МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет обліку та податкового менеджментуКафедра аудиту

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Диджитал-облік»

Галузь знань: 07 «Управління та адміністрування»
Спеціальність: 071 «Облік і оподаткування»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему: **«Організація інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер"»**

(назва теми)

здобувача Мельника Дмитра Олександровича
(ПІБ, підпис)

Науковий керівник: к.е.н., професор Кошець О. В.

_____

Робота допущена до захисту перед екзаменаційноюкомісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.е.н, професор Петрик О.А.

_____

Київ – 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет обліку та податкового менеджменту

Кафедра аудиту

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Диджитал-облік»
Галузь знань: 07 "Управління та адміністрування"
Спеціальність: 071 "Облік і оподаткування"

ПОГОДЖЕНО	**ЗАТВЕРДЖУЮ**
Керівник проєктної групи (гарант) освітньо-професійної програми	Завідувач кафедри
Олена ПЕТРИК *(підпис)*	Олена ПЕТРИК *(підпис)*
_____ 2023р.	_____ 2023р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Мельнику Дмитру Олександровичу

денної форми навчання

на підготовку кваліфікаційної бакалаврської роботи

на тему: **«**Організація інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ “Сервіс-Майстер”»**.**

Тему затверджено наказом ректора Університету від 24 березня 2023р. №505-ст.

Кваліфікаційна бакалаврська робота виконується на матеріалах: ПП СЦ «Сервіс-Майстер».

План кваліфікаційної бакалаврської роботи

Розділ 1	Теоретичні основи організації інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер».
Розділ 2	Стан та вдосконалення інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер».
Об'єкт дослідження:	організація інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер».
Предмет дослідження:	теоретичні та практичні аспекти організації інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер».
Мета кваліфікаційної бакалаврської роботи:	Розкрити особливості організації інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер» та надати пропозиції щодо її вдосконаленню.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1
- визначити та охарактеризувати організаційні та технологічні особливості діяльності ПП СЦ «Сервіс-Майстер»;
- надати характеристику інформаційних технологій, що використовуються для цифровізації обліку та внутрішнього контролю досліджуваного підприємства;
- принципи та організація захисту інформації у системі обліку та внутрішнього контролю підприємства;
У розділі 2
- описати фактичний стан системи обліку та внутрішнього контролю щодо її інформаційної забезпеченості та захищеності;
- визначити потенційні загрози та ризики для інформаційної безпеки системи обліку та внутрішнього контролю для ПП СЦ «Сервіс-Майстер»;
- дати оцінку з підвищення інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»;
- розробити рекомендації щодо удосконалення та підвищення ефективності заходів інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер».

Завдання підготував
науковий керівник _____ Оксана КОШЕЦЬ
(підпис)

«_____» квітня 2023р.

Завдання одержав
здобувач _____ Дмитро МЕЛЬНИК
(підпис)

«_____» квітня 2023р.

ПРИВАТНЕ ПІДПРИЄМСТВО СЕРВІСНИЙ ЦЕНТР «СЕРВІС-МАЙСТЕР»
код ЄДРПОУ 33463138
43000, Волинська область, місто Луцьк, проспект Соборності, будинок 33, квартира 66

ЛИСТ-ЗАМОВЛЕННЯ

ПП СЦ «Сервіс-Майстер» висловлює свою зацікавленість у проведенні наукового прикладного дослідження в межах проекту «Організація інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»» здобувачем першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Диджитал-облік» 4 курсу групи ОД-401 КНЕУ ім. Вадима Гетьмана Мельником Дмитром Олександровичем.

Наукові та практичні результати дослідження, розробки методик та внесення рекомендацій, що очікуються при виконанні даного проекту, маємо намір використати в організації інформаційної безпеки системи обліку та внутрішнього контролю, що є ключовою умовою успішної діяльності бізнесу.

Директор
ПП СЦ «Сервіс-Майстер» **Гурський А.В.**

ПРИВАТНЕ ПІДПРИЄМСТВО СЕРВІСНИЙ ЦЕНТР «СЕРВІС-МАЙСТЕР»
код ЄДРПОУ 33463138
43000, Волинська область, місто Луцьк, проспект Соборності, будинок 33, квартира 66

«30» травня 2023 р.

ДОВІДКА

про впровадження результатів дослідження кваліфікаційної бакалаврської роботи

Мельника Дмитра Олександровича

Довідка надана здобувачу першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Диджитал-облік» кафедри аудиту Київського національного економічного університету імені Вадима Гетьмана Мельнику Дмитру Олександровичу в тому, що виконана ним кваліфікаційна бакалаврська робота на тему: «Організація інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»», на нашу думку, має практичну цінність, а її результати можуть бути використані у господарській діяльності підприємства в частині пропозицій щодо вдосконалення інформаційної безпеки системи обліку та внутрішнього контролю.

Директор
ПП СЦ «Сервіс-Майстер» **Гурський А.В.**

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 71 сторінку, 22 таблиць, 2 рисунка, список використаних джерел з 30 найменувань, додатки.

«Організація інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»»

Об'єктом дослідження є організація інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер».

Предметом дослідження є теоретичні та практичні аспекти організації інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер».

*Мета дослідження***.** Розкриття особливості організації інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер» та надати пропозиції щодо її вдосконаленню.

Відповідно до поставленої мети були визначені такі *завдання*:

- визначити та охарактеризувати організаційні та технологічні особливості діяльності ПП СЦ «Сервіс-Майстер»;
- надати характеристику інформаційних технологій, що використовуються для цифровізації обліку та внутрішнього контролю досліджуваного підприємства;
- принципи та організація захисту інформації у системі обліку та внутрішнього контролю підприємства;
- описати фактичний стан системи обліку та внутрішнього контролю щодо її інформаційної забезпеченості та захищеності;
- визначити потенційні загрози та ризики для інформаційної безпеки системи обліку та внутрішнього контролю для ПП СЦ «Сервіс-Майстер»;
- дати оцінку з підвищення інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»;
- розробити рекомендації щодо удосконалення та підвищення ефективності заходів інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер».

Теоретична, методична та практична значущість отриманих результатів полягає у тому, що результати спрямовані на пошуки напрямків удосконалення інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер».

Рік виконання кваліфікаційної бакалаврської роботи: 2023. Рік захисту роботи: 2023.

Ключові слова: інформаційна безпека, внутрішній контроль, система обліку, цифрові технології, електронна звітність, політика безпеки, оновлення, інформаційні системи обліку, автоматизована обробка даних.

ЗМІСТ

ВСТУП

***Актуальність теми*:** «Організація інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»» є дуже актуальною в сучасному цифровому світі. Запобігання кіберзлочинності та захист інформації є надзвичайно важливим завданням для будь-якої організації. У світлі постійних загроз хакерських атак та витоків даних, впровадження ефективних заходів забезпечення інформаційної безпеки стає пріоритетом. Організація інформаційної безпеки в системі обліку та внутрішнього контролю допомагає запобігти несанкціонованому доступу до конфіденційної інформації, зберегти надійність даних та забезпечити довіру клієнтів і партнерів. Враховуючи розширення цифрових можливостей бізнесу, ця тема залишається актуальною і допомагає забезпечити стійку та безпечну роботу компанії у сучасному інформаційному середовищі.

Тому стає зрозуміло доцільність та необхідність вивчення даної теми, як з боку підприємств – суб'єктів господарювання, так і збоку професіоналів, які забезпечують інформаційну безпеку систем обліку та внутрішнього контролю як на мікро, так і на макро- рівнях . Все це свідчить про актуальність теми дослідження

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки систем обліку та внутрішнього контролю підприємства розглянуто в працях провідних вітчизняних та зарубіжних науковців: Гаркуша С. А., Грабчук І. Л., Титенко Л. В. Стечишин Ю., Чех Н.О. та інші.

Метою дослідження є розкриття особливості організації інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер» та надати пропозиції щодо її вдосконаленню.

Відповідно до поставленої мети були визначені та виконані такі завдання:

- визначити та охарактеризувати організаційні та технологічні особливості діяльності ПП СЦ «Сервіс-Майстер»;

- надати характеристику інформаційних технологій, що використовуються для цифровізації обліку та внутрішнього контролю досліджуваного підприємства;

- принципи та організація захисту інформації у системі обліку та внутрішнього контролю підприємства;

- описати фактичний стан системи обліку та внутрішнього контролю щодо її інформаційної забезпеченості та захищеності;

- визначити потенційні загрози та ризики для інформаційної безпеки системи обліку та внутрішнього контролю для ПП СЦ «Сервіс-Майстер»;

- дати оцінку з підвищення інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»;

- розробити рекомендації щодо удосконалення та підвищення ефективності заходів інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер».

Об'єкт дослідження: організація інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер».

Предметом дослідження є теоретичні та практичні аспекти організації інформаційної безпеки системи обліку та внутрішнього контролю у ПП СЦ «Сервіс-Майстер».

Методи дослідження: *У* вирішенні поставлених завдань були такі загальнонаукові методи: *абстрактно-логічний та історичний* – застосовано при вивченні сутності інформаційної безпеки та визначенні її класифікаційних ознак; *спостереження, порівняння та аналогія* - для оцінки інформаційних технологій, що використовуються для цифровізації обліку та внутрішнього контролю, *метод узагальнення* - для здійснення теоретичних узагальнень, формування висновків і рекомендацій.

Теоретична, методична та практична значущість отриманих результатів полягає у тому, що результати спрямовані на пошуки напрямків удосконалення інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер».

Інформаційною базою дослідження є праці вітчизняних та зарубіжних науковців і практиків, статистичні дані офіційних сайтів, звіти рейтингових агентств, що стосуються організації інформаційної безпеки систем обліку та внутрішнього контролю. Це дозволило отримати узагальнену інформацію про різні підходи, методи та принципи, що застосовуються в даній області.

Також проведено спостереження за діяльністю ПП СЦ "Сервіс-Майстер" щодо організації інформаційної безпеки систем обліку та внутрішнього контролю. Це дозволило отримати практичні відомості про існуючі процеси, процедури та заходи безпеки, що вже застосовуються в організації.

***Структура роботи*.** Робота складається зі вступу, двох розділів, висновків , списку використаних джерел та додатків

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ ОБЛІКУ ТА ВНУТРІШНЬОГО КОНТРОЛЮ У ПП СЦ «СЕРВІС-МАЙСТЕР»

1.1 Організаційні та технологічні особливості діяльності ПП СЦ «Сервіс-Майстер»

Досліджуване приватне підприємство сервісний центр «Сервіс-Майстер» (далі – ПП СЦ «Сервіс-Майстер») знаходиться за адресою: Волинська обл., м. Луцьк, пр. Перемоги, 24.

Підприємство здійснює свою діяльність на основі Статуту і відповідно до чинного законодавства України. Основним видом економічної діяльності досліджуваного підприємства є ремонт техніки побутового призначення.

Метою діяльності підприємства згідно Статуту є виробнича, торгівельна, господарська та інша діяльність, спрямована на отримання прибутку від усіх видів діяльності підприємства, визначених Статутом, а також задоволення на підставі одержаного прибутку соціально-економічних інтересів Учасників та членів трудового колективу.

Основний вид господарської діяльності згідно Статуту:

- ремонт електронної апаратури побутового призначення для приймання, записування, відтворювання звуку й зображення;

- ремонт побутових приладів, домашнього та садового обладнання;

- оптова торгівля побутовими електротоварами й електронною апаратурою побутового призначення для приймання, записування, відтворювання звуку й зображення

- діяльність посередників у торгівлі товарами широкого асортименту;

- роздрібна торгівля в спеціалізованих магазинах електронною апаратурою побутового призначення для приймання, записування, відтворювання звуку й зображення

Підприємство веде бухгалтерський, податковий облік та надає статистичну звітність згідно з чинним законодавством.

Ведення бухгалтерського обліку на підприємстві регулюється Наказом «Про облікову політику підприємства й організацією бухгалтерського обліку» ПП СЦ «Сервіс-Майстер», що було затверджено директором підприємства.

Для забезпечення ведення бухгалтерського обліку на ПП СЦ «Сервіс-Майстер» встановлено наступну форму організації бухгалтерського обліку:

-бухгалтерський облік ведеться бухгалтерською службою підприємства, яку очолює головний бухгалтер;

-головний бухгалтер підприємства може мати заступника (заступників), їх кількість визначається штатним розкладом підприємства;

-кількісний та якісний склад бухгалтерської служби визначається штатним розкладом і затверджується окремим наказом керівника підприємства.

Ведення бухгалтерського обліку здійснюється за допомогою комп’ютерної програми M.E.Doc.

Права та обов’язки головного бухгалтера і посадових осіб бухгалтерської служби визначаються Законом про бухгалтерський облік, статутом і затвердженими посадовими інструкціями.

Розпорядження головного бухгалтера, які стосуються організації та здійснення бухгалтерського обліку на підприємстві, є обов’язковими до виконання усіма структурними підрозділами і працівниками підприємства.

Головний бухгалтер наділяється правом другого підпису, який він проставляє на первинних бухгалтерських документах, регістрах бухгалтерського обліку та відповідних звітах.

Головний бухгалтер несе особисту відповідальність перед керівником підприємства, згідно з переліком питань, наведених у пункті 7 статті 8 Закону про бухгалтерський облік.

За відсутності головного бухгалтера обов'язки та відповідальність покладаються на іншого працівника, згідно з окремим письмовим розпорядженням керівника підприємства.

Відповідальність інших працівників регулюється посадовими інструкціями, які затверджуються керівником підприємства.

Загальну відповідальність за ведення податкового обліку покладено на головного бухгалтера, крім того доручено виписування податкових накладних, ведення обліку продажу та придбання, вести підрахунок валових доходів та валових витрат. Облік доходів та витрат здійснюється за окремими розрахунками у форматі діючої звітності про прибуток підприємства.

ПП СЦ «Сервіс-Майстер» займається наданням послуг ремонту та обслуговування різних типів техніки, такої як телевізори, холодильники, пральні машини та інші побутові прилади. Вони пропонують діагностику, ремонт, заміну деталей, обслуговування та консультації щодо експлуатації техніки.

Це підприємство надає послуги як фізичним особам, так і бізнесам. Клієнти можуть звертатися до них у разі несправностей або поломок своєї техніки, а також для проведення профілактичного обслуговування. ПП СЦ «Сервіс-Майстер» має кваліфікований персонал, який володіє необхідними знаннями і навичками для виконання ремонтних робіт.

Майстри можуть виконувати роботу в сервісному центрі або працювати на мобільній основі, коли працівники виїжджають безпосередньо до клієнтів для проведення ремонтних робіт на місці.

В загальному, метою ПП СЦ «Сервіс-Майстер» є надання швидкого та якісного сервісу для відновлення роботи техніки та задоволення потреб клієнтів у сфері ремонту й обслуговування.

Діяльність досліджуваного підприємства має свої особливості, які відносяться як до організаційної, так і до технологічної сфери.

Організаційні особливості діяльності даної компанії включають наступні аспекти:

- Юридичний статус: ПП СЦ "Сервіс-Майстер" є приватним підприємством що діє на базі приватної власності, яка належить одній або кільком фізичним особам, або приватної власності юридичної особи і реєструється згідно з законами України та відповідає їх вимогам.

- Організаційна структура: В структурі СЦ "Сервіс-Майстер" є такі підрозділи:

✓ Керівництво: Організація має керівника, який приймає стратегічні рішення та встановлює загальну політику підприємства.

✓ Відділ обслуговування клієнтів: Цей відділ відповідає за взаємодію з клієнтами, прийом заявок на обслуговування, управління графіками роботи, вирішення розбіжностей та надання інформації клієнтам.

✓ Технічний відділ: Відділ, який займається безпосередньо технічним обслуговуванням або ремонтом продукції. Він може включати в себе спеціалістів з різних галузей або фахівців з певного виду техніки.

✓ Адміністративний відділ: відділ, що забезпечує адміністративну підтримку, таку як фінанси, кадри, закупівлі та інші адміністративні функції.

- Обсяги діяльності: ПП СЦ "Сервіс-Майстер" займається наданням послуг з ремонту, обслуговування, монтажу, налаштування, консультування та інших супутніх послуг для різних видів техніки, пристроїв або систем. В основному це побутові пристрої.

- Клієнтська база: Компанія спрямовує свою діяльність на обслуговування як корпоративних, так і приватних клієнтів. Це можуть бути фізичні особи, організації, бізнеси. Організаційно, в ПП СЦ "Сервіс-Майстер" клієнтська база забезпечує можливість збирати та зберігати дані про клієнтів, їх контактну інформацію, історію взаємодії та деталі технічних проблем. Ця інформація дозволяє підприємству створювати індивідуальні профілі клієнтів, розуміти їхні потреби та вимоги, а також вести персоналізований підхід до надання послуг.

- Кваліфікація та персонал: ПП СЦ "Сервіс-Майстер" наймає фахівців з високою кваліфікацією, які мають досвід роботи в сфері сервісу та ремонту. Це механіки, електрики, програмісти, інженери та інші фахівці з технічного та

сервісного обслуговування. Компанія надає увагу якісній підготовці свого персоналу, включаючи постійне професійне навчання, оновлення знань та використання сучасних технологій та методів обслуговування. Крім того, СЦ "Сервіс-Майстер" має спеціалізовані сертифікації та партнерства з виробниками апаратури або обладнання, що дозволяє їм мати доступ до офіційних ремонтних інструкцій та запасних частин.

