутрішні аудитори краще знають організацію, в якій працюють. Як засвідчує практика функціонування сучасних підприємств, однією із причин утримання або відтермінування ІТ-аудиту виступає вартість послуг, якщо підприємство використовуватиме послуги зовнішніх аудиторів. Однак, що стосується внутрішнього аудиту, то тут можливо є такий варіант, залучити свого працівника, оскільки підприємство стовідсотково довіряє йому проведення цього виду аудиту.

3.2 Зовнішній ІТ-аудит

Зовнішній ІТ-аудит є консалтинговою послугою, яка застосовується в системі управління організацією, як правило, на періодичній основі з метою отримання незалежного професійного висновку стосовно поточного стану ІТ-середовища, його сильних і слабких сторін, а також рекомендацій щодо його удосконалення. Замовником у такому випадку може бути як сама організація (в особі її вищого керівництва), ІТ-середовище яке підлягає аудиту, так і третя сторона – контрагент, орган сертифікації тощо. Виконавцем є зовнішня організація

(приватна аудиторська фірма, діяльність якої регламентується юридично), сертифікована уповноваженим державою органом для професійного здійснення такої діяльності (надання таких послуг).

Діяльність зовнішнього аудитора регулюється чинним Законодавством, а також вищими органами державного нагляду за здійсненням аудиторської діяльності (наприклад, в Україні – це Аудиторська палата України – АПУ), на підставі затверджених на національному рівні відповідних стандартів, кодексу професійної етики, інструкцій та інших положень.

Підставою для проведення зовнішнього ІТ-аудиту є двосторонній договір, складений за формою і вимогами національних нормативів (стандартів) аудиту. У договорі про ІТ-аудит обов'язково узгоджуються та фіксуються його мета, цілі, об'єкти, завдання, питання, відповідальність і повноваження сторін, а також інші організаційні та юридичні аспекти.

На відміну від внутрішнього ІТ-аудиту, за результати якого виконавець несе відповідальність безпосередньо перед вищим керівництвом організації, виконавець зовнішнього ІТ-аудиту за поданий замовнику висновок несе юридичну відповідальність. Нині найбільш розповсюдженими є два основні способи застосування зовнішнього ІТ-аудиту в системі управління організацією: як самостійної консалтингової (аудиторської) послуги, або у складі інших видів аудиту організацій (комбінований аудит).

Як самостійна консалтингова послуга зовнішній аудит інформаційних технологій застосовується з метою отримання аудиторського висновку щодо поточного стану об'єкта аудиту (відповідно до визначених цілей, завдань і обмежень аудиту) забезпеченого аудиторськими доказами і свідоцтвами. У складі інших видів аудиту організацій, ІТ-аудит застосовується як правило, з метою дослідження тих аспектів господарської діяльності об'єкта аудиту, які потребують спеціальних знань і навичок у сфері ІТ, і надання у такий спосіб додаткової

впевненості щодо якості і достовірності результатів аудиту, у межах якого він був залучений. Наприклад, у межах фінансового аудиту організації IT-аудит застосовують для підтвердження достовірності та захищеності даних в інформаційних системах, перевірки рівня автоматизації бізнес-процесів, їх надійності та відповідності стандартам інформаційної безпеки тощо. Перед тим, як проводити IT-аудит, необхідно першочергово зібрати інформацію про такі факти, як:

- вид діяльності та рівень ефективності функціонування підприємства;
- стан цільового ринку підприємства, взаємовідносини із споживачами та клієнтами;
- рівень управління організаційною культурою підприємства;
- стратегічні цілі та майбутнє бачення діяльності.

Результати доводять, що аудиторський висновок дає можливість оцінити поточний рівень і стан діяльності підприємства, визначити недоліки та встановити ризики із перспективою їх подальшого усунення.