- Обладнання та ресурси: в загальному розумінні, обладнання та ресурси, які використовуються в ПП СЦ "Сервіс-Майстер", включають наступне:

Інструменти ремонту - ручні інструменти, електроінструменти, діагностичне обладнання, прилади для вимірювання та тестування, лабораторне обладнання тощо. Запчастини та матеріали - резервні частини, комплектуючі, кабелі, дроти, конектори, паяльне обладнання, мастила, розчинники, термопаста тощо. Інформаційні ресурси - комп'ютери, програмне забезпечення, бази даних, інтернет-підключення, електронні ресурси для пошуку інформації про ремонт і обслуговування різних пристроїв. Робоче приміщення - сервісний центр має спеціально обладнане приміщення для ремонту та обслуговування пристроїв, де є робочі столи, стелажі для зберігання обладнання та запчастин, освітлення, вентиляція тощо.

- Контроль якості: Так, як ПП СЦ «Сервіс-Майстер» являється малим підприємством, тому застосовані більш прості і доступні підходи до контролю якості. Розроблений план контролю якості, який включає методи і процедури перевірки якості виробленої продукції або наданої послуги. Також встановлені процедури оцінки постачальників, які допомагають переконатись, що вони також дотримуються стандартів якості. Компанія має систему контролю якості, що дозволяє перевіряти якість виконаних робіт та задовольняти вимоги клієнтів.

- Комунікація з клієнтами: ПП СЦ "Сервіс-Майстер" підтримує активну комунікацію зі своїми клієнтами. Це включає прийом заявок, консультації, планування робіт, звітність щодо виконаних послуг, розрахунок вартості та інші аспекти взаємодії. Оскільки СЦ "Сервіс-Майстер" надає послуги, взаємодія з клієнтами є важливою складовою його діяльності. Організація має процедури для

прийому заявок на обслуговування, контактний центр та онлайн-систему для взаємодії з клієнтами та систему контролю якості надання послуг.

- Гнучкість та швидкість реагування: Компанія має гнучку структуру та швидкість реагування на потреби клієнтів. Це дозволяє швидко реагувати на заявки, надавати екстрені послуги або здійснювати ремонт у встановлені терміни.

- Партнерство та співпраця: ПП СЦ "Сервіс-Майстер" укладає партнерські угоди з виробниками техніки та постачальниками компонентів для забезпечення швидкого доступу до необхідних запчастин та технічної підтримки. Угоди підписані з такими відомими компаніями як Bosch,Siemens, Electrolux, gorenje та іншими виробниками побутової техніки.

- Графік роботи: Компанія працює у режимі регулярного робочого часу з 9:00 до 18:00 з понеділка по п’ятницю. А також має розширений графік для деяких працівників, щоб задовольнити потреби клієнтів, які потребують надання послуг поза стандартними годинами роботи.

- Мобільний сервіс: ПП СЦ "Сервіс-Майстер" має мобільну бригаду яка виїжджає безпосередньо до місця розташування клієнта для виконання ремонтних або сервісних робіт. Тобто надає послуги на місці, виїжджаючи до клієнтів з мобільними бригадами. Це може включати ремонт або обслуговування техніки безпосередньо в домі або офісі клієнта.

- Гарантія та обслуговування: Компанія надає гарантійні терміни на виконані роботи та забезпечує обслуговування, включаючи ремонт або заміну в разі виявлення дефектів.

- Індивідуальний підхід: ПП СЦ "Сервіс-Майстер" може пропонувати індивідуальні рішення та пакети послуг, що відповідають конкретним потребам та бюджету клієнта відповідно до створеного прайс-листа.

- Використання сучасних технологій: Компанія використовує сучасні технології, такі як онлайн-системи заявок, відеодіагностика, дистанційне керування та інші інструменти для поліпшення якості та ефективності своїх послуг.

Основні технологічні особливості діяльності ПП СЦ «Сервіс-Майстер» наведені у таблиці 1.1.

Таблиця 1.1 – Технологічні особливості діяльності ПП СЦ «Сервіс-Майстер»

№ п/п	Особливість діяльності	Шляхи реалізації
1	Діагностика	Компанія використовує спеціалізоване обладнання та програмне забезпечення для проведення діагностики несправностей у техніці. Це дозволяє швидко та точно виявляти проблеми та визначати потрібні ремонтні дії
2	Експертиза	Висококваліфіковані фахівці ПП СЦ "Сервіс-Майстер" проводять експертизу техніки, що дозволяє встановити причину несправності та визначити оптимальний спосіб відновлення роботи пристрою
3	Ремонт	Компанія має досвідчених техніків, які виконують ремонтні роботи з високою якістю. Вони володіють знаннями і навичками для відновлення роботи різних типів техніки
4	Заміна комплектуючих	У разі потреби у заміні окремих деталей або комплектуючих, ПП СЦ "Сервіс-Майстер" має доступ до оригінальних або якісних замінників, що гарантує надійність та тривалість відновленої техніки
5	Технічна підтримка	Після ремонту або обслуговування, компанія надає технічну підтримку своїм клієнтам. Це включає консультації щодо правильної експлуатації техніки та вирішення можливих проблем
6	Інновації	ПП СЦ "Сервіс-Майстер" слідкує за новітніми технологіями та розвитком ринкових стандартів у сфері технічного обслуговування та ремонту. Компанія впроваджує інноваційні методики та технології для поліпшення якості своїх послуг і забезпечення більш швидкого та ефективного виконання робіт.
7	Автоматизація процесів	ПП СЦ "Сервіс-Майстер" використовує системи автоматизації для управління процесами обслуговування та ремонту. Це дозволяє оптимізувати час і зусилля, зменшити ймовірність помилок та забезпечити швидке реагування на замовлення клієнтів
8	Клієнтська орієнтованість	ПП СЦ "Сервіс-Майстер" ставить на перше місце задоволення потреб своїх клієнтів. Компанія надає індивідуальний підхід до кожного замовлення, забезпечуючи високу якість обслуговування та виконання ремонтних робіт.
9	Надійність та конфіденційність	ПП СЦ "Сервіс-Майстер" дотримується високих стандартів безпеки та конфіденційності. Клієнти можуть бути впевнені в тому, що їх техніка буде оброблена з уважністю та дотриманням приватності. Програмне забезпечення є стабільним та працює безперебійно. Воно виконувати свої функції без помилок, перебоїв або недоліків, які можуть призвести до втрати даних або збоїв у роботі. Програмне забезпечення забезпечує захист конфіденційної інформації користувачів. Це означає, що дані, які вводяться або зберігаються в системі, захищені від несанкціонованого доступу або витоку. Компанія вживає заходів для забезпечення безпеки даних та використовує шифрування, аутентифікацію та інші заходи безпеки для запобігання порушення конфіденційності.

Джерело: розроблено автором на основі спостережень за підприємством

СЦ "Сервіс-Майстер" є організацією, яка спеціалізується на ремонті та обслуговуванні електронної техніки. Вона відрізняється своїми організаційними та технологічними особливостями. Загалом, ПП СЦ "Сервіс-Майстер" забезпечує високу якість технічного обслуговування та ремонту техніки за допомогою передових технологій, професійного підходу та прагне бути у курсі останніх розвитків у галузі.

1.2 Характеристика інформаційних технологій, що використовуються для цифровізації обліку та внутрішнього контролю досліджуваного підприємства

Інформаційні технології (ІТ) використовуються для автоматизації процесів обліку та внутрішнього контролю ПП СЦ "Сервіс Майстер". Це дозволяє зменшити кількість помилок і підвищити ефективність діяльності підприємства. Інформаційні технології, що використовуються для цифровізації обліку та внутрішнього контролю сервісного центру включають в себе наступне:

Електронні таблиці: На підприємстві використовуються програми для створення електронних таблиць, які дозволяють зберігати та обробляти числові дані. Вони можуть бути використані для обліку фінансових операцій, інвентаризації, контролю запасів тощо. Електронні таблиці також забезпечують можливість створення формул і автоматизацію розрахунків. Найбільш використовуваною програмою на підприємстві є Microsoft Excel.

Microsoft Excel є одним з найпопулярніших програмних засобів для обробки даних та аналізу на підприємствах. Він надає широкий спектр можливостей для створення та редагування електронних таблиць, обчислень, графіків та звітів. Використання Microsoft Excel на підприємстві має суттєві переваги сприяє покращенню ефективності та продуктивності бізнес-процесів. Деякі аспекти використання Microsoft Excel на підприємстві наведені у таблиці 1.2.

Таблиця 1.2 – Основні аспекти використання Microsoft Excel ПП СЦ "Сервіс Майстер"

№ п/п	Місце використання	Як використовується Microsoft Excel ПП СЦ "Сервіс Майстер"?
1	Аналіз та візуалізація даних:.	Excel дозволяє виконувати різноманітні обчислення, сортування, фільтрацію та аналіз даних. Завдяки широкому спектру функцій і формул, користувачі можуть створювати складні моделі і розрахунки, які сприяють прийняттю обґрунтованих рішень. Крім того, Excel надає можливість візуалізувати дані за допомогою графіків, діаграм та інших інструментів, що полегшує сприйняття та аналіз інформації
2	Управління запасами та облік	Excel може бути використаний для ведення обліку запасів, включаючи складські запаси, закупівлі та реалізацію товарів. Він дозволяє створювати таблиці зі списками товарів, їх кількостями, цінами та іншими релевантними даними. За допомогою вбудованих формул і функцій можна виконувати автоматичний розрахунок сум запасів, середньої вартості, звіту про обороти тощо.
3	Фінансовий облік і бюджетування	Excel є потужним інструментом для фінансового обліку та бюджетування. Він дозволяє створювати фінансові звіти, обчислювати прибуток та витрати, контролювати бюджет та відстежувати фінансові показники. Також можна використовувати фінансові моделі для прогнозування майбутніх результатів та прийняття стратегічних рішень.
4	Управління проектами	Excel являється ефективним інструментом для управління проектами. За його допомогою можна створювати графіки Ганта (використовується для ілюстрації плану, графіка робіт), контролювати терміни, відстежувати виконання завдань та ресурсів, обчислювати витрати і прибутки. Excel також дозволяє створювати звіти про стан проекту та аналізувати ефективність його виконання.
5	Звітність та аналітика	Excel використовується для створення звітів та аналітики на підприємстві. Завдяки можливості обробки та аналізу великого обсягу даних, Excel дозволяє генерувати звіти, таблиці з підсумками, аналітичні звіти та інші види документів, необхідних для звітності та прийняття рішень.

Джерело: розроблено автором на основі [14]

Загалом, Microsoft Excel є потужним інструментом для обробки даних, аналізу та управління в ПП СЦ «Сервіс-Майстер». Він дозволяє ефективно виконувати різноманітні завдання, спрощує роботу з даними та допомагає в прийнятті обґрунтованих бізнес-рішень.

Ведення бухгалтерського обліку у ПП СЦ "Сервіс Майстер" здійснюється із використанням різних програмних продуктів для ведення бухгалтерського обліку, які дозволяють здійснювати швидкий та точний облік фінансових операцій. Основною програмою бухгалтерського обліку підприємства є M.E.Doc, який спрощує процес подання звітності до державних органів, забезпечує точності облікових записів та полегшує взаємодію між підприємством та державними органами.

Комп'ютеризована бухгалтерія в ПП СЦ "Сервіс Майстер" є сучасною системою обліку, яка використовує комп'ютерні програми та спеціалізоване програмне забезпечення для обробки бухгалтерської інформації. Що дозволяє автоматизувати багато рутинних процесів, пов'язаних з обліком і звітністю, та забезпечує більшу точність та ефективність управління фінансовою інформацією.

Переваги комп'ютеризованої бухгалтерії на досліджуваному підприємстві наведені у таблиці 1.3.

Таблиця 1.3 – Переваги використання автоматизованого ведення бухгалтерського обліку у ПП СЦ "Сервіс Майстер"

№ п/п	Ознака переваги	Комп'ютеризована бухгалтерська система дозволить:
1	Ефективність	виконувати рутинні завдання швидше та ефективніше, зменшуючи час на їх виконання та потребу вручну обробляти багато даних.
2	Точність	уникнути помилок, пов'язаних з ручним введенням даних та розрахунками. Вона також дозволяє автоматично перевіряти правильність обробки даних та проводити автоматичні розрахунки.
3	Зручність	мати зручний інтерфейс для введення та обробки даних, а також для генерації звітів та фінансової інформації. Це спрощує ведення бухгалтерського обліку і полегшує доступ до важливої інформації.
4	Звітність	швидко генерувати різноманітні фінансові звіти та звіти для внутрішнього управління. Це допомагає забезпечити вчасну та точну звітність для власників бізнесу, податкових органів та інших зацікавлених сторін
5	Автоматичний облік	автоматично відстежувати та обліковувати фінансові операції, включаючи продажі, покупки, заробітну плату та інші транзакції. Це спрощує процес ведення обліку та дозволяє зберігати всю необхідну інформацію в одному централізованому місці.
6	Відстеження податків	автоматично розраховувати та відстежувати податки, такі як ПДВ, податок на прибуток, збір на соціальне страхування та інші. Це дозволяє вчасно розраховувати податкові зобов'язання та уникнути потенційних проблем з податковими органами.

Продовження таблиці 1.3

7	Безпека даних	забезпечує можливість зберігання даних в захищеному середовищі. Можна встановити обмежений доступ до фінансової інформації, щоб забезпечити конфіденційність даних та запобігти несанкціонованому доступу.
8	Інтеграція з іншими системами	бути інтегрованою з іншими системами управління, такими як системи управління клієнтами (CRM). Це дозволяє автоматично обмінюватися даними між різними системами і покращує загальну ефективність бізнес-процесів.
9	Автоматичний аналіз даних	проводити аналіз фінансових даних, використовуючи різноманітні фінансові показники та індикатори. Це допомагає виявляти тенденції, аномалії та можливі проблеми у фінансовому стані підприємства.
10	Електронний документообіг	здійснювати обмін документами та інформацією в електронному форматі. Це зменшує потребу у використанні паперової документації, полегшує зберігання та пошук необхідних документів, а також сприяє швидкому та зручному обміну інформацією з контрагентами та податковими органами.
11	Можливість масштабування	легко бути розширена та адаптована до зростання потреб бізнесу. Вона може вміщати більшу кількість даних, додаткові функції та модулі, що дозволяють підприємству розширювати свої можливості без значних зусиль.
12	Забезпечення виконання законодавства.	підприємству виконувати вимоги законодавства щодо фінансового звітування та обліку. Вона автоматично враховує податкові норми, стандарти бухгалтерського обліку та інші правові вимоги, що забезпечує дотримання відповідних правил і зменшує ризик санкцій

Джерело: розроблено автором на основі [16]

Отже, комп'ютеризована бухгалтерія в ПП СЦ "Сервіс Майстер" допомагає підвищити ефективність управління фінансовими ресурсами, забезпечує точність та надійність обліку, спрощує процеси звітності та сприяє більшій прозорості фінансової інформації. Вона дозволяє зосередитися на стратегічному аналізі та прийнятті обґрунтованих фінансових рішень, сприяючи подальшому розвитку бізнесу.

Однак, важливо зазначити, що комп'ютеризована бухгалтерія потребує належного налаштування, впровадження та підтримки. Компанії потрібно постійно мати доступ до спеціалістів з бухгалтерії та інформаційних технологій,

які забезпечують правильну роботу системи, забезпечують захист даних та надають підтримку користувачам.

Узагалі, комп'ютеризована бухгалтерія є важливим інструментом для сучасних підприємств, який допомагає покращити ефективність, точність та звітність бухгалтерського обліку, а також сприяє ефективному управлінню фінансами підприємства.

При використанні електронного документообігу по кожній операції, яку здійснює ПП СЦ "Сервіс Майстер", створюється електронний документ, що зберігається в електронній базі даних. Це дозволяє забезпечити швидкий та легкий доступ до інформації, а також зменшити кількість паперової документації.

Електронна звітність є важливим елементом сучасної бухгалтерії та фінансового управління. Вона дозволяє ПП СЦ "Сервіс Майстер" зручно та ефективно генерувати, зберігати та подавати різноманітні фінансові звіти та декларації в електронному форматі. Основні переваги електронної звітності наведено у таблиці 1.4.

Таблиця 1.4 – Переваги електронної звітності

№ п/п	**Ознака переваги**	**Електронна звітність дозволить:**
1	Ефективність	автоматично генерувати звіти на основі фінансових даних, що зберігаються в комп'ютеризованій бухгалтерській системі. Це значно зменшує час та зусилля, потрібні для складання звітів вручну.
2	Точність	сприяти точному розрахунку фінансових показників та уникненню помилок, пов'язаних з ручними обчисленнями та перенесенням даних.
3	Зручність	легко зберігати звіти, переглядати та редагувати на комп'ютері. Вони займають менше місця, порівняно з паперовими звітами, і легко доступні для подальшого аналізу та аудиту.
4	Сумісність	електронні звіти можна легко передавати електронним шляхом між сторонами, такими як податкові органи, банки та інші зацікавлені сторони. Це спрощує процес обміну інформацією та забезпечує швидку доставку звітів.
5	Законність	використання електронної звітності відповідає сучасним вимогам законодавства та податкового законодавства. Багато країн впроваджують електронну звітність як обов'язковий стандарт для підприємств, що мають звітувати перед податковими органами.
6	Забезпечення безпеки даних	електронна звітність дозволяє забезпечити захист фінансової інформації шляхом використання шифрування та інших заходів безпеки. Це допомагає запобігти несанкціонованому доступу до конфіденційних даних.