3.3 Алгоритм проведення аудиторської перевірки

Алгоритм проведення аудиторської перевірки охоплює п’ять етапів:

1) етап попередньої діагностики, яка необхідна для встановлення видів, термінів здійснення та вартості IT-аудиту (передбачає збір інформації про підприємство, на основі якої встановлюються ключові проблеми у IT-сфері та представляються пропозиції щодо їх вирішення);

2) етап аудиту IT-інфраструктури, який необхідний для одержання точної та правдивої інформації щодо поточного стану інфраструктури упроваджених інформаційних технологій на підприємстві (передбачає визначення сильних та слабких сторін інфраструктури упроваджених інформаційних технологій, рівня ефективності функціонування, що дозволять виділити та представити професійні рекомендації стосовно удосконалення IT-інфраструктури підприємства);

3) етап аудиту ІТ-підрозділу, який необхідний для одержання точної та правдивої інформації щодо поточного стану підрозділу, який спеціалізується на управлінні інформаційними технологіями (передбачає виявлення сильних та

слабких сторін підрозділу, що відповідає за управління інформаційними технологіями, які дозволять виділити та представити професійні рекомендації стосовно удосконалення ІТ-підрозділу підприємства);

4) етап ІТ-безпеки, який необхідний для одержання точної та правдивої інформації щодо стану інформаційної безпеки підприємства, його сильних та слабких сторін, рівня ефективності функціонування з метою розроблення та впровадження рекомендацій удосконалення ІТ-безпеки підприємства;

5) етап контролю за впровадженням рекомендацій ІТ-аудиту (проводиться із ціллю забезпечення контролю і підтримки упровадження результатів, отриманих за рахунок здійснення ІТ-аудиту його замовником).

3.4 Аудит, як форма контролю роботи ІТ-компанії

Аналізуючи результати аудиту ІТ-компанії, отримуємо рекомендації щодо коригувальних заходів, які необхідно виконати для усунення виявлених недоліків, невідповідностей вимогам внутрішніх політик і правил бізнесу чи вимогам еталону, обраного для порівняння.

Контроль роботи підприємства через ІТ-аудит, призначено для використання як відповідні аудиторські свідоцтва у подальших етапах керування и для формування на їх основі висновку та рекомендацій щодо поточного стану ІТ-середовища організації. Контроль за допомогою внутрішнього чи зовнішнього ІТ-аудиту залежить від ініціатора аудиту (зацікавленої сторони у його проведенні), цілей аудиту (складності питань і завдань аудиту, необхідності застосування спеціальних методів, моделей тощо), кваліфікації виконавця (рівня професійності, незалежності, об’єктивності тощо), вартості, вагомості аудиторського висновку для зацікавлених сторін (рівня довіри замовника аудиту до його виконавця) тощо.

Незалежно від того, хто виконує ІТ-аудит, технологія його проведення і кінцевий результат можуть бути ідентичними або різними. Розглянемо складники контролю за допомогою внутрішнього та зовнішнього аудиту (табл. 3.1).

Таблиця 3.1. – Складники контролю за допомогою внутрішнього та зовнішнього аудиту

Ознака	**Зовнішній ІТ-аудит**	**Внутрішній ІТ-аудит**
Мета	Отримання незалежного професійного висновку щодо стану ІТ-середовища, його сильних і слабких сторін, а також рекомендацій стосовно його покращення	Постійне удосконалення ІТ-середовища, підвищення зрілості ІТ-процесів, гарантування надійності та ефективності заходів ризик-менеджменту ІТ, а також обґрунтування відповідних інвестицій тощо
Масштаб	Вибірковий	Повний
Замовник	Вище керівництво об’єкта аудиту, контрагенти, власники, інвестори, регулюючі органи тощо	Вище керівництво об’єкта аудиту, акціонери
Виконавець	Приватна аудиторська фірма або аудитор-підприємець	Спеціальний підрозділ організації (служба внутрішнього ІТ-аудиту)
Підстава для проведення	Договір між замовником аудиту і виконавцем	Положення про службу внутрішнього ІТ-аудиту, узгоджений план аудиторських перевірок, наказ керівництва тощо
Правове регулювання відносин між сторонами	Відносини регулюються юридичними нормами цивільного законодавства на засадах партнерства і рівності сторін	Відносини регулюються нормами законодавства про працю. Наявна субординація виконавця перед вищим керівництвом замовника аудиту

Залежність від національних стандартів аудиту	Обов’язкове дотримання і використання у роботі	На рівні рекомендацій
1	2	3
Оплата послуг	Оплата консалтингових послуг за умовами укладеного господарського договору про ІТ-аудит	Заробітна плата за трудовою угодою
Результат	Аудиторський висновок за формою і вимогами національних стандартів аудиту	Акти, звіти, рекомендації тощо, визначені внутрішніми угодами (Положенням про СВ- ІТ-аудиту)
Незалежність	Висока	Середня або низька
Регулярність	Періодична - залежить від потреб замовника аудиту (зацікавлених сторін)	Неперервний процес
Знання бізнесу замовника	Середні (є потреба у тривалому вивченні особливостей бізнесу замовника)	Високі (це обумовлено безперервним процесом аудиту, структурною приналежністю до об’єкта аудиту)

Також використовується аудит інформаційних технологій за ініціацією, тобто, виходячи із причин, які спонукали до проведення аудиту. Контроль готовності до інновацій за допомогою аудиту інформаційних технологій є невід'ємною частиною розвитку ІТ-компанії. Наведемо варіанти таких заходів (табл. 3.2).

Таблиця 3.2 – Контроль готовності до інновацій за допомогою аудиту інформаційних технологій

Вид ІТ-аудиту	Характеристика
Аудит перед сертифікацією	Може проводитись на відповідність різноманітним стандартам (COBIT, ISO 20000x тощо). Застосування такого аудиту потребують, наприклад, сервісні ІТ-компанії, а також організації, які планують вийти на міжнародний ринок співпраці.
1	2
Аудит перед реструктуризацією ІТ-підрозділів	Проводиться, наприклад, холдингами при купівлі нових компаній з метою визначення раціональної процедури інтеграції їх інформаційних технологій з ІТ-середовищем головної, а також отримання рекомендацій щодо ефективної організації ІТ-підрозділу.
Аудит перед впровадженням інформаційної системи	Виконується перед початком проектів модернізації або впровадження в організації інформаційних систем чи інших комплексних ІТ рішень. При проведенні такого аудиту обстеження ІТ-середовища організації завершує собою певний етап його розвитку. Виконується оцінювання й аналіз поточного стану інформаційних систем та ІТ-середовища в цілому, з метою формування обґрунтованого плану впровадження змін для досягнення стратегічних цілей його розвитку.
Аудит перед впровадженням систем управління конфігурацією або ІТ-активами	Проводиться перед впровадженням в організації автоматизованих засобів, обліку активів ІТ-середовища, зокрема, з метою визначення найбільш критичних напрямків такого контролю в організації.

3.5 Система контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту

Проаналізувавши ІТ-ризики та аудит, як форму контролю, пропонується наступна система технічного контролю роботи ІТ-компанії (табл. 3.3). Як видни із таблиці, вид техничного контролю описується характеристикой мети аудиту.

Таблиця 3.3 Система технічного контролю роботи IT-компанії за допомогою аудиту

Вид технічного контролю	**Характеристика мети аудиту**
Обстеження IT	Проводиться з метою збору інформації, яка буде використовуватись в інших роботах, наприклад, у межах проекту впровадження нової інформаційної системи. Послуга потрібна, якщо необхідно зібрати достовірну інформацію про поточний стан IT-середовища.
Експертна оцінка IT	Проводиться з метою перевірки адекватності фінансування IT-проектів, а також витрат на обладнання та IT-послуги. Виконується оцінювання й аналіз запланованих і поточних IT-проектів, IT-бюджету, вартості володіння IT-середовищем тощо.
Технічний аудит IT	Проводиться з метою збору, оцінювання й аналізу інформації щодо конкретних технічних елементів IT-середовища, а також надання рекомендацій для покращення їх роботи.
IT-аудит бізнес-процесу	Проводиться з метою перевірки інформаційних технологій, які є критичними для виконання конкретних бізнес-процесів за визначеними критеріями (якість, ефективність, економічність тощо). Для цього встановлюються власники, оператори і клієнти бізнес-процесів, а також оцінюються й аналізуються IT, дії учасників процесу, проектна документація тощо.
IT-аудит за критеріями	Проводиться з метою збору, оцінювання й аналізу інформації щодо стану IT-середовища об'єкта аудиту за певним обраним критерієм (безпека, надійність, доступність тощо), а також надання відповідних рекомендацій щодо удосконалення.
Комплексний IT-аудит	Проводиться з метою комплексного дослідження відповідності IT-середовища організації стратегії, цілям і процесам бізнесу.

Також пропонується система економічного контролю IT-компанії (табл. 3.4).