Продовження таблиці 1.4

7	Автоматична перевірка та валідація	багато комп'ютерних програм для електронної звітності мають вбудовані механізми перевірки та валідації даних. Вони автоматично перевіряють правильність введених даних та виявляють можливі помилки або некоректні значення.
8	Автоматична відправка звітів	електронні звіти можуть бути автоматично відправлені до відповідних органів або сторін. Це спрощує процес звітності та дозволяє забезпечити вчасну доставку звітів без затримок чи помилок, пов'язаних з ручною відправкою.
9	Зменшення витрат	використання електронної звітності може допомогти зменшити витрати на папір, друкування та доставку звітів. Крім того, це дозволяє знизити час, витрачений на ручне складання та обробку звітів
10	Інтеграція з іншими системами	електронна звітність може бути легко інтегрована з іншими системами, такими як комп'ютеризована бухгалтерська система, система управління клієнтами (CRM) або система управління складом. Це спрощує обмін даними та забезпечує єдину інформаційну систему для управління підприємством.

Джерело: розроблено автором на основі [17]

Електронна звітність для ПП СЦ "Сервіс Майстер" включає такі типи звітності: Податкова звітність, фінансова звітність, звіти про заробітну плату та соціальні виплати, звіти про запаси, звіти про заборгованість, звіти про кредиторську та дебіторську заборгованість, звіти про фінансовий аналіз.

Електронна звітність містить звіти та аналітичні документи, які допомагають проводити фінансовий аналіз підприємства. Ці звіти містять показники ефективності, рентабельності, ліквідності та інші фінансові показники, які дозволяють оцінити фінансове становище та ризики підприємства.

Використання електронної звітності спрощує процес складання, зберігання та подання різноманітних звітів, забезпечує точність та надійність фінансової інформації, а також сприяє швидкому та зручному доступу до неї. Важливо мати відповідну бухгалтерську програму або систему, яка підтримує генерацію електронної звітності та відповідає вимогам законодавства.

Ліцензійна версія Windows застосовується як інформаційна технологія для цифровізації обліку та внутрішнього контролю в організації ПП СЦ "Сервіс-майстер". Ця операційна система встановлена на всіх комп’ютерах підприємства.

Вона надає широкий спектр функцій і інструментів, які корисні для автоматизації бізнес-процесів, зберігання та обробки даних, забезпечення безпеки та контролю доступу до інформації.

На досліджуваному підприємстві використовують ліцензійну версію Windows для встановлення спеціалізованого програмного забезпечення для обліку та внутрішнього контролю. Вона дозволяє налаштувати мережу, створити користувачів з різними рівнями доступу, забезпечити захист даних і мережі, регулярно оновлювати систему для отримання нових функцій і заходів безпеки.

Використання POS-терміналів: Для здійснення безготівкових операцій ПП СЦ "Сервіс Майстер" використовує POS-термінали. Це дозволяє зменшити кількість готівки в обігу та забезпечити швидкий та точний облік операцій.

Використання POS-терміналів (Point of Sale) є поширеною практикою в багатьох підприємствах, включаючи й ПП СЦ "Сервіс-Майстер". POS-термінали є електронними пристроями, які дозволяють здійснювати оплату за товари та послуги безготівковими засобами, такими як кредитні або дебетові картки. Вони забезпечують швидкий, зручний та безпечний процес оплати для клієнтів.

Основні переваги використання POS-терміналів для ПП СЦ "Сервіс-Майстер" подано на рисунку 1.1.

Загалом використання POS-терміналів допомагає ПП СЦ "Сервіс-Майстер" покращити ефективність своєї діяльності, забезпечити швидку та зручну оплату, зменшити ризики та підвищити задоволення клієнтів.

Використання CRM-систем: Для підтримки взаємодії з клієнтами ПП СЦ "Сервіс Майстер" використовує CRM-системи. Це дозволяє забезпечити ефективний та швидкий облік взаємодії з клієнтами. Основні переваги використання CRM-систем у досліджуваній компанії подано на рисунку 1.2

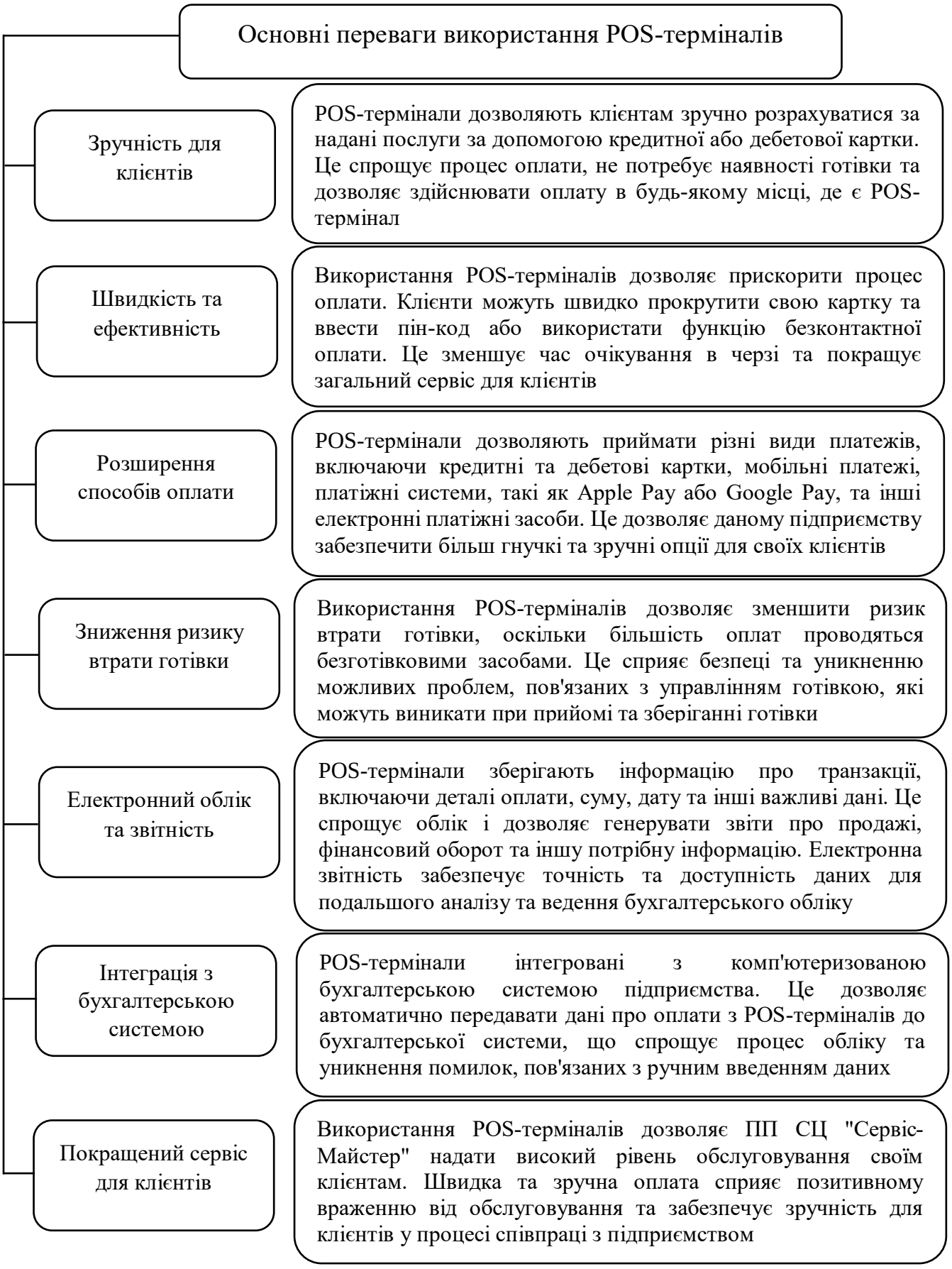


Рисунок 1.1 – Основні переваги використання POS-терміналів

Джерело: розроблено автором на основі [20]

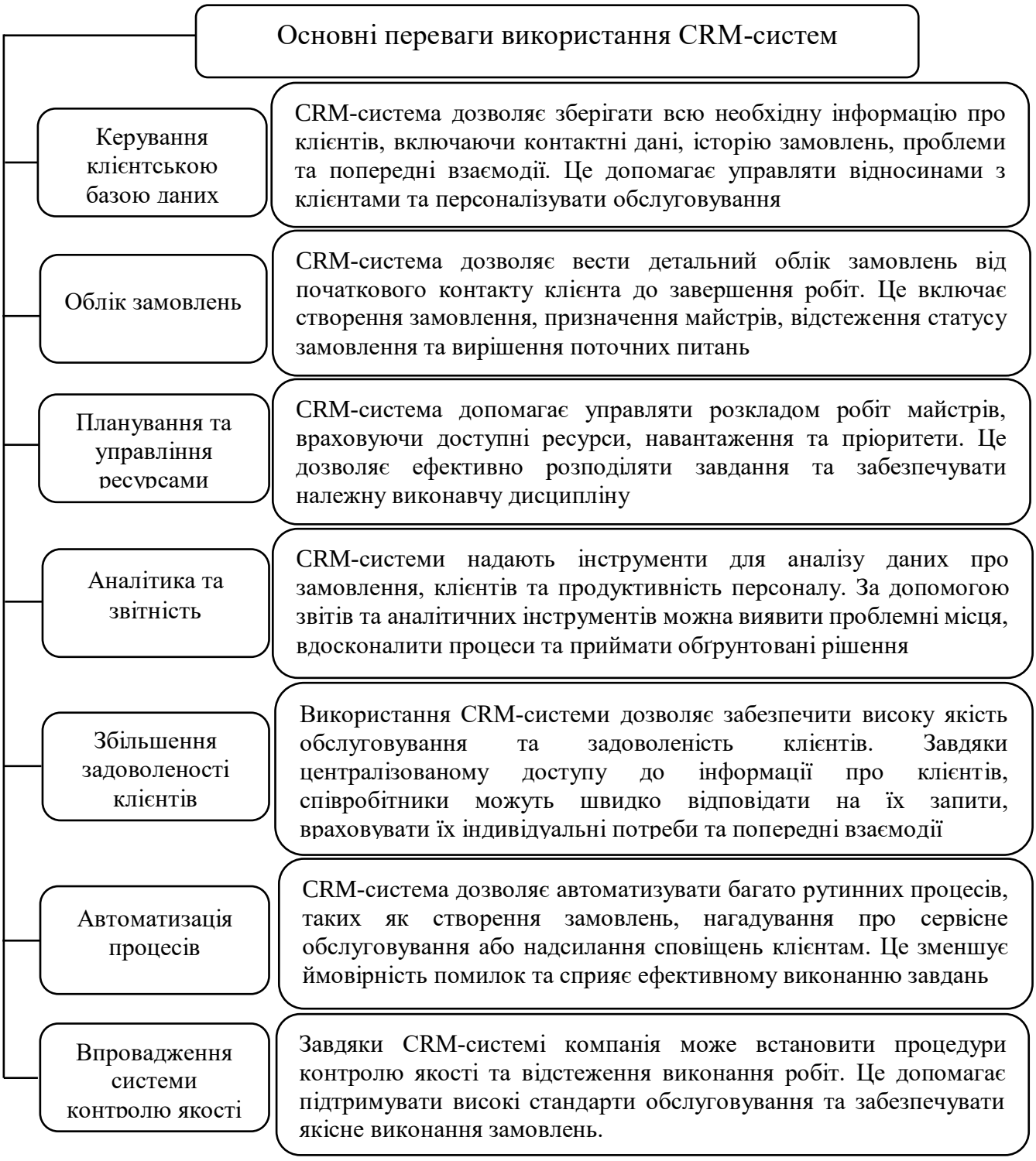


Рисунок 1.2 – Переваги використання CRM-систем

Джерело: розроблено автором на основі [20]

Використання CRM-систем в ПП СЦ "Сервіс-Майстер" допомагає упорядковувати процеси обслуговування клієнтів, покращує комунікацію та ефективність роботи, сприяє зростанню задоволеності клієнтів та покращенню загальної продуктивності компанії.

Система автоматизації обліку ПП СЦ "Сервіс-Майстер" є комплексним програмним рішенням, спеціально розробленим для потреб сервісного центру. Основною метою такої системи є полегшення та оптимізація процесів обліку, управління, взаємодії з клієнтами та роботи сервісного центру загалом.

Основні функції системи автоматизації обліку включають:

Клієнтський портал: Система має веб-інтерфейс для клієнтів, де вони можуть реєструвати свої заявки на ремонт, перевіряти статус ремонту, отримувати повідомлення про готовність, сплачувати рахунки тощо.

Облік заявок: Система дозволяє реєструвати, відстежувати та керувати заявками на ремонт в сервісному центрі. Інформація про заявку, така як опис проблеми, пристрій, гарантійний термін, історія обслуговування тощо, може бути збережена в централізованій базі даних.

Управління запасними частинами: Система включає інвентаризацію та управління запасними частинами, що використовуються для ремонту. Запасні частини можуть бути відстежені, замовлені у постачальників та контрольовані залишки на складі.

Розрахунки та фінансовий облік: Система може автоматизувати розрахунки з клієнтами, формувати рахунки на оплату, виставляти акти виконаних робіт. Також можуть бути включені звіти про фінансову діяльність сервісного центру.

Аналітика та звітність: Система може надавати звіти та аналітичні дані на основі зібраних даних. Це може включати звіти про кількість заявок, тривалість ремонтів, ефективність роботи співробітників, фінансові показники, задоволення клієнтів тощо. Аналітична інформація допомагає керівництву сервісного центру зробити обґрунтовані рішення для покращення ефективності та якості обслуговування.

Керування робочими процесами: Система може допомагати впорядковувати та автоматизувати робочі процеси в сервісному центрі, наприклад, планування робочого графіка, розподіл завдань між співробітниками, контроль термінів виконання робіт.

Збереження клієнтської інформації: Система може зберігати дані про клієнтів, їхні пристрої, історію обслуговування, контактну інформацію тощо. Це дозволяє забезпечити персоналу доступ до необхідної інформації при обробці заявок і забезпечити більш індивідуальний та персоналізований підхід до кожного клієнта.

1.3 Принципи та організація захисту інформації у системі обліку та внутрішнього контролю підприємства

Захист інформації є дуже важливим у сучасному світі, де технології та інтернет відіграють ключову роль на будь-якому підприємстві.

Законодавча база з інформаційної безпеки в Україні включає кілька ключових законодавчих актів, які були прийняті з метою забезпечення безпеки в кіберпросторі.

Одним з ключових законів є Закон України «Про основні засади забезпечення кібербезпеки України». Цей закон визначає правові та організаційні засади забезпечення кібербезпеки в Україні. Він регулює питання щодо захисту критичної інформації, кіберінфраструктури та мереж зв'язку від кіберзагроз. Закон також встановлює відповідальність за порушення кібербезпеки та визначає процедури реагування на кіберінциденти [9].

Та закон України "Про захист персональних даних". Цей закон встановлює правила щодо збору, обробки та захисту персональних даних громадян, а також встановлює відповідальність за їхнє порушення [10].

Система обліку та внутрішнього контролю у ПП СЦ "Сервіс-Майстер" має на меті забезпечити високий рівень захисту інформації в організації. Для цього застосовуються різноманітні принципи та організаційні заходи.

Принципи та організація захисту інформації в системі обліку та внутрішнього контролю підприємства є важливими аспектами для забезпечення конфіденційності, цілісності та доступності даних [2]. Принципи захисту інформації ПП СЦ «Сервіс-Майстер» включають:

Управління доступом: Встановлення механізмів контролю доступу, таких як унікальні ідентифікатори користувачів, паролі, двофакторна аутентифікація та обмеження прав доступу до системи обліку. Це дозволяє забезпечити, що тільки авторизовані користувачі мають доступ до інформації.

Управління доступом є ключовим принципом та організаційним заходом, що використовується для захисту інформації. Воно забезпечує контроль над тим, хто має доступ до конфіденційної інформації, яким чином та в якому обсязі.

Основні аспекти управління доступом включають:

1) Ідентифікація та аутентифікація визначає, як користувачі ідентифікуються в системі та підтверджують свою автентичність. Зазвичай використовуються комбінації логінів, паролів, біометричних даних, токенів або інших методів для перевірки ідентифікації користувача.

Принцип найменшого можливого привілею (Principle of Least Privilege - PoLP): Цей принцип передбачає, що користувачам надаються тільки необхідні привілеї та рівень доступу для виконання їхніх робочих обов'язків. Це дозволяє обмежити можливість несанкціонованого доступу та мінімізувати ризики.

2) Керування правами доступу включає в себе встановлення і управління правами доступу до різних ресурсів інформаційної системи. Він забезпечує можливість надавати або відкликати доступ до файлів, папок, додатків, баз даних тощо в залежності від потреб користувачів та їхніх ролей.

3) Аудит та моніторинг доступу включає систематичний аудит та моніторинг дій користувачів в системі. Це дозволяє виявляти несанкціонований доступ, спроби

порушення безпеки, аномальні поведінки тощо, що допомагає усунути вразливості та запобігти можливим інцидентам безпеки.

4) Фізичний контроль доступу: Досягнення безпеки інформації також вимагає захисту фізичного доступу до комп'ютерних систем, серверних приміщень, дата-центрів тощо. Використання фізичних бар'єрів, електронних замків, систем відеоспостереження та інших засобів контролю допомагає управляти фізичним доступом та забезпечити безпеку інформації [13].