Таблиця 3.4 Система економічного контролю роботи IT-компанії за допомогою аудиту

Вид економічного контролю	**Характеристика дій аудиту**
Аудит цифрових методів контролю	Детальна перевірка ручних й автоматизованих IT-контролів з метою оцінити рівень достовірності виконаних транзакцій і звітів, що були згенеровані відповідними системами.
Аудит фінансових систем	Аудит фінансових звітів, оброблених або згенерованих IT-системами, з представленням аудиторського висновку.
Аудит ефективності та економічності IT-систем	Перевірка систем з метою оцінити, чи ефективно досягаються очікувані цілі від їх впровадження, зокрема, відповідно до вимог їх ефективності й економічності.
Аудит систем, що розробляються	Аудит, який проводиться з метою оцінити: чи виконано планування, проектування та розроблення інформаційних систем у чітко структурованому порядку, контрольованому середовищі, а також у відповідності до вимог певної методології; чи продумано адекватні й ефективні контролі на кожній стадії процесу розроблення тощо.

Запропонована система контролю роботи IT-компанії за допомогою внутрішнього та зовнішнього аудиту, включає в себе дві складові:

- систему технічного контролю роботи IT-компанії за допомогою аудиту;
- систему економічного контролю роботи IT-компанії за допомогою аудиту

Слід також зазначити, що рішення про необхідність внутрішнього аудиту не повинне визначатися наявністю в компанії зовнішнього аудитора, оскільки зовнішній і внутрішній аудит виконують різні функції.

По-перше, зовнішній аудит традиційно займається підтвердженням

достовірності фінансової звітності підприємства й фокусується на операціях і подіях, здатних спричинити матеріальний вплив на фінансову звітність підприємства. Внутрішній аудит спрямований, насамперед, на оцінку існуючих систем контролю й управління ризиками підприємства й фокусується на операціях і подіях, що перешкоджають ефективному досягненню підприємством поставлених цілей.

По-друге, зовнішній аудит відповідає головним чином інтересам зовнішніх зацікавлених сторін – потенційних інвесторів, кредиторів та ін., у той час як внутрішній аудит служить інтересам наглядової раді (комітету з аудиту) і менеджменту підприємства.

По-третє, зовнішній аудит у рамках надання аудиторських послуг не дає оцінку економічної обґрунтованості управлінських рішень й ефективності діяльності підрозділів підприємства, що звичайно є одним із завдань аудиту внутрішнього.

Ефективний внутрішній аудит може знизити витрати підприємства на зовнішній аудит: якщо зовнішній аудитор буде мати можливість покладатися на результати роботи внутрішнього аудиту, це, не скасовуючи необхідності зовнішнього аудиту для підприємства, скоротить обсяг аудиторських процедур, які виконуються зовнішнім аудитором. У межах внутрішнього аудиту здійснюється не лише контроль збереження активів, збільшення доходів, захист майнових інтересів власника, але й контроль за політикою та якістю менеджменту.

Економічна частина

Метою даних розрахунків є обчислення вартості виконання науково-дослідної роботи « Розробка системи контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту».

Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення. Розрахунок трудомісткості НДР здійснений в наступній послідовності:

1) Складений перелік всіх етапів і видів робіт, які необхідно виконати в ході даної НДР. Після узгодження з керівником проекту допущено виключення, доповнення, об'єднання окремих етапів і видів робіт;

2) По кожному виду робіт визначений кваліфікаційний рівень виконавців.. Розподіл робіт по етапах і видах виконавців вироблений формою, наведено в таблиці 5.1.

Розподіл робіт по етапах і видах виконавців

Таблиця 5.1.

Етап проведення НДР	**Вигляд робіт**	**Посада виконавця**
Розробка технічного завдання (ТЗ)	1.Складання і затвердження ТЗ для НДР «Розробка системи контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту»	Дипломник, керівник
Вибір напряму дослідження	1. Збір і вивчення науково-технічної літератури. 2. Формулювання можливих напрямів вирішення завдань,	Дипломник керівник

	поставлених в технічному завданні НДР . 3. Вибір напряму проведення досліджень для подальшої розробки. 4. Розробка плану проведення досліджень для подальшої розробки.	
Теоретичні і експериментальні дослідження	1. СКЛАДНИКИ КОНТРОЛЮ РОБОТИ ІТ-КОМПАНІЇ 2. ПОЛІТИКА БЕЗПЕКИ ІТ-КОМПАНІЇ 3. РОЗРОБКА СИСТЕМИ КОНТРОЛЮ РОБОТИ ІТ-КОМПАНІЇ ЗА ДОПОМОГОЮ АУДИТУ 4. ЕКОНОМІЧНІ РОЗРАХУНКИ 5. ОХОРОНА ПРАЦІ. 6. ВИСНОВОК	Дипломник керівник консультанти
Узагальнення і оцінка результатів досліджень	1. Узагальнення результатів попередніх етапів роботи. 2. Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття результатів в цілому.	Дипломник керівник консультанти

Очікувана трудомісткість робіт.

Таблиця 5.2.

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР « Розробка системи контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту»	1
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	3
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	3
4. Вибір напряму проведення досліджень і способів вирішення поставлених завдань. Розробка плану проведення досліджень для подальшої розробки.	2
5. Визначення складників контролю роботи ІТ компанії.	2
6. Розбір аудиту як форми контролю.	4
7. Написання частини з економічних розрахунків та охорони праці.	5
8. Оформлення роботи.	4
Всього:	24

Результатом виконання НДР є науково-технічна продукція, що є закінчені науково – дослідницькі роботи, виконані відповідно до вимог, передбачених договором, і прийнятими замовником. Розрахунок собівартості і ціни виконання НДР включає наступні статті витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями, і деякі інші.

1) Витрати на матеріали, купувальні комплектуючі, напівфабрикати визначають на основі розрахунку потреби в них за оптовими цінами, що діють і складають (ПАПІР формат А4 + друк) приблизно 150-200 грн (115,50*~1,50 грн диплом + >30 грн сшивання).

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної зарплати встановлюється виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за один робочий день. Відповідно до статті 8 «Закону про Державний бюджет України на 2022» встановлено мінімальну заробітну плату у місячному розмірі з 1 січня 2022 року - 6500 гривень; мінімальну погодинну тарифну ставку – 39,26 грн.

Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

$$Зден= п.т.с. * 8;$$

де п.т.с – погодинна тарифна ставка, грн..;

8 – тривалість робочого дня,год.

Зден дипломника = 39.26*8 = 314,08 грн.

Зден керівника = 60 * 8 = 480 грн.

Зден консультантів = 50 *8= 400грн.

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в таблиці 5.3.

Витрати на основну заробітну плату.

Таблиця 5.3.

Виконавець	**Погодинна тарифна ставка, грн**	**Денна ставка, грн**	**Трудомісткість робочих днів**	**Сума основної зарплати, грн**
Дипломник	39,26	314.08	20	6281,6
Керівник	60	480	1	480
Консультант по економічній частині	50	400	0,25	100
Консультант по охороні праці	50	400	0,25	100
Нормоконтроль			0,25	
Всього (Зо)	6961,6			

3) Витрати на додаткову заробітну плату визначаються у відсотках від основної і враховують виплати за час, що не пропрацював, встановлений законом. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

$$Зд=10\%Зо= 10\% * 6961,6 = 696,16 \text{ грн};$$

4)До складу собівартості НДР включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Відрахування до єдиного соціального внеску складає.

Зєсв=0,22*(Зо+Зд)= 0,22*(6961,6+696,16) = 1684,7 грн;

5) До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР.. У наукових закладах накладні витрати складають 40 -120% від основної і додаткової заробітної плати.

Рнакл= (Зо+Зд)*0,4= (6961,6+696,16)*0,4= 3063,104 грн;

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 5.4.

Калькуляція планової собівартості

Таблиця 5.4.

Статті витрат	Сума, грн.
1. Матеріали	*150*
2. Основна заробітна плата	*6961,6*
3. Додаткова заробітна плата	*696,16*
4. Відрахування до єдиного соціального внеску	*1684,7*
5. Накладні витрати	*3063,104*
Планова собівартість (Спл)	12555,5

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл=0,1*12555,5= 1255,55 грн

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції.

Договірна ціна визначається по формулі:

$$Цнір = Спл + Ппл = 12555+1255,55= 13811,05 \text{ грн}$$

Звідси ціна реалізації становить:

$$Цр = Цнір + ПДВ= Цнір+ Цнір*0,2 = 13811,05 + 13811,05*0,2= 13811,05 + 2762,21= 16573,26 \text{ грн.}$$

Розділ «Охорона праці»

1. Вступ

2. Аналіз та забезпечення безпеки умов праці.