Ефективне управління доступом допомагає уникнути несанкціонованого доступу до конфіденційної інформації, забезпечує цілісність даних та конфіденційність, а також сприяє виконанню регуляторних вимог щодо безпеки даних.

5) Проведення оцінки ризиків пов'язаних з конфіденційністю, цілісністю та доступністю даних. Це дозволяє визначити потенційні загрози та уразливості системи обліку та внутрішнього.

Аналіз ризиків є важливим принципом та організаційним заходом, який використовується для захисту інформації на досліджуваному підприємстві. Цей процес допомагає ідентифікувати потенційні загрози безпеці інформації, оцінювати їх вплив і вірогідність виникнення, а також розробляти та впроваджувати стратегії мінімізації ризиків. Основні етапи аналізу ризиків наведені в таблиці 1.5.

Таблиця 1.5. - Основні етапи аналізу ризиків

№ п/п	**Етапи аналізу ризиків**	**Характеристика етапу**
1	Ідентифікація загроз	Виявлення потенційних загроз безпеці інформації, таких як злам, виток даних, фізичні атаки, соціальний інжиніринг і т. д. Це включає огляд існуючих систем безпеки, аналіз інцидентів безпеки та оцінку вразливостей
2	Оцінка ризиків	Визначення впливу загроз на безпеку інформації та вірогідності їх виникнення. Це вимагає кількісної або якісної оцінки ризиків на основі доступних даних та експертної оцінки

Продовження таблиці 1.5

3	Ранжування ризиків	Упорядкування ризиків за їх важливістю або пріоритетністю. Це допомагає зосередити зусилля на найбільш значущих загрозах та прийняти необхідні заходи для їх управління.
4	Розробка стратегій управління ризиками:	Визначення і впровадження заходів для зниження ризиків. Це можуть бути технічні, організаційні або адміністративні заходи, такі як встановлення файрволів, шифрування даних, політик доступу та навчання персоналу.
5	Моніторинг та перегляд:	Постійне спостереження за змінами в загрозах та ефективності прийнятих заходів. Регулярний аналіз ризиків дозволяє виявляти нові загрози та вдосконалювати стратегії управління ризиками.

Джерело: розроблено автором на основі [25]

6) Розробка та впровадження політик безпеки, які встановлюють правила та процедури використання інформації, захисту паролів, контролю доступу та інші аспекти безпеки. Ці політики повинні бути чіткими, добре відомими та дотримуватися всіма працівниками.

Політика безпеки є важливим принципом та організаційним заходом, який використовується для захисту інформації в організації. Вона визначає набір правил, процедур і рекомендацій, що стосуються безпеки інформації та встановлює вимоги щодо захисту конфіденційності, цілісності та доступності даних. Основні цілі політики безпеки наведені в таблиці 1.6.

Таблиця 1.6. - Основні цілі політики безпеки

№ п/п	**Основні цілі політики безпеки**	**Характеристика цілі політики безпеки**
1	Захист конфіденційності	Політика безпеки встановлює правила та процедури для забезпечення конфіденційності інформації. Вона визначає, які типи інформації є конфіденційними, хто має доступ до цієї інформації та як її захищати від несанкціонованого доступу.
2	Збереження цілісності даних	Політика безпеки встановлює правила для забезпечення цілісності даних, що означає, що інформація повинна залишатися незмінною та точною. Вона включає в себе контроль за змінами даних, застосування електронних підписів та інші заходи для запобігання незаконній або неправомірній модифікації даних.

Продовження таблиці 1.6

3	Забезпечення доступності	Політика безпеки визначає заходи для забезпечення доступності інформації для авторизованих користувачів. Вона включає в себе резервне копіювання даних, створення систем резервування та відновлення, а також заходи для запобігання відмовам у обслуговуванні та забезпечення надійності системи.
4	Управління доступом	Політика безпеки встановлює правила та процедури для управління доступом до інформації. Вона визначає, які користувачі мають доступ до певних видів інформації, які права доступу вони мають, і як цей доступ контролюється та аудитується.
5	Свідомість та навчання	Політика безпеки також включає в себе заходи для підвищення свідомості та навчання співробітників щодо питань інформаційної безпеки. Це може включати навчання про правила безпеки, освіту щодо соціального інжинірингу, фішингу та інших загроз, а також навчання користувачів щодо використання безпечних паролів та заходів захисту даних.

Джерело: розроблено автором на основі [25]

Важливо, щоб політика безпеки була регулярно переглянута, оновлювана та виконувана всіма співробітниками організації. Вона повинна бути гнучкою і пристосованою до змін у загрозах і технологіях, щоб забезпечити ефективний захист інформації.

7) Захист фізичного обладнання, що містить систему обліку та внутрішнього контролю, шляхом обмеження фізичного доступу до серверних кімнат та інших приміщень. Це може включати в себе встановлення систем відеоспостереження, контроль входу та виходу, а також забезпечення безпеки даних під час транспортування.

Фізична безпека є важливим принципом та організаційним заходом, який використовується для захисту інформації. Цей підхід спрямований на запобігання несанкціонованому фізичному доступу до фізичних об'єктів, приміщень, пристроїв та систем, де зберігається або обробляється інформація. Основні аспекти фізичної безпеки наведено у таблиці 1.7.

Фізична безпека доповнює технічні та організаційні заходи, що використовуються для захисту інформації, і є важливим елементом повноцінної стратегії безпеки даних і систем.

Таблиця 1.7. - Основні аспекти фізичної безпеки

Вид фізичної безпеки	**Характеристика**
Фізичний доступ та обмеження	передбачає контроль над фізичним доступом до будівель, приміщень та інших фізичних об'єктів, де знаходиться інформація. Використання фізичних бар'єрів, які можуть включати брами, замки, карти доступу, біометричні системи, дозволяє обмежити доступ лише авторизованим особам.
Відеоспостереження	допомагає відслідковувати та записувати дії, що відбуваються в приміщеннях або на території, де розташована інформація. Це не тільки допомагає виявити потенційні загрози або порушення безпеки, але й служить важливим доказом в разі розслідування інцидентів.
Захист від несанкціонованого доступу	включає заходи для запобігання фізичному злому або несанкціонованому доступу до приміщень, серверних кімнат, комунікаційних кабелів тощо. Це можуть бути захисні системи, такі як системи тривоги, фізичні бар'єри, контроль доступу та інші заходи безпеки.
Захист обладнання та носіїв інформації	для забезпечення фізичної безпеки інформації важливо враховувати захист обладнання, яке обробляє або зберігає дані, а також носіїв інформації, таких як сервери, комп'ютери, флеш-накопичувачі, жорсткі диски тощо. Це може включати захист від фізичних пошкоджень, крадіжок або незаконного використання.
Евакуаційні плани та відновлення після інциденту	охоплює ситуації надзвичайного стану, пожежі, природні катастрофи та інші загрози. Крім того, необхідно мати плани відновлення після інциденту для відновлення фізичного доступу та відновлення роботи систем та інфраструктури після випадків порушення безпеки.

Джерело: розроблено автором на основі [25]

8) Забезпечення безпеки мережі шляхом використання механізмів шифрування даних, встановлення брандмауерів, мережевих апаратних пристроїв та систем виявлення вторгнень. Регулярне оновлення програмного забезпечення та застосування заходів для запобігання атакам зламу мережі.

Захист мережі є ключовим принципом та організаційним заходом, який використовується для захисту інформації. Враховуючи постійний розвиток технологій та зростаючі загрози в сфері кібербезпеки, ефективний захист мережі є необхідним для забезпечення конфіденційності, цілісності та доступності даних.

Основні аспекти захисту мережі наведено в таблиці 1.8.

Таблиця 1.8. - Основні аспекти захисту мережі

Основні аспекти захисту мережі	**Характеристика**
Файрволи	Використання файрволів дозволяє контролювати трафік, який входить і виходить з мережі. Файрволи надають можливість встановлювати правила, які обмежують доступ до ресурсів мережі залежно від джерела, призначення, портів та інших параметрів, що допомагає уникнути несанкціонованого доступу та зберегти безпеку мережі.
Віртуальні приватні мережі (Virtual Private Networks - VPNs)	VPN-підключення забезпечують захищений тунель між віддаленими мережами або користувачами, що працюють з мережі зовнішнім чином. Вони шифрують трафік і забезпечують конфіденційність даних під час передачі через незахищені мережі, такі як Інтернет.
Аутентифікація та авторизація	Використання механізмів аутентифікації та авторизації дозволяє контролювати доступ користувачів до ресурсів мережі. Це може включати використання паролів, ідентифікаторів, біометричних методів аутентифікації та ролей для обмеження привілеїв користувачів.
Захист від вторгнень (Intrusion Prevention Systems - IPS)	IPS використовуються для виявлення та запобігання вторгненням в мережу. Вони аналізують мережевий трафік на наявність шкідливих або підозрілих дій та приймають заходи для блокування такого трафіку або сповіщення адміністраторів про потенційну загрозу.
Оновлення та патчі	Регулярні оновлення програмного забезпечення, операційних систем, мережевих пристроїв та застосунків є важливим кроком для захисту мережі. Вони допомагають усувати вразливості та уникати використання зловмисниками відомих вразливостей.
Моніторинг та журналювання	Системи моніторингу та журналювання відслідковують події та активність в мережі для виявлення аномальної поведінки або можливих загроз. Це дозволяє оперативно реагувати на потенційні інциденти та проводити розслідування.

Джерело: розроблено автором на основі [25]

Захист мережі вимагає поєднання технічних та організаційних заходів, таких як правильна конфігурація мережевих пристроїв, шифрування трафіку, навчання персоналу щодо кібербезпеки та розробки політик безпеки. Це сприяє підвищенню рівня захищеності мережі та забезпеченню безпеки інформації.

9) Регулярне створення резервних копій даних системи обліку та внутрішнього контролю, щоб забезпечити можливість відновлення даних у разі випадку втрати або пошкодження.

Резервне копіювання є важливим принципом та організаційним заходом, який використовується для захисту інформації. Воно передбачає створення копій даних та збереження їх на віддалених або незалежних носіях з метою відновлення інформації у разі втрати, пошкодження або несанкціонованого доступу до основних джерел даних. Основні аспекти резервного копіювання наведено у таблиці 1.9.

Таблиця 1.9. – Організаційні заходи резервного копіювання

Організаційні заходи резервного копіювання	**Результат використання**
Регулярність	Ефективна стратегія резервного копіювання передбачає регулярне виконання процесу копіювання для забезпечення актуальності інформації. Відповідність графіку копіювання до частоти змін даних дозволяє мінімізувати втрату інформації в разі відновлення.
Збереження на віддалених носіях	Копії даних повинні бути збережені на віддалених медіа або системах зберігання. Це дозволяє уникнути втрати даних в разі фізичних або природних катастроф, крадіжок або інших подібних інцидентів.
Перевірка цілісності та доступності	Крім створення копій даних, важливо періодично перевіряти цілісність та доступність резервних копій. Це може бути здійснено шляхом проведення регулярних перевірок, тестів відновлення або перевірки цифрових підписів.
Захист доступу до резервних копій	Резервні копії мають бути захищені від несанкціонованого доступу. Використання шифрування та контролю доступу до копій даних допомагає забезпечити конфіденційність та інтегрітет інформації.
Тестування та відновлення	Резервні копії повинні бути періодично тестовані та перевірятись на можливість успішного відновлення даних. Це дозволяє переконатись в ефективності стратегії резервного копіювання та готовності до відновлення в разі потреби.

Джерело: розроблено автором на основі [25]

Резервне копіювання є важливим елементом стратегії захисту інформації, оскільки допомагає зменшити ризик втрати даних та забезпечити можливість відновлення після небажаного інциденту.

10) Проведення навчань та інформування працівників про загрози безпеки, політики безпеки та процедури, а також про правильні методи роботи з інформацією. Свідомість персоналу про ризики та практики безпеки є важливим елементом в захисті інформації.

Навчання та свідомість персоналу є важливим принципом та організаційним заходом, який використовується для захисту інформації. Люди є одним з найсуттєвіших факторів в системі безпеки, і правильне навчання та підвищення свідомості персоналу можуть значно зменшити ризик витоку, несанкціонованого доступу або втрати конфіденційної інформації. Основні аспекти навчання та свідомості персоналу наведені у таблиці 1.10.

Таблиця 1.10 - Організаційні заходи навчання та свідомості персоналу

Основні аспекти навчання та свідомості персоналу	**Шляхи реалізації**
Курси з кібербезпеки	Навчання персоналу про основні принципи кібербезпеки, загрози та захисні заходи є важливим етапом. Це може включати організацію обов'язкових курсів з кібербезпеки, де співробітники ознайомлюються з основними правилами безпеки, розпізнаванням шкідливих елементів, захистом паролів та процедурами повідомлення про інциденти.
Створення політик безпеки	Організація повинна розробити чітку політику безпеки, яка включатиме в себе правила щодо використання паролів, доступу до систем та даних, обмеження використання зовнішніх пристроїв та інші безпечні практики. Всі працівники повинні бути ознайомлені з політикою і відповідальністю за дотримання її вимог.
Свідоме використання електронної пошти та Інтернету	Працівники повинні бути навчені про ризики, пов'язані з небезпечними електронними листами, фішинговими атаками та шкідливими посиланнями. Вони повинні бути остережними та практикувати безпечне використання електронної пошти та Інтернету, уникати невідомих або підозрілих джерел та не передавати конфіденційну інформацію без необхідності.
Сильні паролі та багаторівнева аутентифікація	Працівники повинні бути навчені про важливість використання сильних паролів і регулярну їх зміну. Також варто впровадити багаторівневу аутентифікацію (наприклад, використання двохфакторної аутентифікації), щоб забезпечити додатковий шар захисту.
Свідоме використання зовнішніх пристроїв	Працівники повинні бути навчені про ризики використання зовнішніх пристроїв, таких як USB-накопичувачі або зовнішні жорсткі диски. Важливо дотримуватись політики щодо використання цих пристроїв і перевіряти їх на наявність потенційно шкідливих програм або вірусів.

Джерело: розроблено автором на основі [25]

Навчання та свідомість персоналу допомагають збільшити усвідомлення про кібербезпеку та впровадження безпечних практик у робочому середовищі. Вони

доповнюють технічні заходи безпеки та створюють міцний колективний захист інформації в організації.

11) Проведення систематичного аудиту та моніторингу системи обліку та внутрішнього контролю для виявлення потенційних загроз безпеці та порушень безпекових політик. Це дозволяє швидко виявляти та реагувати на вразливості та атаки.

Аудит та моніторинг є важливим принципом та організаційним заходом, який використовується для захисту інформації. Вони допомагають виявляти потенційні загрози, слабкі місця та несанкціоновані дії в системі інформаційної безпеки. Основні аспекти аудиту та моніторингу наведено у таблиці 1.11.

Таблиця 1.11. - Основні аспекти аудиту та моніторингу

Вид організаційного заходу	**Характеристика організаційного заходу**
Аудит систем безпеки	Аудит систем безпеки включає періодичну оцінку технічних та організаційних заходів безпеки, таких як конфігурація мережі, керування доступом, шифрування даних тощо. Аудит допомагає перевірити відповідність системи безпеки стандартам, політикам та нормативним вимогам, а також виявляти можливі уразливості та слабкі місця.
Моніторинг системи	Моніторинг системи передбачає постійне спостереження за подіями, діями та взаємодією в мережі та інформаційних системах. Це включає виявлення та реагування на підозрілі активності, спроби несанкціонованого доступу, вторгнення або аномалії в системі. Моніторинг допомагає вчасно виявляти інциденти безпеки та вживати відповідних заходів для їх припинення.
Журналювання та аналіз журналів	Системи безпеки повинні мати механізми журналювання, які реєструють події та дії в системі. Журнали допомагають відстежувати активності користувачів, виявляти несподівані події та аналізувати їх для виявлення потенційних загроз або вразливостей.

Джерело: розроблено автором за матерыалами [25]

Аудит та моніторинг допомагають виявляти порушення безпеки, вчасно реагувати на них та приймати відповідні заходи для запобігання подібним інцидентам у майбутньому. Ці заходи забезпечують постійний контроль над системою інформаційної безпеки, що допомагає забезпечити конфіденційність, цілісність та доступність інформації.

12) Система захисту інформації повинна постійно вдосконалюватися, враховуючи нові загрози та технології. Важливо слідкувати за оновленнями безпекових патчів, використовувати сучасні методи шифрування та інші заходи для підтримки високого рівня безпеки.

Постійне вдосконалення є важливим принципом та організаційним заходом, який використовується для захисту інформації. З урахуванням постійно змінюючогося кіберзлочинного середовища та нових технологій, організації повинні активно вдосконалювати свої практики безпеки, процедури та технології. Основні складові постійного вдосконалення системи захисту інформації наведено у таблиці 1.12.

Таблиця 1.12. - Основні складові вдосконалення систем захисту інформації

Основні складові вдосконалення систем захисту інформації	**Характеристика**
Оцінка ризиків	Регулярна оцінка ризиків дозволяє виявляти нові загрози та потенційні вразливості. Організації повинні проводити оцінку ризиків та аналізувати потенційні наслідки інцидентів, щоб виявити слабкі місця та прийняти необхідні заходи для захисту інформації.
Оновлення політик та процедур	Політики та процедури безпеки повинні бути регулярно оглядані та оновлювані для врахування нових загроз та вимог. Це може включати вдосконалення паролів, правил доступу, шифрування даних та інших безпечних практик.
Технічне оновлення	Організації повинні відстежувати оновлення програмного забезпечення, операційних систем та інших технологій, які використовуються для захисту інформації. Важливо встановлювати патчі безпеки та оновлення для заповнення вразливостей, які можуть бути використані зловмисниками.
Свідомість персоналу	Працівники повинні бути постійно навчані та свідомі загроз, оновлених політик та процедур безпеки. Це допомагає підтримувати культуру безпеки в організації та забезпечує вчасну реакцію на потенційні загрози.
Тестування безпеки	Регулярне тестування системи на безпеку є важливою складовою постійного вдосконалення. Це може включати етичне вторгнення (penetration testing), внутрішній аудит безпеки та інші методи перевірки системи на наявність слабких місць.

Джерело: розроблено автором на основі [25]

Постійне вдосконалення допомагає організаціям адаптуватися до нових загроз та забезпечити ефективний захист інформації. Воно підтримує актуальність

заходів безпеки та допомагає зменшити ризики втрати конфіденційності, цілісності та доступності інформації.

13) Використання шифрування для захисту конфіденційної інформації. Шифрування може застосовуватися як при зберіганні даних, так і при передачі через мережу, що дозволяє забезпечити їх конфіденційність у разі несанкціонованого доступу. Види шифрування даних наведено у таблиці 1.13.

Таблиця 1.13. - Види шифрування даних

Види шифрування даних	**Характеристика шифрування даних**
Керування ключами	для шифрування і розшифрування даних використовуються ключі. Ключі повинні бути довгими та складними для запобігання підбору. Керування ключами включає генерацію, зберігання, обмін і знищення ключів у безпечний спосіб.
Захист ключів	ключі повинні зберігатися в безпечному місці з обмеженим доступом. Можуть використовуватися фізичні та логічні заходи безпеки для захисту ключів від несанкціонованого доступу.
Шифрування даних у спокої та під час передачі	дані повинні бути шифровані як у спокої (збережені на сервері або в базі даних), так і під час передачі по мережі. Шифрування даних у спокої забезпечує захист інформації в разі фізичного доступу до носія даних. Шифрування під час передачі дозволяє захистити дані від перехоплення та несанкціонованого доступу під час передачі через мережу.
Аудит та моніторинг	важливим аспектом шифрування даних є проведення аудиту та моніторингу процесу шифрування. Це дозволяє виявити будь-які проблеми або порушення безпеки та прийняти відповідні заходи.

Джерело: розроблено автором на основі [25]

Шифрування даних допомагає забезпечити високий рівень безпеки в системі обліку та внутрішнього контролю, запобігаючи несанкціонованому доступу до конфіденційної інформації та зміні даних під час передачі та зберігання.

Ці принципи організації захисту інформації у системі обліку та внутрішнього контролю підприємства створюють цілісну систему захисту, що забезпечує конфіденційність, цілісність та доступність даних. Процеси захисту повинні бути постійно оновлюваними та піддаватися аудиту для забезпечення ефективності і відповідності стандартам безпеки.

Загальні принципи захисту інформації, такі як необхідний принцип найменшого доступу, шифрування даних, резервне копіювання та відновлення,

контроль цілісності даних та систем, аутентифікація та авторизація користувачів, слідування найкращим практикам у сфері безпеки та використання спеціалізованого програмного забезпечення для захисту, мають важливе значення для інформаційної безпеки підприємства. Загальна мета організації захисту інформації у системі обліку та внутрішнього контролю підприємства полягає в забезпеченні конфіденційності, цілісності та доступності даних, а також у запобіганні втраті даних, несанкціонованому доступу та іншим загрозам безпеці.

РОЗДІЛ 2
СТАН ТА ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ ОБЛІКУ ТА ВНУТРІШНЬОГО КОНТРОЛЮ ПП СЦ «СЕРВІС-МАЙСТЕР»

2.1 Стан системи обліку та внутрішнього контролю щодо її інформаційної забезпеченості та захищеності

Інформаційна безпека системи обліку та внутрішнього контролю є критично важливою для ПП СЦ "Сервіс-Майстер", оскільки підприємство працює зі сторонньою технікою та обробляє конфіденційну інформацію своїх клієнтів. Для забезпечення безпеки даних та ефективного внутрішнього контролю, підприємство вживає наступні заходи які наведено в таблиці 2.1.

Таблиця 2.1. - Заходи забезпечення безпеки даних та ефективного внутрішнього контролю

Заходи забезпечення безпеки даних та ефективного внутрішнього контролю	**Характеристика заходу**
Фізична безпека	Усі комп'ютери, сервери та зберігання даних фізично захищені від несанкціонованого доступу. Застосовуються фізичні заходи безпеки, такі як контроль доступу, системи відеоспостереження. Фізичний доступ до приміщень, де знаходяться комп'ютери, сервери та зберігання даних, обмежений. Також використовуються захисні заходи, такі як електронні кодові замки на дверях. Крім того, серверна кімната має контроль температури та вологості для забезпечення оптимальних умов для обладнання.
Кібербезпека	Усі комп'ютери та мережа захищені від зловмисників за допомогою антивірусних програм.
Резервне копіювання	Вся важлива інформація регулярно резервно копіюється та зберігається на захищених зовнішніх пристроях або в хмарних системах забезпечення безпеки даних. Це забезпечує можливість відновлення даних в разі випадкового видалення або виникнення технічних проблем. Резервні копії важливої інформації створюються регулярно. Вони зберігаються на захищених зовнішніх пристроях, таких як фізичні пристрої зберігання та у хмарних системах забезпечення безпеки даних. Крім того, періодично проводяться перевірки резервних копій для впевненості в їхній доступності та функціональності.

Продовження таблиці 2.1

Доступ до даних	Підприємство обмежує доступ до конфіденційної інформації лише для необхідних працівників. Для запобігання в несанкціонованому доступу до конфіденційної інформації використовуються принципи мінімізації привілеїв. Кожен співробітник має унікальний обліковий запис зі своїми обліковими даними (логіном та паролем), і доступ до конфіденційних даних надається лише на основі необхідності для виконання робочих обов'язків. Крім того, встановлюються правила щодо безпеки паролів, які вимагають складних комбінацій символів та періодичності їх зміни.
Моніторинг	Підприємство використовує систему моніторингу активності на мережевому рівні та на рівні користувачів, щоб виявити потенційні загрози та аномальну активність. Збираються лог-файли з подробицями про вхідні та вихідні підключення, виконані команди та іншу активність. Ці дані аналізуються з використанням спеціалізованих програм, що допомагають виявляти підозрілу діяльність, наприклад, невдалі спроби авторизації або спроби несанкціонованого доступу.
Навчання персоналу	Працівники проходять навчання з питань інформаційної безпеки та внутрішнього контролю. Це включає ознайомлення з правилами використання паролів, усвідомлення загроз безпеці, використання безпечних методів комунікації та поведінку в разі виявлення підозрілої діяльності.

Джерело: розроблено автором на основі [25]

Система обліку та внутрішнього контролю в ПП СЦ "Сервіс-Майстер" демонструє достатній рівень інформаційної забезпеченості та захищеності. Підприємство ретельно враховує фізичну безпеку своїх обладнання та даних, використовуючи контроль доступу до приміщень та спеціалізовані системи замків та карток. Це забезпечує захист від несанкціонованого фізичного доступу до системи обліку та важливих даних, зменшуючи ризик викрадення або пошкодження обладнання.

Що стосується кібербезпеки, підприємство приділяє велику увагу захисту своїх комп'ютерів та мережі від потенційних загроз. Встановлення сучасних антивірусних програм та мережевих брандмауерів, які періодично оновлюються, дозволяє ефективно виявляти та блокувати шкідливі програми та зловмисники. Крім того, використання систем виявлення вторгнень допомагає вчасно виявляти підозрілу активність та запобігати потенційним інцидентам безпеки.

ПП СЦ "Сервіс-Майстер" також піклується про забезпечення резервного копіювання важливої інформації. Регулярне створення резервних копій та їх зберігання на захищених зовнішніх пристроях або в хмарних системах дозволяє забезпечити відновлення даних в разі випадкового видалення або технічних неполадок. Проведення перевірок резервних копій дозволяє переконатися в їхній доступності та цілісності, забезпечуючи відновлення системи у випадку потенційних проблем.

ПП СЦ "Сервіс-Майстер" також ретельно контролює доступ до конфіденційної інформації. Застосування принципу мінімізації привілеїв та встановлення правил безпеки паролів допомагають запобігати несанкціонованому доступу до важливих даних. Кожен співробітник має унікальний обліковий запис, і доступ до конфіденційних даних надається тільки на основі необхідності для виконання робочих обов'язків. Це забезпечує високий рівень захищеності даних та убезпечує їх від несанкціонованого розголошення чи втрати.

Загалом, ПП СЦ "Сервіс-Майстер" виконує різноманітні заходи забезпечення інформаційної безпеки та захищеності системи обліку та внутрішнього контролю. Це дозволяє підприємству ефективно захищати конфіденційну інформацію, запобігати втратам даних та забезпечувати безперебійне функціонування своїх робочих процесів.

Ці превентивні та захисні заходи створюють надійне середовище для функціонування системи обліку та внутрішнього контролю, забезпечуючи відповідність нормам безпеки та регуляторним вимогам. ПП СЦ "Сервіс-Майстер" демонструє свою зосередженість на важливості інформаційної безпеки та внутрішнього контролю, що сприяє підвищенню довіри клієнтів, забезпеченню надійності роботи та успішному функціонуванню підприємства у галузі ремонту побутової техніки.

2.2 Потенційні загрози та ризики для інформаційної безпеки системи обліку та внутрішнього контролю для ПП СЦ «Сервіс-Майстер»

Система обліку та внутрішнього контролю в ПП СЦ "Сервіс-Майстер" може стикатися з різноманітними потенційними загрозами для інформаційної безпеки. Нижче наведено основні з них:

1) Кібератаки**:** Зловмисники можуть спробувати проникнути в систему обліку та внутрішнього контролю шляхом використання різних технік, таких як введення шкідливого програмного забезпечення, фішингові атаки, DDoS-атаки тощо. Це може призвести до несанкціонованого доступу до конфіденційної інформації, втрати даних або недоступності системи.

Кібератаки є серйозним ризиком для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер». Такі атаки можуть мати наступні наслідки, наведено у таблиці 2.2.

Таблиця 2.2. - Можливі наслідки кібератак

Наслідки кібератак	Ризик для інформаційної безпеки
Витрати	Кібератаки можуть призвести до фінансових втрат через втрату чутливої інформації, пошкодження систем або втрату даних. Відновлення після кібератаки може також вимагати значних витрат на відновлення систем та розслідування події.
Втрата даних	Злочинці можуть спробувати вкрасти або пошкодити важливу інформацію, яка зберігається в системі обліку та внутрішнього контролю. Це може призвести до втрати даних, що може вплинути на роботу компанії та призвести до негативних наслідків для клієнтів і партнерів.
Порушення конфіденційності	У разі успішної кібератаки злочинці можуть отримати доступ до конфіденційної інформації, такої як особисті дані клієнтів, фінансові документи, патенти або комерційні таємниці. Це може призвести до порушення конфіденційності і привести до негативного впливу на довіру клієнтів та партнерів.
Пошкодження репутації	Кібератаки можуть суттєво підірвати репутацію ПП СЦ «Сервіс-Майстер». Втрата конфіденційності, втрата даних або нездатність забезпечити безпеку інформації можуть призвести до втрати довіри клієнтів та партнерів, а також до негативного впливу на ринкову позицію компанії.
Юридичні наслідки	Кібератаки можуть мати юридичні наслідки для ПП СЦ «Сервіс-Майстер». Залежно від країни та її законодавства, компанія може зазнати штрафів, позовів або інших правових наслідків внаслідок витоку інформації або недостатньої захищеності системи.

Джерело: розроблено автором на основі [13]

Отже, важливо вжити всіх необхідних заходів для захисту системи обліку та внутрішнього контролю від кібератак. Це включає використання сучасних технологій безпеки, регулярні аудити безпеки, навчання персоналу правилам кібербезпеки та усвідомленням потенційних загроз.

2) Витік інформації: Недостатня безпека системи може призвести до витоку конфіденційної інформації про клієнтів, співробітників або внутрішніх процесів компанії. Це може призвести до порушення довіри клієнтів, втрати репутації компанії та можливих правових наслідків.

Витік інформації є серйозною загрозою для інформаційної безпеки будь-якої організації, включаючи систему обліку та внутрішнього контролю. У випадку ПП СЦ «Сервіс-Майстер», витік інформації може мати наступні наслідки, наведено у таблиці 2.3.

Таблиця 2.3. – Наслідки витоку інформації

Витік інформації	**Наслідки витоку інформації**
Втрата конфіденційності	Якщо конфіденційна інформація, така як фінансові дані, договори, клієнтська база або інші конфіденційні дані, витікає, це може призвести до негативних наслідків. Конкуренти можуть отримати доступ до цієї інформації і використовувати її для своїх переваг. Крім того, це може порушити довіру клієнтів і призвести до втрати бізнесу.
Порушення цілісності даних	Витік інформації може призвести до незаконного доступу до системи обліку та внутрішнього контролю, що може призвести до порушення цілісності даних. Хакери або зловмисники можуть змінити дані, внести фальшиву інформацію або знищити важливі дані, що може призвести до серйозних проблем з управлінням та контролем.
Зниження доступності	Витік інформації може спричинити проблеми з доступністю системи обліку та внутрішнього контролю. Наприклад, якщо хакери атакують систему або витікають конфіденційні дані, це може призвести до зупинки системи або її недоступності для користувачів. Це може вплинути на продуктивність бізнесу та послуги, які надає ПП СЦ «Сервіс-Майстер».
Втрата репутації	Якщо стає відомо про витік інформації з системи обліку та внутрішнього контролю, це може призвести до серйозного пошкодження репутації ПП СЦ «Сервіс-Майстер». Втрата довіри клієнтів і партнерів може мати довготривалі наслідки і негативно впливати на бізнес організації.

Джерело: розроблено автором на основі [13]

Загальна увага до інформаційної безпеки і прийняття необхідних заходів допоможуть зменшити ризик витоку інформації та зберегти інформаційну безпеку системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер».

3) Недостатня аутентифікація та авторизація: Якщо система обліку та внутрішнього контролю має слабкі механізми аутентифікації і авторизації, зловмисники можуть здійснити несанкціонований доступ до системи або підмінити права доступу, що дозволяє їм отримувати несанкціонований доступ до конфіденційної інформації або змінювати дані. Недостатня аутентифікація та авторизація є серйозною загрозою для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер". Відсутність адекватної аутентифікації та авторизації може призвести до втрати даних або пошкодження системи. Основні загрози та ризики пов'язані з недостатньою аутентифікацією та авторизацією наведено у таблиці 2.4.

Таблиця 2.4. - Загрози та ризики пов'язані з недостатньою аутентифікацією та авторизацією

Загрози та ризики пов'язані з недостатньою аутентифікацією та авторизацією	**Характеристика**
Підкреслена ідентичність	Зловмисники можуть намагатися піддурити систему, претендуючи на ідентичність інших користувачів або проникнення до облікових записів з правами доступу. Якщо аутентифікаційні механізми не ефективні, зловмисники можуть отримати неправомірний доступ до системи і виконувати дії, що становлять загрозу.
Слабкі паролі	Якщо система допускає використання слабких або легко вгадуваних паролів, зловмисники можуть легко підібрати або зламати паролі користувачів і отримати доступ до системи. Слабкі паролі, такі як "123456" або "password", зроблять систему уразливою до атак.
Недостатній рівень авторизації	Якщо система не використовує належні механізми авторизації, зловмисники можуть отримати доступ до функцій і ресурсів, до яких не мають права. Це може призвести до несанкціонованого доступу до конфіденційної інформації або зміни важливих налаштувань системи.
Мережеві атаки	Зловмисники можуть використовувати недостатню аутентифікацію та авторизацію для здійснення мережевих атак, таких як перехоплення сеансів, маніпулювання даними або введення шкідливих кодів у систему.

Джерело: розроблено автором на основі [13]

Приділення належної уваги аутентифікації та авторизації в системі обліку та внутрішнього контролю є ключовим для забезпечення конфіденційності, цілісності та доступності даних, а також для збереження довіри клієнтів та доброї репутації організації.

4) Соціальний інжиніринг: Соціальний інжиніринг є серйозною загрозою для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер". Соціальний інжиніринг - це маніпуляція людьми з метою отримання неправомірного доступу до конфіденційної інформації або виконання шкідливих дій.

Основна ідея соціального інжинірингу полягає в тому, щоб використовувати вразливості людського фактору для отримання доступу до системи або конфіденційної інформації. Це може включати підманювання співробітників під час телефонних розмов, електронних листів або особистих зустрічей, щоб вони розкрили свої паролі, надали доступ до комп'ютера або надіслали конфіденційну інформацію.

Наприклад, хакер може використовувати метод фішингу, надсилаючи співробітнику електронний лист, який видаватиме себе за легітимне повідомлення від внутрішнього відділу підтримки, вимагаючи оновити пароль або надати доступ до системи. Якщо співробітник упадеться на цю пастку і надасть свої облікові дані, хакер отримає доступ до системи.

Інший приклад - соціальний інжиніринг через особистий контакт. Хакер може намагатися стати знайомим зі співробітниками ПП СЦ "Сервіс-Майстер" під прикриттям іншої особи або використовуючи підроблені облікові записи в соціальних мережах. Завдяки цьому він може отримати доступ до довірливої інформації або переконати співробітників здійснити дії, які можуть пошкодити систему обліку та внутрішнього контролю.