2.1. Організація робочого місця.

2.2. Основні вимоги безпеки до мікроклімату виробничих приміщень, освітлення.

2.3. Шум, вібрація, ультразвук, інфразвук.

2.4. Небезпека ураження електричним струмом.

3. Розробка заходів з охорони праці.

4.Значення пожежної безпеки.

5. Висновок.

1.ВСТУП

Соціальне значення охорони праці полягає у сприянні зростанню ефективності суспільного виробництва шляхом безперервного вдосконалення і поліпшення умов праці, підвищення її безпеки на робочому місці, зниження захворюваності та випадків травматизму на роботі.

Окрім соціального, охорона праці має, безперечно важливе економічне значення – це зниження витрат на виплату зарплатні та лікарняних, компенсацій за важкі та шкідливі умови праці, а також висока продуктивність.

В даній дипломній праці розглядається питання контролю часу та підвищення ефективності його використання в IT-компанії. Програмний комплекс являє собою вдосконалений метод планування та управління проектом разом із програмним забезпеченням, що полегшує його використання в подальшому.

2.Аналіз та забезпечення безпека умов праці

Несприятливу дію шкідливих факторів виробничого середовища на здоров'я працівників і викликані ними професійні захворювання можемо розділити на п'ять груп:

1. Захворювання, викликані фізичними факторами
2. Захворювання, викликані дією хімічних факторів органічного пилу.
3. Захворювання, викликані дією біологічних факторів.
4. Захворювання під дією психофізіологічних шкідливих факторів
5. Захворювання шкіри алергійного і не алергійного характеру.

В кожному виробничому середовищі на організм людини одночасно можуть діяти декілька шкідливих факторів, які або взаємно компенсуються, або накладаються один на жодний, шкідливо впливаючи на здоров'я людини. Правильно організований в санітарно-гігієнічному відношенні трудовий процес повинен виключати вплив шкідливих факторів на працюючих.

2.1. Організація робочого місця програміста

Робоче місце – це найголовніше , від того, наскільки людині затишно працювати, залежить її продуктивність, стан здоров'я, задоволеність самим робочим процесом. Основними меблями робочого місця програміста є крісло і стіл. Бажано, щоб у крісла були підлокітники та трохи увігнута поверхня і незначний нахил спинки назад. Стіл повинен мати відповідну для конкретної людини висоту, а його нижня частина повинна бути такої конструкції, щоб не вимагалося підтискати ноги. Що стосується розміщення предметів праці програміста, то монітор повинен знаходитися по центру столу, принтер – праворуч, а системний блок ліворуч. Клавіатуру потрібно встановити в зоні, де будуть знаходитися руки працівника, коли він сидить за столом.

2.2. Основні вимоги безпеки до мікроклімату виробничих приміщень, освітлення

Щоб робочий легко виконував поставлені перед ним завдання, важливо, щоб на його місце попадало досить світла. При слабкій освітленості очі втомлюються швидше, увага слабшає. Якщо освітлення занадто яскраве, воно буде зліпити і провокувати різь в очах, стане причиною дратівливості.

У більшості випадків природного освітлення на робочому місці програміста недостатньо або його зовсім немає, тому потрібно правильно вибрати джерела штучного освітлення та їх розташування**.** Кращим варіантом вважають люмінесцентні лампи, так як вони дають яскраве світло, схоже на денне. Щодо мікроклімату, для комфортної роботи в приміщенні, повинні бути визначені показники температури та вологості. В теплий період року в кімнаті , має бути +20-25, в холодний – +18… + 21°С, а в перехідний – +17… 21°С. Що стосується вологості, то оптимальним показником є від 40% до 60%. Щоб організувати комфортні умови**,** приділяють увагу системі опалення, вентиляції, кондиціонування повітря**.**

2.3. Шум, вібрація, ультразвук, інфразвук

Для зниження рівня шуму стіни і стеля приміщень, де встановлені комп'ютери, можуть бути облицьовані звукопоглинальними матеріалами. Рівень вібрації в приміщеннях обчислювальних центрів може бути понижений шляхом встановлення устаткування на спеціальні віброізолятори. Ультразвук являє собою механічні коливання пружного середовища і відрізняються від звукових хвиль більш високою частотою, що перевищує верхній поріг чутності. За способом передачі від джерела до людини ультразвук поділяють на: повітряний (передається через повітря) та контактний (передається на руки людини, що працює через тверде чи рідинне середовище).

Ультразвук, так само як і інфразвук, орган слуху людини не сприймає, однак він може спричиняти біль голови, загальну втому, розлади серцево-судинної та нервової систем. Можливі порушення периферичної нервової системи та порушення вестибулярного апарата. Щоб знизити негативний вплив

інфразвуку на людину співробітниками інституту розроблені Державні санітарні норми «Допустимі рівні інфразвуку в приміщеннях житлових та громадських будинків та на прилеглих до них територіях».

2.4. Електробезпека

Електронасиченість сучасного виробництва формує електричну небезпеку, джерелом якої можуть бути електричні мережі, електрифіковане устаткування та організаційна техніка, що працює на електриці. Електричний струм, діючи на організм людини, може привести до різних поразок: електричному удару, опіку, металізації шкіри, механічному ушкодженню. Ступінь важкості електричного враження залежить від багатьох факторів: величини опору організму, тривалості дії, природи й частоти шуму, умов зовнішнього середовища. Тому до обслуговування електричного обладнання допускаються особи, що пройшли спеціальний медичний огляд. Для захисту від дотику до частин нормально чи випадково знаходяться під напругою застосовується подвійна ізоляція - електронна ізоляція, що складається з робочої і додаткової ізоляції. Робоча ізоляція - ізоляція струмоведучих частин електроустановки, що забезпечує її нормальну роботу і захист від ураження електричним струмом. Додаткова ізоляція, яка передбачена додатково до робочої ізоляції для захисту від ураження електричним струмом в разі ушкодження робочої ізоляції. Захисне **заземлення** є простим, ефективним і поширеним способом **захисту** людини від ураження електричним струмом при дотику до металевих поверхонь, які виявились під напругою. Це забезпечується зниженням напруги між обладнанням, що виявилось під напругою, і землею до безпечної величини.

4. Пожежної безпеки

Пожежна безпека об’єкта – стан об’єкта, за якого з регламентованою імовірністю виключається можливість виникнення і розвитку пожежі та впливу на

людей її небезпечних факторів, а також забезпечує захист матеріальних цінностей. Основними напрямками забезпечення пожежної безпеки є усунення умов виникнення пожежі та мінімізація наслідків.

До первинних засобів пожежогасіння належать: *вогнегасники*; *ящики з піском*; *бочки з водою*; *покривала з негорючого теплоізоляційного матеріалу*; *совкові лопати, пожежний інструмент — кирки, сокири, багри, ломи* тощо. Найефективнішим первинним засобом пожежогасіння є вогнегасник. Первинні засоби пожежогасіння можна зберігати на пожежних щитах (стендах) червоного кольору, які встановлюють у виробничих, складських, допоміжних приміщеннях, будинках, спорудах, а також на території підприємств.

ВИСНОВОК

Дотримання вимог охорони праці та техніки безпеки дає можливість уникнути випадків травматизму, зберегти здоров’я та життя працюючих, що є основним завданням в системі заходів охорони праці.

Під час праці на людину впливають різні параметри виробничої обстановки, в якій протікає праця. Все це у сукупності характеризує певні умови, тобто це є умовами праці. Можна сказати, що дієздатність людини є фізіологічною основою продуктивності живої праці. Тому при рівності всіх інших умов, продуктивність праці буде тим вище, чим вище працездатність людини, яка бере участь у трудовому процесі.

ВИСНОВОК

Ключовою особливістю ІТ-аудиту у системі управління підприємством виступає те, що за результатами його проведення можна чітко отримати інформацію про те, яку роль інформаційні технології відіграють у загальній організаційній структурі підприємства. Поряд з тим, отримана інформацію дозволить визначити рівень адекватності ІТ-стратегії у відповідності до загальної стратегії підприємства, а також рівень зрілості ІТ-процесів та рівень управління ІТ-ризиками.