5) Внутрішні загрози: Усередині організації можуть бути співробітники, які зловживають своїми привілеями та доступом до системи обліку та внутрішнього

контролю. Вони можуть незаконно змінювати дані, викривати конфіденційну інформацію або порушувати процедури контролю.

Внутрішні загрози є серйозними ризиками для інформаційної безпеки системи обліку та внутрішнього контролю в будь-якій організації, включаючи ПП СЦ "Сервіс-Майстер". Внутрішні загрози виникають всередині самої організації і можуть бути спричинені працівниками, керівництвом, сторонніми підрядниками або іншими особами з доступом до системи обліку та внутрішнього контролю.

Ось деякі приклади внутрішніх загроз, які можуть вплинути на інформаційну безпеку системи обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер" , наведено у таблиці 2.5.

Таблиця 2.5 - Приклади внутрішніх загроз та їх вплив на інформаційну безпеку системи обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер"

Внутрішні загрози	**Характеристика внутрішніх загроз та їх вплив на інформаційну безпеку**
Несанкціонований доступ до даних	Працівники, які мають привілеї доступу до системи, можуть використовувати свої повноваження для незаконного доступу до конфіденційної інформації. Наприклад, вони можуть використовувати цей доступ для отримання конкурентної переваги або для зловживання інформацією з метою шахрайства.
Втрати даних	Недбалість або зловмисний умисел працівників може призвести до втрати даних. Це може бути через неправильну обробку, випадкове видалення або відсутність адекватних заходів з резервного копіювання.
Витік конфіденційної інформації	Працівники можуть намагатися використовувати або розголошувати конфіденційну інформацію поза організацією. Це може бути навмисна дія, щоб продати інформацію конкурентам або для особистої вигоди.
Слабкі паролі та недостатня автентифікація	Якщо працівники використовують слабкі паролі або ігнорують процедури автентифікації, це може сприяти несанкціонованому доступу до системи.
Зловживання повноважень	Працівники, які мають великі повноваження в системі обліку та внутрішнього контролю, можуть зловживати цими повноваженнями для зміни даних, зміни прав доступу або знищення аудиторських слідів.

Джерело: розроблено автором на основі [13]

Важливо постійно моніторити та оновлювати безпекові заходи, щоб зменшити ризик внутрішніх загроз і підвищити рівень інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер", оскільки загрози постійно еволюціонують.

6) Недостатня оновлення та патчі безпеки: Якщо система обліку та внутрішнього контролю не оновлюється регулярно або не встановлюються необхідні патчі безпеки, вона може стати вразливою перед новими видами кіберзагроз або експлойтами, які можуть бути використані зловмисниками.

Недостатнє оновлення та патчі можуть становити серйозну загрозу для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер». Оновлення та патчі часто випускаються для виправлення відомих помилок, уразливостей та вдосконалення безпеки програмного забезпечення.

Основні загрози, які можуть виникнути через недостатнє оновлення та патчі наведено у таблиці 2.6.

Таблиця 2.6 - Основні загрози, які можуть виникнути через недостатнє оновлення та патчі

Основні загрози недостатнього оновлення та патчі	**Характеристика загрози**
Уразливості безпеки	Нові вразливості можуть бути виявлені в програмному забезпеченні, і виробники випускають патчі для їх виправлення. Якщо система не оновлюється, вона залишається вразливою перед атаками зловмисників, які можуть скористатися цими вразливостями для злому системи.
Крадіжка даних	Недостатнє оновлення системи може призвести до витоку чутливих даних. Зловмисники можуть використовувати відомі вразливості, щоб отримати доступ до конфіденційної інформації, такої як особисті дані клієнтів, фінансові відомості або інша конфіденційна інформація.
Втрата функціональності	Деякі оновлення можуть також включати виправлення помилок, які впливають на функціональність системи. Якщо система не оновлюється, можуть виникнути проблеми з її роботою, що може призвести до перерв у роботі, втрати даних або незадоволення користувачів.
Відсутність нових функцій і вдосконалень	Оновлення також можуть включати нові функції, покращення продуктивності та вдосконалення в інтерфейсі користувача. Якщо система не оновлюється, вона може залишитися застарілою, а це може негативно вплинути на продуктивність та ефективність роботи.
Несумісність з іншими системами	Оновлення можуть також включати покращення сумісності з іншими системами або стандартами. Якщо система не оновлюється, вона може втратити сумісність з іншими системами, що може призвести до проблем з обміном даними та інтеграції з іншими системами.

Джерело: розроблено автором на основі [13]

Отже, недостатнє оновлення та патчі можуть створювати серйозні ризики для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер». Рекомендується встановлювати всі оновлення та патчі, наданих виробником програмного забезпечення, щоб зменшити ризик вразливостей та зберегти безпеку системи.

7) Недостатня фізична безпека: Якщо фізичний доступ до серверів або інфраструктури системи не належним чином захищений, зловмисники можуть отримати фізичний доступ до обладнання та зламати систему або викрасти конфіденційні дані.

Недостатня фізична безпека може становити серйозну загрозу для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер». Оскільки система обліку та внутрішнього контролю містить важливу та конфіденційну інформацію, таку як фінансові дані, внутрішні процедури, особисті дані співробітників тощо, недостатня фізична безпека може призвести до наступних ризиків які наведені у таблиці 2.7.

Таблиця 2.7. – Ризики недостатньої фізичної безпеки

Ризики недостатньої фізичної безпеки	**Характеристика ризику та його наслідки**
Фізичний доступ до обладнання	Якщо фізичний доступ до серверних кімнат, комп'ютерів чи інших пристроїв, на яких зберігається інформація, недостатньо захищений, зловмисники можуть отримати фізичний доступ до системи та нанести шкоду, вкрасти або змінити дані.
Крадіжка або втрата обладнання	Якщо обладнання, на якому зберігається інформація, викрадають або загублюють, це може призвести до втрати даних і порушення безпеки системи.
Фізичні атаки	Зловмисники можуть спробувати використати фізичну силу, щоб отримати доступ до обладнання або систем, виконати фізичні атаки або знищити обладнання, що може спричинити втрату даних та зупинку роботи системи.
Недостатня контрольована зона доступу	Якщо зона доступу до серверних кімнат або приміщень, де зберігається обладнання, недостатньо контрольована, сторонні особи можуть отримати незаконний доступ до системи.
Фізична безпека персоналу	Якщо персонал, який має фізичний доступ до системи, не отримує достатньої підготовки з питань безпеки, виконує неправильні процедури або несвідомо порушує правила безпеки, це може відкрити шлях для зловмисників.

Джерело: розроблено автором на основі [13]

Загальним підходом повинно бути забезпечення комплексної безпеки, яка включає як фізичні, так і технічні заходи, а також правильну організацію та навчання персоналу.

8) Недостатній криптографічний захист: Недостатній криптографічний захист є ситуацією, коли криптографічні механізми, що використовуються для захисту конфіденційності, цілісності та доступності інформації, не забезпечують належного рівня безпеки. Якщо комунікація між компонентами системи обліку та внутрішнього контролю не захищена належним рівнем шифрування, зловмисники можуть перехопити інформацію та отримати доступ до конфіденційних даних.

Недостатній криптографічний захист може представляти серйозну загрозу для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер". Криптографічний захист відіграє важливу роль у забезпеченні конфіденційності, цілісності та доступності інформації, а також у перевірці автентичності та безвідмовності системи. Основні ризики, пов'язані з недостатнім криптографічним захистом наведено у таблиці 2.8.

Таблиця 2.8. – Ризики недостатнього криптографічного захисту

Вид ризику	**Характеристика ризику та його наслідки**
Витік конфіденційної інформації	Якщо криптографічний захист не належним чином реалізований, зловмисники можуть отримати доступ до конфіденційної інформації, такої як паролі, особисті дані клієнтів або фінансові дані. Це може призвести до фінансових втрат, порушення репутації компанії та правових проблем.
Зміна або порушення цілісності даних	Недостатній криптографічний захист може дозволити зміну або підробку даних, що зберігаються в системі обліку. Це може призвести до спотворення фінансових звітів, неправильного розрахунку оплати або інших помилок, які можуть негативно вплинути на ділову діяльність компанії.
Атаки на аутентифікацію та авторизацію	Недостатній криптографічний захист може відкрити шлях до атак на процеси аутентифікації та авторизації в системі. Зловмисники можуть перехоплювати і підробляти ідентифікаційні дані, отримувати несанкціонований доступ до системи та зловживати привілеями користувачів.
Втрата доступності	Недостатній криптографічний захист може зробити систему більш вразливою до атак на доступність, таких як DDoS-атаки (атаки з відмовою в обслуговуванні). Атаки цього типу можуть перекривати роботу системи обліку та внутрішнього контролю, призводячи до перебоїв у роботі, втрати продуктивності та недоступності послуг для користувачів.

Джерело: розроблено автором на основі [13]

Недостатній криптографічний захист представляє серйозну загрозу для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер". Він може призвести до витоку конфіденційної інформації, порушення цілісності даних, атак на аутентифікацію та авторизацію, а також втрати доступності системи.

9) Недостатня резервне копіювання та відновлення даних: Якщо система не має належних механізмів резервного копіювання та відновлення даних, можуть виникнути проблеми з відновленням даних після випадку втрати, пошкодження або катастрофи, що може призвести до втрати важливих даних і порушення бізнес-процесів.

10) Софт і фізичні помилки: Помилки в програмному забезпеченні або несправності обладнання можуть призвести до вразливостей, збоїв в системі, втрати даних або недоступності системи.

11) Законодавчі та регуляторні вимоги: Нормативно-правове регулювання інформаційної безпеки здійснюється Конституцією України і такими базовими законами України: «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про поштовий зв'язок» та ін.

Законодавчі та регуляторні вимоги можуть становити загрозу та ризик для інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер». Ось кілька потенційних проблем, які можуть виникнути:

12) Вимоги щодо конфіденційності даних: Законодавство вимагає, щоб деякі дані були захищені від несанкціонованого доступу або розкриття. Це може створити виклик для системи обліку, оскільки вона повинна забезпечувати відповідні заходи безпеки, такі як шифрування або контроль доступу, щоб запобігти несанкціонованому доступу до таких даних.

13) Вимоги щодо цілісності даних: Законодавство вимагає, щоб дані були збережені в незмінному стані і не піддавалися несанкціонованій модифікації. Це означає, що система обліку повинна мати механізми контролю цілісності даних,

такі як цифрові підписи або хеш-функції, які дозволяють виявити будь-які зміни в даних.

14) Вимоги щодо доступу до даних: Законодавство встановлює вимоги щодо доступу до даних, зокрема обмеженням доступу до конфіденційної інформації тільки для авторизованих осіб. Це може вимагати впровадження механізмів аутентифікації та авторизації, які забезпечують, що лише правомірні користувачі мають доступ до важливих даних.

15) Вимоги щодо зберігання даних: Деякі законодавчі вимоги включають збереження даних протягом певного періоду часу або дотримання певних правил щодо знищення даних. Це може створити потребу в ефективному системі зберігання даних та управлінні їх життєвим циклом.

16) Вимоги щодо звітності: Законодавство вимагає звітність про діяльність та безпеку системи обліку. Це означає, що система повинна здати звіт про події, які стосуються безпеки, такі як спроби несанкціонованого доступу або модифікації даних.

Невиконання вимог законодавства та регуляторних норм щодо захисту конфіденційності, цілісності та доступності даних може призвести до правових наслідків, штрафів та втрати репутації.

Зважаючи на характер діяльності ПП СЦ «Сервіс-Майстер» у сфері обліку та внутрішнього контролю, наявність ефективної інформаційної безпеки є важливим аспектом для забезпечення довіри клієнтів, захисту конфіденційної інформації, запобігання втратам даних та забезпечення стабільності роботи системи.

2.3 Оцінка з підвищення інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»

Оцінка з підвищення інформаційної безпеки системи обліку та внутрішнього контролю підприємства має на меті ідентифікувати потенційні загрози безпеці інформації та виявити недоліки в існуючих заходах безпеки.

Оцінка стану інформаційної безпеки системи обліку та внутрішнього контролю в досліджуваному підприємстві наведено у таблиці 2.9.

Таблиця 2.9. – Оцінка стану інформаційної безпеки системи обліку та внутрішнього контролю в ПП СЦ «Сервіс-Майстер»

Заходи інформаційної безпеки системи обліку та внутрішнього контролю	**Характеристика заходу та шляхи його реалізації**
Фізична безпека	Усі комп'ютери, сервери та зберігання даних фізично захищені від несанкціонованого доступу. Застосовуються фізичні заходи безпеки, такі як контроль доступу, системи відеоспостереження та замки на дверях.
Захист даних	Підприємство забезпечує захист конфіденційної інформації, такої як контактні дані клієнтів, серійні номери пристроїв та інші важливі дані. Доступ до цих даних обмежений лише працівниками, які мають необхідні дозволи, і забезпечується шифруванням при їх передачі та зберіганні.
Резервне копіювання	Вся важлива інформація регулярно резервно копіюється та зберігається на захищених зовнішніх пристроях або в хмарних системах забезпечення безпеки даних. Це забезпечує можливість відновлення даних в разі випадкового видалення або виникнення технічних проблем.
Контроль доступу та моніторинг:	Наявні механізми контролю доступу, які обмежують права користувачів відповідно до їхніх ролей та обов'язків. Система моніторингу активності користувачів дозволяє виявляти підозрілу активність або несподівані зміни в системі, що можуть свідчити про можливі загрози безпеці.
Свідомість та навчання персоналу	Здійснюється постійне навчання співробітників щодо безпеки інформації. Це включає онлайн курси для розуміння працівниками ризиків, пов'язаних з обробкою інформації, а також визнання їхньої відповідальності за захист цієї інформації. Також проводяться нерегулярні наглядові перевірки щодо дотримання політик інформаційної безпеки.
Кібербезпека	Усі комп'ютери та мережа захищені від зловмисників за допомогою оновлених антивірусних програм, мережевих брандмауерів та систем виявлення вторгнень. Працівники проходять навчання з питань кібербезпеки та свідомі про основні загрози, такі як фішингові атаки та шкідливий софт.

Джерело: розроблено автором на основі спостереження за підприємством

На основі наданих відомостей про підприємство "ПП СЦ Сервіс-Майстер" та заходів, які вживаються для забезпечення інформаційної безпеки системи обліку та внутрішнього контролю, можна зробити загальну оцінку. Загалом, підприємство демонструє свідомість про важливість захисту даних та використовує ряд заходів для забезпечення безпеки інформації.

Оцінка рівню інформаційної безпеки на основі дослідження роботи підприємства може бути класифікована як "задовільна". Заходи, такі як обмеження фізичного доступу до приміщень, використання антивірусних програм, мережевих брандмауерів та систем виявлення вторгнень, регулярне створення резервних копій та використання принципу "необхідного доступу" до даних, свідчать про наявність основних елементів безпеки.

Загальна оцінка "задовільна" вказує на наявність базових заходів безпеки, але можливість поліпшення та удосконалення системи інформаційної безпеки, щоб відповідати зростаючим вимогам та загрозам у цифрову епоху. Регулярне оновлення та аудит системи безпеки може допомогти забезпечити безпеку даних і підвищити рівень інформаційної безпеки підприємства "ПП СЦ Сервіс-Майстер".

2.4 Рекомендації щодо удосконалення та підвищення ефективності заходів інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»

Захист інформації є надзвичайно важливим аспектом сучасного бізнесу. Особливо в системах обліку та внутрішнього контролю, де зберігаються і обробляються конфіденційні дані підприємства. Забезпечення безпеки цих систем є необхідністю, яка стає все більш актуальною в умовах швидкого розвитку інформаційних технологій та зростання кількості кіберзагроз.

Однак, необхідно розуміти, що заходи інформаційної безпеки не є статичними. Вони повинні постійно удосконалюватися та адаптуватися до нових загроз і викликів. Відсутність належних заходів безпеки може призвести до втрати даних, порушення довіри клієнтів, юридичних проблем та інших негативних наслідків для підприємства.

До рекомендацій щодо удосконалення та підвищення ефективності заходів інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер» можна віднести наступні заходи:

1) Проведення повного аудиту інформаційної безпеки;
2) Поліпшення культури безпеки.
3) Оцінка ризику;
4) Регулярне оновлення програмного та апаратного забезпечення;
5) Захист від шкідливих програм;
6) Правильно організувати доступ до даних;
7) Навчання та підвищення кваліфікації персоналу;
8) План відновлення після інциденту.

Розглянемо більш детально ці заходи.

1) Виконати комплексний аудит системи обліку та внутрішнього контролю, включаючи аналіз наявних процесів, політик, процедур, систем та технологій [23].

Виявити потенційні вразливості, слабкі місця та загрози, а також оцінити існуючі заходи безпеки.

Розробити та впровадити стратегії інформаційної безпеки:

Визначити конкретні цілі та об'єктиви, які слід досягти в галузі інформаційної безпеки, враховуючи специфіку ПП СЦ «Сервіс-Майстер».

Розробити детальний план дій для досягнення цих цілей, зазначивши відповідальних за реалізацію кожного етапу та встановивши чіткі терміни виконання.

2) Забезпечити регулярне навчання та свідомість персоналу щодо безпеки інформації, включаючи навчання з протидії соціальному інжинірингу та фішингу.

Впровадити обов'язкові курси безпеки для всіх співробітників, зосереджуючись на важливості сильних паролів, безпечних практик роботи з електронною поштою та використанні VPN для віддаленого доступу.