Результати проведеного огляду та аналізу в дипломному проєкті засвідчують, що ІТ-аудит виступає складовою частиною процесу стратегічного управління підприємством. З'ясовано, що з року в рік все більшої популярності набуває використання послуг ІТ-аудиту серед вітчизняних суб'єктів господарювання. Встановлено, що ІТ-аудит дозволяє формувати висновки про реальний стан захисту ІТ-ресурсів, а також рівень їх здатності протистояти внутрішнім та зовнішнім загрозам, що виникають у середовищі функціонування. Таким чином, внаслідок проведеного ІТ-аудиту отримується інформація про рівень ефективності функціонування ІТ-середовища, а також його основних складових частин. В дипломному проєкті розроблена система контролю роботи ІТ-компанії за допомогою внутрішнього та зовнішнього аудиту, що повністю відповідає поставленим цілям.

ПЕРЕЛІК ПОСИЛАНЬ

1. Астахова М. М. Використання комп'ютерних інформаційних систем при проведенні аудиту резервів і забезпечень підприємства / М. М. Астахова // Наукові праці Кіровоградського 30 національного технічного університету. Економічні науки: збірник наукових праць – 2007. – Вип. 12, Ч. 1. – С. 319–324. – URI: http://dspace.kntu.kr.ua/jspui/handle/123456789/873.

2. Бенько М. М. Інформаційні технології як фактор інтеграції внутрішнього і зовнішнього аудиту / М. М. Бенько, В. В. Сопко // Економічний форум. – 2015. – № 1. – С. 254–262. – URL: http://nbuv.gov.ua/UJRN/ecfor_2015_1_44.

3. Голяш І. Д. Аудит безпеки підприємства у сфері застосування інформаційних технологій / І. Д. Голяш, С. І. Саченко // Бухгалтерський облік, контроль і аналіз. – 2012. – С.90 – 95 .– URL:http://dspace.tneu.edu.ua/handle/ 316497/22636

4. Гребешков О. М. Стратегічний інформаційний аудит як інструмент розробки інформаційної стратегії підприємства / О. М. Гребешков // Вісник Національного університету "Львівська політехніка". – 2010. – № 683. – С. 202–205. – URL: http://ena.lp.edu.ua:8080/bitstream/ntb/20292/1/41- 202-205.pdf.

5. Гужва В. М. Інформаційні системи і технології на підприємствах: [навч. посібник] / В. М. Гужва. – К.: КНЕУ, 2001. – 400 с. – URL: http://www.dut.edu.ua/uploads/l_1366_68707543.pdf .

6. Данилюк І. IT- аудит: проблеми та перспективи / І. Данилюк // Модернізація національної системи управління державним розвитком: виклики і перспективи.–2016.–Ч.2.–С.75–77.–URL:http://econf.at.ua/publ/konferencija_2016_ 12_8_9/sekcija_5_ekonomichni_nauki/it_audit_problemi_ta_perspe ktivi/61-1-0-1467.

7. Денисенко М. П. Інформаційне забезпечення ефективного управління підприємством / М. П. Денисенко, І. В. Колос // Економіка та держава. – 2006. – № 7. – С. 19–24. – URL: http://dspace.nuft.edu.ua/jspui/handle/123456789/2214 1 .

8. Івахненков С. В. Поняття комп'ютерного контролю та аудиту / С. В. Івахненков // Менеджмент: збірник наукових праць. – 2009. – Вип.11. – 225 с. – С. 24–38.–URL:http://ekmair.ukma.edu.ua/bitstream/handle/123456789/644/Ivakhnenkov_Poniattia%20kompiuternoho.pdf.

9. Москаленко Ф. І. Проблемні питання проведення аудиту інформаційних систем у сучасних умовах / Ф. І. Москаленко // Таврійський науковий вісник. Економічні науки. – 2013. – № 84. – С. 327–332. – URL: http://irbis-nbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBNUJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Tavnv_2013_84_66.pd f.

10. Бойчик І. М. Економіка підприємства : навчальний посібник для студентів економічних спеціальностей вищих навчальних закладів I-IV рівнів акредитації. Третє видання, випр. і доп. / І. М. Бойчик, П. С. Харів., М. І. Холчан, Ю. В. Піча. – К. : Каравела, 2016. – 328 с.

11. Закон України Про охорону праці , №235-IV, 22.11.2002.

12. ДНАОП 0.03-8.03-97 Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процессу

13. ГОСТ 12.003–74 ССБТ. Опасные и вредные производственные факторы. Классификация.