Запровадження поліпшень у культурі безпеки відіграє важливу роль у забезпеченні безпечної робочої атмосфери та захисті працівників. Це вимагає визнання безпеки як основної цінності, активної участі всіх співробітників та постійного навчання. Шляхи досягнення цього включають організацію навчальних

програм, залучення співробітників до участі, встановлення процедур безпеки, створення системи звітності та аналізу інцидентів. Послідовне вдосконалення системи безпеки підприємства сприяє створенню безпечного та продуктивного робочого середовища для всіх працівників.

3)Досліджуване підприємство повинно проводити регулярну оцінку ризиків, пов’язаних із системами обліку та внутрішнього контролю, щоб оперативно визначати потенційні загрози та ризики.

Для проведення оцінки ризиків ПП СЦ "Сервіс-Майстер" можна виконати такі кроки:

Ідентифікація активів: Визначте всі активи, які пов'язані з системами обліку та внутрішнього контролю, такі як сервери, бази даних, мережеве обладнання, програмне забезпечення, конфіденційна інформація тощо. Важливо врахувати всі компоненти, які мають значення для ділової діяльності компанії.

Визначення загроз: Визначте потенційні загрози, які можуть вплинути на безпеку систем обліку та внутрішнього контролю. Це можуть бути зовнішні загрози, такі як хакерські атаки, фішинг, віруси, а також внутрішні загрози, такі як некоректна робота співробітників, втрата даних або несанкціонований доступ.

Оцінка вразливостей: Визначте вразливості систем обліку та внутрішнього контролю, які можуть бути використані загрозами для отримання несанкціонованого доступу або виконання шкідливих дій. Це можуть бути слабкі місця в мережевій інфраструктурі, відсутність необхідних заходів безпеки, помилки конфігурації або неактуальне програмне забезпечення.

Визначення ризиків: На основі ідентифікованих загроз та вразливостей визначте ризики, пов'язані з системами обліку та внутрішнього контролю. Оцініть ймовірність виникнення ризику та його вплив на ділову діяльність компанії. Це допоможе визначити найкритичніші ризики, які вимагають негайного врегулювання.

Розроблення стратегії управління ризиками: На основі ідентифікованих ризиків розробіть стратегію управління ризиками. Це може включати в себе впровадження технічних заходів безпеки, розроблення політик та процедур

безпеки, навчання співробітників та розроблення планів відновлення після інцидентів.

Регулярне оновлення оцінки ризиків: Оцінка ризиків повинна бути процесом, який виконується на постійній основі. Враховуйте зміну в загрозах, нові вразливості та зміни в діловій діяльності компанії. Проводьте регулярні перегляди та оновлення оцінки ризиків, щоб забезпечити актуальність стратегій управління ризиками.

Оцінка ризиків повинна бути систематичним інструментом управління безпекою інформації. Вона допоможе ідентифікувати та вирішити потенційні загрози, зменшити ризики та забезпечити безпеку систем обліку та внутрішнього контролю ПП СЦ "Сервіс-Майстер".

4) Досліджуване підприємство повинно забезпечити постійне оновлення апаратного та програмного забезпечення, щоб зменшити ризик кібератак.

Рекомендацій щодо оновлення забезпечення:

Поновлення програмного забезпечення: Регулярно оновлюйте всі програми та операційні системи, які використовуються в системах обліку та внутрішнього контролю. Це включає в себе встановлення оновлень безпеки, патчів та нових версій програмного забезпечення, які виробник випускає для виправлення виявлених вразливостей.

Апаратне оновлення: Розгляньте можливість оновлення апаратного забезпечення, такого як сервери, мережеве обладнання та роутери, для забезпечення актуальних заходів безпеки та підтримки останніх стандартів безпеки. Періодично перевіряйте можливість поновлення апаратних компонентів, щоб забезпечити їхню надійність та сумісність зі сучасними вимогами безпеки.

Управління вразливостями: Використовуйте систему управління вразливостями для ідентифікації та вирішення потенційних проблем безпеки в програмному та апаратному забезпеченні. Такі системи допомагають відстежувати вразливості, надають сповіщення про оновлення та допомагають впроваджувати патчі та оновлення системи.

Автоматичне оновлення: Налаштуйте автоматичне оновлення для програмного забезпечення та операційних систем, де це можливо. Це дозволить системам автоматично отримувати та встановлювати оновлення безпеки, необхідні для зменшення ризиків кібератак.

5) ПП СЦ "Сервіс-Майстер" повинно забезпечити захист від шкідливих програм, таких як віруси, хробаки та троянські програми. Це включає використання покращеного антивірусного програмного забезпечення та застосування політики безпеки щодо використання електронної пошти, Інтернету та USB-накопичувачів.

Для забезпечення захисту від шкідливих програм (шкідливих вірусів, шпигунського програмного забезпечення, троянів та інших загроз) для ПП СЦ "Сервіс-Майстер" рекомендується виконати наступні заходи:

Встановлення антивірусного програмного забезпечення: Встановіть надійне антивірусне програмне забезпечення на всі комп'ютери та сервери, що використовуються в компанії. Регулярно оновлюйте вірусні бази даних та програмне забезпечення антивірусу для забезпечення виявлення та блокування нових загроз.

Оновлення програмного забезпечення: Регулярно оновлюйте всі програми, включаючи операційні системи та інші програми, до останніх версій. Виробники програм часто випускають оновлення, які виправляють виявлені вразливості і запобігають атакам.

Брандмауер та фільтрація мережі: Встановіть брандмауери та системи фільтрації мережі для контролю вхідного та вихідного трафіку. Це допоможе блокувати небезпечний мережевий трафік, який може містити шкідливі програми.

Захист електронної пошти: Використовуйте механізми антиспаму та антивірусного сканування для електронної пошти. Це допоможе виявити та блокувати шкідливі вкладення та посилання, які можуть бути використані для поширення шкідливих програм.

Заборона виконання небезпечних файлів: Налаштуйте системи таким чином, щоб заборонити виконання файлів з небезпечних розширень (наприклад, .exe, .bat)

з мережевих сховищ та електронної пошти. Це може допомогти уникнути випадкового запуску шкідливих програм.

6) Досліджуване підприємство повинно забезпечити належний рівень контролю доступу до даних, щоб уникнути несанкціонованого доступу до конфіденційної інформації.

Рекомендації щодо організації доступу до даних:

Рольова модель: Використовуйте рольову модель доступу, що означає, що кожен користувач має визначену роль або групу, яка визначає його права доступу до різних категорій даних. Це дозволить обмежити доступ до конфіденційної інформації тільки тим користувачам, які мають відповідні повноваження.

Принцип найменшого доступу: Надавайте користувачам лише ті права доступу до даних, які необхідні для виконання їхніх робочих обов'язків. Це допоможе зменшити ризик несанкціонованого доступу та недбалого поводження з даними.

Аутентифікація та авторизація: Застосовуйте сильну аутентифікацію для перевірки ідентифікації користувачів перед наданням доступу до системи. Крім того, реалізуйте механізми авторизації, які забезпечують перевірку прав доступу користувача перед отриманням доступу до конкретних даних.

Моніторинг доступу: Встановіть систему моніторингу доступу до даних, щоб виявляти та реагувати на недостовірну або підозрілу діяльність. Це може включати журналювання подій, системи виявлення вторгнень або інші інструменти моніторингу.

7) Організація повинна навчати та вдосконалювати персонал щодо заходів із забезпечення інформаційної безпеки та культури безпеки в цілому.

Рекомендації щодо навчання та підвищення кваліфікації персоналу:

Свідомість про безпеку: Проведіть навчання персоналу щодо загроз і вразливостей інформаційної безпеки, а також процедур і політик безпеки, що застосовуються в ПП СЦ "Сервіс-Майстер". Розберіться з основними поняттями безпеки, включаючи паролі, соціальний інжиніринг, фішинг та інші методи атак.

Політики та процедури безпеки: Навчіть персоналу про актуальні політики та процедури безпеки, які мають бути дотримувані в ПП СЦ "Сервіс-Майстер". Це можуть бути правила щодо використання паролів, обмеження доступу до конфіденційної інформації, захисту фізичних пристроїв та інше.

Оновлення знань: Забезпечте періодичне оновлення знань персоналу щодо останніх трендів та розвитку в області інформаційної безпеки. Організуйте навчальні семінари, тренінги або запрошуйте зовнішніх експертів для надання актуальної інформації та кращих практик.

8) Підприємству необхідно розробити план відновлення після інциденту, який включатиме процедури відновлення даних, забезпечення безперебійності бізнес-процесів та комунікацію зі зацікавленими сторонами.

Рекомендації щодо створення плану відновлення після інциденту для ПП СЦ "Сервіс-Майстер":

Ідентифікація та класифікація інцидентів: Створіть процедури для ідентифікації та класифікації інцидентів інформаційної безпеки. Визначте рівні серйозності інцидентів та встановіть прийнятні строки відновлення для кожного рівня.

Екстрені дії: Визначте конкретні кроки, які слід вжити в разі виявлення інциденту. Наприклад, ізолюйте пошкоджені системи або вимкніть їх від мережі, забезпечте резервну копію важливих даних, залучіть експертів з безпеки та інші необхідні заходи.

Аналіз причин: Проведіть детальний аналіз причин інциденту, щоб з'ясувати, як він стався та які уразливості були використані. Це допоможе визначити необхідні заходи для запобігання подібним інцидентам у майбутньому.

Відновлення систем: Розробіть план відновлення систем, який включатиме кроки для відновлення роботи інфраструктури та даних. Врахуйте пріоритети відновлення та визначте послідовність кроків для ефективного відновлення.

Перевірка безпеки: Перевірте безпеку систем та мережі після відновлення, щоб впевнитися, що уразливості були усунені і система залишається безпечною. Проведіть аудит безпеки та перевірку наявності потенційних загроз.

Ці рекомендації мають на меті покращити рівень безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер» і зменшити ризики витоку даних, вторгнень та інших інцидентів інформаційної безпеки.

Загалом, ефективна інформаційна безпека вимагає постійного вдосконалення та оновлення. Потрібно регулярно оцінювати свою систему та впроваджувати заходи для зменшення ризиків та забезпечення надійного захисту даних та інформації системи обліку та внутрішнього контролю.

ВИСНОВКИ

У даній дипломній роботі було проведено детальне дослідження процесу організації інформаційної безпеки системи обліку та внутрішнього контролю в приватному підприємстві СЦ "Сервіс-Майстер". На основі проведеного дослідження можемо зробити такі висновки:

У підрозділі «Організаційні та технологічні особливості діяльності ПП СЦ «Сервіс-Майстер»» було досліджено і описано основні організаційні та технологічні аспекти діяльності даної компанії. Можна зробити висновок, досліджуване підприємство успішно поєднує організаційні та технологічні аспекти своєї діяльності. Компанія забезпечує якісне обслуговування та ремонт побутової техніки завдяки ефективній організаційній структурі, наявності необхідних ресурсів та використанню передових технологій. Задоволення потреб клієнтів і підтримання високої репутації є основними пріоритетами компанії.

У підрозділі "Характеристика інформаційних технологій, що використовуються для цифровізації обліку та внутрішнього контролю досліджуваного підприємства" було проведено детальний огляд і опис інформаційних технологій, що використовуються для цифровізації обліку та внутрішнього контролю в досліджуваному підприємстві.

Досліджуване підприємство успішно впроваджує інформаційні технології з метою цифровізації обліку та внутрішнього контролю. Ці технології дозволяють автоматизувати процеси збору, обробки та аналізу даних, що сприяє покращенню точності, ефективності та надійності обліку та контролю.

У підрозділі "Принципи та організація захисту інформації у системі обліку та внутрішнього контролю підприємства" було досліджено принципи та заходи, спрямовані на забезпечення безпеки інформації в системі обліку та внутрішнього контролю досліджуваного підприємства.

Загалом, досліджуване підприємство демонструє свідоме і відповідальне ставлення до захисту інформації в системі обліку та внутрішнього контролю. Застосування принципів та заходів безпеки інформації допомагає підприємству

забезпечити надійність, довіру та успішну функціонування своєї інформаційної системи.

У підрозділі "Стан системи обліку та внутрішнього контролю щодо її інформаційної забезпеченості та захищеності" було проведено аналіз стану системи обліку та внутрішнього контролю підприємства з точки зору її інформаційної забезпеченості та захищеності.

Загалом, система обліку та внутрішнього контролю підприємства має позитивний стан щодо її інформаційної забезпеченості та захищеності. Проте, рекомендується постійне вдосконалення заходів безпеки з метою забезпечення стійкості та надійності системи обліку та внутрішнього контролю в умовах зростаючих загроз та викликів інформаційної безпеки.

У підрозділі "Потенційні загрози та ризики для інформаційної безпеки системи обліку та внутрішнього контролю для ПП СЦ «Сервіс-Майстер»" було проведено аналіз потенційних загроз та ризиків, які можуть вплинути на інформаційну безпеку системи обліку та внутрішнього контролю підприємства. Розуміння потенційних загроз та ризиків дозволяє ПП СЦ «Сервіс-Майстер» покращити свою інформаційну безпеку, прийняти належні заходи для запобігання інцидентам та забезпечити надійність та цілісність своєї системи обліку та внутрішнього контролю.

В підрозділі "Оцінка з підвищення інформаційної безпеки системи обліку та внутрішнього контролю ПП СЦ «Сервіс-Майстер»" була проведена оцінка існуючих заходів безпеки та запропоновані рекомендації щодо підвищення рівня інформаційної безпеки системи обліку та внутрішнього контролю. Загальна оцінка "задовільна" вказує на наявність базових заходів безпеки, але можливе поліпшення та удосконалення системи інформаційної безпеки, щоб відповідати зростаючим вимогам та загрозам у цифрову епоху. Регулярне оновлення та аудит системи безпеки може допомогти забезпечити безпеку даних і підвищити рівень інформаційної безпеки підприємства "ПП СЦ Сервіс-Майстер".

В підрозділі "Рекомендації щодо удосконалення та підвищення ефективності заходів інформаційної безпеки системи обліку та внутрішнього

контролю ПП СЦ «Сервіс-Майстер»" були запропоновані конкретні рекомендації для поліпшення рівня безпеки та підвищення ефективності заходів.

Отже, у процесі дослідження було проведено аналіз поточного стану інформаційної безпеки та внутрішнього контролю в СЦ "Сервіс-Майстер". Виявлено ряд недоліків і проблем, які створюють загрози для безпеки інформації та можуть призвести до фінансових втрат та репутаційних проблем для компанії.

Для вирішення цих проблем було запропоновано комплекс заходів щодо підвищення рівня інформаційної безпеки системи обліку та внутрішнього контролю. Надані рекомендації щодо вдосконалення інформаційної безпеки системи обліку та внутрішнього контролю підприємства сприятимуть попередженню можливих загроз безпеці, зменшенню ризиків кібератак та збереженню конфіденційності, цілісності та доступності даних. Регулярний моніторинг системи та встановлення правильних рівнів доступу також гарантують забезпечення безпеки інформації.

Отже, системи обліку та внутрішнього контролю підприємств мають бути захищені від можливих кібератак та забезпечувати конфіденційність, цілісність та доступність даних. Для цього потрібна регулярна оцінка ризиків, оновлення програмного забезпечення, надійні паролі, захист мережі та резервне копіювання даних. Організаційний персонал також повинен бути навчений і знати про культуру безпеки та практику інформаційної безпеки.

Підприємству важливо розуміти загрози і ризики інформаційної безпеки, планувати та вживати заходи для їх уникнення та управління ними. Крім того, необхідно пам’ятати про постійний розвиток та оновлення засобів захисту інформації, оскільки кіберзлочинці постійно знаходять нові способи атак і проникнення в системи

Можна зробити висновок, що реалізація запропонованих рекомендацій дозволить покращити інформаційну безпеку та внутрішній контроль в СЦ "Сервіс-Майстер". Рекомендується продовжити моніторинг інформаційної безпеки та регулярно оновлювати політику і заходи безпеки, щоб забезпечити тривалий захист інформації та стабільну роботу системи обліку та внутрішнього контролю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вітер С. А., І. І. Світлишин. Захист облікової інформації та кібербезпека підприємства. *Економіка та суспільство*. 2017. № 11. С. 497–502. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf (дата звернення 10.05.2023).

2. Ілляшенко К.В. Інформаційна безпека сучасного бухгалтерського обліку. *Науковий вісник Міжнародного гуманітарного університету.* 2019. № 40. С. 179–183. URL: http://vestnik-econom.mgu.od.ua/journal/2019/40-2019/25.pdf (дата звернення 10.05.2023).

3. Данилюк І.В., Зорій Н.М. Оцінка обліку та системи внутрішнього контролю як інструменти безпеки бізнесу. *Глобальні та національні проблеми економіки.* 2016. № 9. С. 765-770. URL: http://global-national.in.ua/archive/9-2016/157.pdf (дата звернення 10.05.2023)

4. Гаркуша С.А. Особливості зберігання, архівування та захисту інформації в процесі організації бухгалтерського обліку. *Інфраструктура ринку.* 2019. № 30. С. 478-485.
URL: http://www.marketinfr.od.ua/journals/2019/30_2019_ukr/75.pdf (дата звернення 10.05.2023)

5. Грабчук І. Л. Організація захисту облікової інформації в умовах гібридної війни. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу.* 2018. № 3. С. 20-24. URL:
http://pbo.ztu.edu.ua/article/view/151399 (дата звернення 10.05.2023)

6. Титенко Л. В. Управління інформаційними ризиками облікової системи підприємства. *Інфраструктура ринку.* 2020. № 42. С. 379-383.
URL: http://www.marketinfr.od.ua/journals/2020/42_2020_ukr/66.pdf (дата звернення 10.05.2023)

7. Чех Н. О. Забезпечення інформаційної безпеки бухгалтерського обліку підприємства. 2019. № 2. С. 111-117. URL:
http://nbuv.gov.ua/UJRN/kgm_econ_2019_2_22 (дата звернення 10.05.2023)

8. Коломоєць, О. Д. Особливості контролю при використанні інформаційних систем і технологій. *Облік, аналіз і аудит: виклики інституціональної економіки.* 2021. № 8. С. 229-232. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/12015/1/%d0%97%d0%b1%d1%96%d1%80%d0%bd%d0%b8%d0%ba%20%d1%82%d0%b5%d0%b7%d0%9a%d1%83%d0%b7%d0%bc%d0%b5%d0%bd%d0%ba%d0%be.pdf (дата звернення 06.05.2023)

9. Закон України: Про основні засади забезпечення кібербезпеки України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 06.05.2023)

10. Закон України: Про захист персональних даних , від 01.06.2010 № 2297-VI URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 06.05.2023)

11. Спільник, Ірина, Микола Палюх. "Бухгалтерський облік в умовах цифрової економіки". *Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації.* 2019. С. 83-86. URL: http://188.190.43.194:7980/jspui/bitstream/123456789/8446/1/83-96.pdf (дата звернення 06.05.2023)

12. Климчук О.В. Сучасні аспекти використання інформаційних систем і технологій в управлінні. *Збірник тез доповідей II Міжнародної науково-практичної конференції «Бізнес, інновації, менеджмент: проблеми та перспективи».* 2021. С. 170- 171 URL: http://confmanagement.kpi.ua/proc/article/view/230931 (дата звернення 10.05.2023)

13. Северина, С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету.* 2016. № 1. С. 155-161. URL: http://nbuv.gov.ua/UJRN/Vznu_eco_2016_1_21 (дата звернення 10.05.2023)

14. В.В. Овсянніков. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2015. № 3. С. 187–193. URL: http://nbuv.gov.ua/UJRN/sitsbo_2015_3_35 (дата звернення 10.05.2023)

15. Ткачук Т. Система інформаційної безпеки. *Бізнес і безпека.* 2018. URL: http://ippi.org.ua/sites/default/files/11_7.pdf (дата звернення 10.05.2023)

16. Міщенко С.П. Інформаційна складова економічної безпеки підприємства. *Вісник економіки транспорту і промисловості*. 2012. № 39. С. 250–254. URL: https://cyberleninka.ru/article/n/informatsiyna-skladova-ekonomichnoyi-bezpeki-pidpriemstva/viewer (дата звернення 10.05.2023)

17. Василішин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи. *Вісник Економіки.* 2021. № 1. С. 97–110. URL: http://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1218 (дата звернення 10.05.2023)

18. Кононенко Г. І. Проблеми інформаціїної безпеки вищої освіти в умовах глобалізації. *Матеріали Міжнародної науково-практичної конференції «Проблеми інтеграції освіти, науки та бізнесу в умовах глобалізації»* URL:https://er.knutd.edu.ua/bitstream/123456789/14498/1/PIONBUG_20191004_P125-126.pdf (дата звернення 10.05.2023)

19. Гребенніков В. Політика управління інформаційною безпекою. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/10220 (дата звернення 10.05.2023)

20. Легенчук С. Ф.. Царук І. М., Назаренко Т. П. Принципи захисту даних у системі обліку: управлінські аспекти. *Економіка, управління та адміністрування.* 2021. № 2. С. 61–69. URL: http://ema.ztu.edu.ua/article/view/236861 (дата звернення 10.05.2023)

21. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка.* 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення 19.05.2023)

22. Рішення Ради національної безпеки і оборони України від 27.01.2016. «Про Стратегію кібербезпеки України». URL: www.president.gov.ua/documents/962016-19836 (дата звернення 19.05.2023)

23. Кушнір І.Б. Аудит організації системи обліку та внутрішнього контролю в підприємстві. 2020. URL:http://dspace.wunu.edu.ua/bitstream/316497/41132/1/%D0%9A%D1%83%D1%88%D0%BDi%D1%80.pdf (дата звернення 10.05.2023)

24. Головко В.І. Фінансово-економічна діяльність підприємств: контроль, аналіз та безпека. 2006. С. 448 (дата звернення 10.05.2023)

25. Сметанко О.В. Удосконалення процесу внутрішнього аудиту протидії кібершахрайству в системі корпоративного управління. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/4208 (дата звернення 10.05.2023)

26. Грабар Н.С. Інформаційна безпека в умовах становлення глобального інформаційного суспільства. 2019. № 7. URL: http://www.dy.nayka.com.ua/pdf/7_2019/23.pdf (дата звернення 10.05.2023)

27. Антонова С.Є. Інформаційна безпека. *Державне управління: удосконалення та розвиток.* 2019. № 11. URL: http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf (дата звернення 10.05.2023)

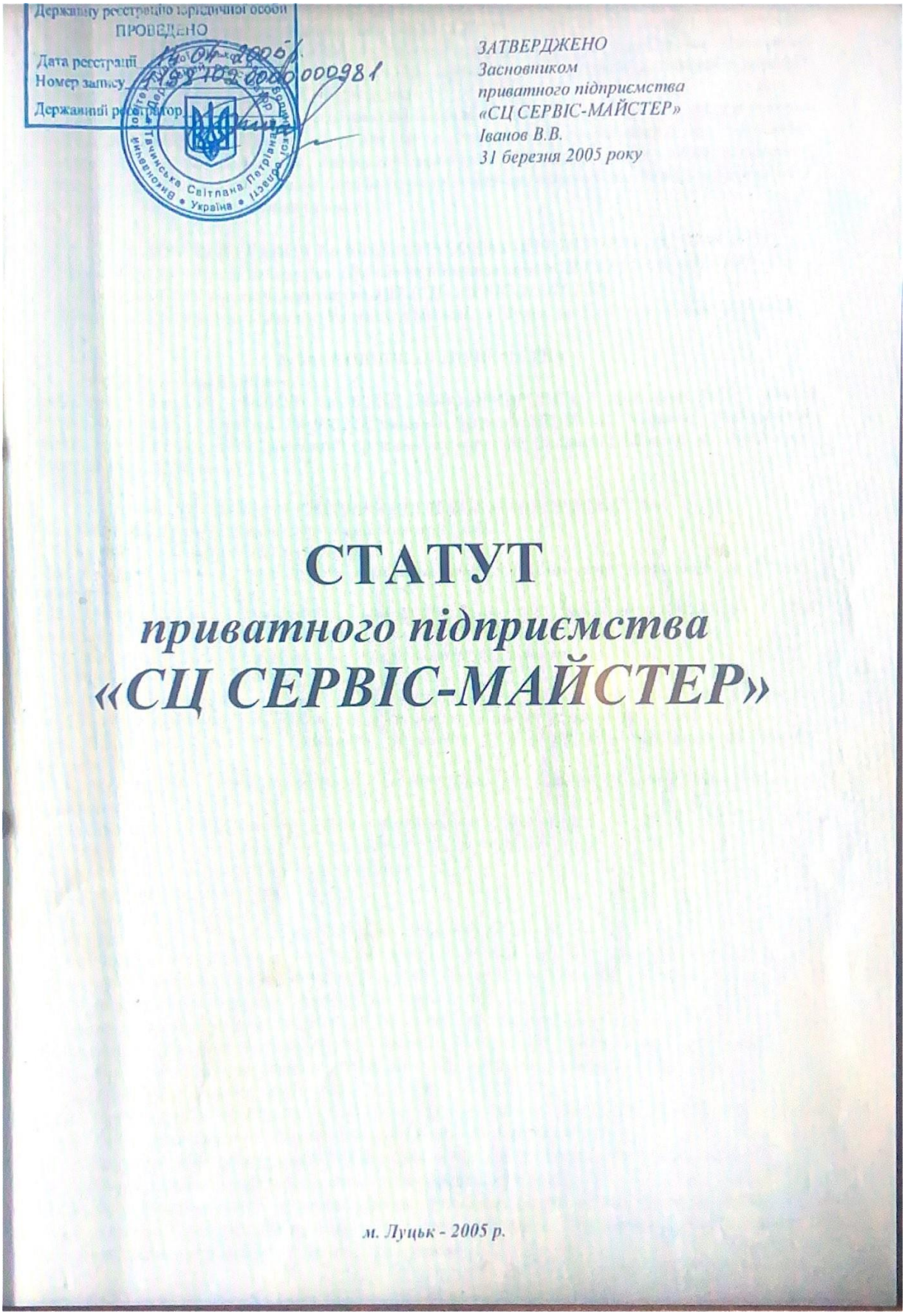
28. Мулик Я.І. Методичні та організаційні підходи до системи внутрішнього контролю на підприємстві. 2020, № 17-18: С. 28-38. URL: http://www.agrosvit.info/pdf/17-18_2020/6.pdf (дата звернення 10.05.2023)

29. Єршова Н.Ю. Шляхи вдосконалення системи внутрішнього контролю на підприємстві. 2013. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/2948 (дата звернення 10.05.2023)

30. Євдокимов В.В. Взаємозв'язок бухгалтерського обліку та внутрішнього контролю в управлінській діяльності підприємства. 2009. №4. С 42-44. URL: http://ven.ztu.edu.ua/article/viewFile/82676/86064 (дата звернення 19.05.2023)

ДОДАТКИ

Додаток А



Продовження додатку А

Статут приватного підприємства «СЦ СЕРВІС-МАЙСТЕР» (надалі по тексту «Підприємство») розроблено відповідно до вимог Господарського кодексу України, Цивільного кодексу України та інших законів і нормативних актів України. Статут встановлює порядок створення, діяльності та ліквідації підприємства.

Підприємство створюється з метою здійснення підприємницької діяльності, організації виробництва товарів, продукції, виконання робіт, розширення сфери послуг та збільшення кількості робочих місць у сфері зайнятості населення, торгівлі і обміну матеріальними і сировинними ресурсами, продукцією виробничо-технічного призначення та товарами народного споживання, надання різноманітних послуг.

1. НАЙМЕНУВАННЯ ТА МІСЦЕЗНАХОДЖЕННЯ ПІДПРИЄМСТВА

1.1. Повне найменування підприємства: ***Приватне підприємство «СЦ СЕРВІС-МАЙСТЕР»***.
1.2. Скорочене найменування підприємства: ***ПП «СЦ СЕРВІС-МАЙСТЕР»***.
1.3. Місцезнаходження підприємства: Волинська область, м. Луцьк, пр. Соборності, буд. 33, кв. 66.

2. ЗАСНОВНИК ПІДПРИЄМСТВА

2.1. Засновником підприємства є:
громадянин України ІВАНОВ ВАЛЕРІЙ ВОЛОДИМИРОВИЧ, ідентифікаційний номер 2350013212, паспорт серії АС № 933227, виданий Луцьким МВ УМВС України у Волинській області 17 листопада 2004 року, який проживає за адресою: Волинська область, м. Луцьк, пр. Соборності, буд. 33, кв. 66.

3. МЕТА ТА ПРЕДМЕТ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

3.1. Метою діяльності підприємства є одержання прибутку.
3.2. Предметом діяльності підприємства є:
3.2.1. Ремонт, технічне, сервісне та гарантійне обслуговування електроприладів, побутової електротехніки.
3.2.2. Оптова та роздрібна торгівля електроприладами, побутовою електротехнікою та їх комплектуючими.
3.2.3. Послуги по підключенню (встановленню) та налагодженню електроприладів.
3.2.4. Посередницька діяльність.
3.2.5. Торгівельна діяльність у сфері оптової, роздрібної торгівлі та громадського харчування по реалізації продовольчих та непродовольчих товарів, алкогольних та тютюнових виробів.
3.2.6. Виробництво товарів народного споживання та продукції виробничо-техничного призначення.
3.2.7. Виробництво товарів народного споживання та продукції виробничо-техничного призначення.
3.2.8. Оптова та роздрібна торгівля пально-мастильними матеріалами.
3.2.9. Постачання, реалізація та обслуговання обладнання для АЗС.
3.2.10. Послуги в сфері готельного господарства.
3.2.11. Операції з нерухомістю.
3.2.12. Проведення аукціонів.
3.2.13. Діяльність, пов'язана з відповідальним збереженням товарів.
3.2.14. Видавнича діяльність, виготовлення продукції та надання послуг у сфері поліграфії.
3.2.15. Організація та проведення видовищних мероприємств, фестивалів, концертів тощо.
3.2.16. Фізкультурно-оздоровча та спортивна діяльність:
- організація та проведення спортивних занять професіоналів та любителів спорту;
- діяльність з підготовки спортсменів до змагань з різних видів спорту, визнаних в Україні.

3.2.17. Організація та проведення виставок, ярмарок, аукціонів, семінарів, симпозіумів.
3.2.18. Туроператорська та турагентська діяльність.
3.2.19. Організація та утримання тоталізаторів, гральних закладів, випуск та проведення лотерей.
3.2.20. Лісове господарство, лісозаготівля, деревообробне виробництво.
3.2.21. Закупівля у населення сільскогосподарської продукції та продуктів її переробки.
3.2.22. Вирощування та переробка сільскогосподарської продукції.
3.2.23. Проведення навчання населення шляхом організації різноманітних курсів, учбових програм.
3.2.24. Надання послуг, пов'язаних із профорієнтацією населення, посередництво у працевлаштуванні на роботу, в тому числі за кордоном.

Продовження додатку А

3.2.25. Добування та переробка корисних копалин згідно з діючим законодавством.
3.2.26. Надання послуг з перевезення пасажирів і вантажів автомобільним транспортом загального користування (крім надання послуг з перевезення пасажирів та їх багажу на таксі).
3.2.27. Надання послуг з перевезення пасажирів та їх багажу на таксі.
3.2.28. Транспортно-експедиційні послуги без робіт і послуг, що виконуються на замовлення населення.
3.2.29. Вантажні та пасажирські перевезення всіма видами транспорту, експедиторські послуги.
3.2.30. Надання транспортно-експедиційних послуг при перевезеннях у внутрішньому сполученні, зовнішньоторговельних і транзитних вантажів.
3.2.31. Організація та надання послуг по ремонту, технічному та сервісному обслуговуванню автотранспортної техніки.
3.2.32. Інформаційна діяльність, надання консалтингових послуг.
3.2.33. Послуги по перекладу з/на іноземні мови.
3.2.34. Організація митних ліцензійних складів.
3.2.35. Отримання, доставка, зберігання та відпуск лікарських засобів та виробів медичного призначення, медтехніки та медобладнання.
3.2.36. Розробка та реалізація медикаментів, медтехніки та медобладнання.
3.2.37. Надання побутових послуг.
3.2.38. Кіно-, відео- зйомка, аудіозапис, прокатна діяльність.
3.2.39. Здійснення лізингових операцій.
3.2.40. Рекламна, представницька діяльність, дизайн.
3.2.41. Розробка та виготовлення печаток, штампів, емблем, товарних знаків, візиток тощо.
3.2.42. Розробка та впровадження програмного забезпечення, встановлення та обслуговування інформаційно-обчислювальних систем, ремонт комп'ютерної техніки.
3.2.43. Виробництво, передача та постачання електроенергії.
3.2.44. Діяльність, пов'язана з проектуванням, будівництвом, ремонтом та експлуатацією об'єктів трубопровідного транспорту.
3.2.45. Використання радіочастот.
3.2.46. Проведення маркетингових, соціологічних та інших досліджень.
3.2.47. Проведення науково-дослідних досліджень, конструкторських розробок тощо.
3.2.48. Монтаж, ремонт і профілактичне обслуговування засобів охоронної сигналізації.
3.2.49. Збирання, заготівля, переробка, купівля і продаж брухту та відходів кольорових та чорних металів.
3.2.50. Видобування дорогоцінних металів і дорогоцінних каменів, виготовлення і реалізація виробів з їх використанням.
3.2.51. Збирання, переробка твердих і рідких відходів виробництв, що містять дорогоцінні метали й дорогоцінне каміння, та їх брухту.
3.2.52. Діяльність, пов'язана з реалізацією транспортних засобів, що підлягають реєстрації та обліку.
3.2.53. Зовнішньоекономічна діяльність, в тому числі по напрямках перелічених у даній статті.
3.2.54. Здійснення інших видів діяльності, що відповідають меті створення підприємства і не заборонені чинним законодавством України.
3.3. При необхідності підприємство повинно одержати ліцензії на окремі види діяльності відповідно до вимог чинного законодавства.

4. ЮРИДИЧНИЙ СТАТУС ПІДПРИЄМСТВА

4.1. Підприємство є юридичною особою згідно з законодавством України, має самостійний баланс, круглу печатку, штампи, фірмові бланки із своїм найменуванням, емблему, товарний та фірмовий знак та іншу атрибутику.
4.2. Підприємство набуває прав юридичної особи з моменту його державної реєстрації.
4.3. Підприємство для досягнення мети своєї статутної діяльності має право від свого імені укладати угоди, набувати майнових та особистих немайнових прав і нести обов'язки, бути позивачем і відповідачем у суді, господарському та третейському судах.
4.4. Підприємство у встановленому порядку бере участь у зовнішньоекономічній діяльності та здійснює експортно-імпортні операції як в Україні, так і за її межами, включаючи товарообмін, посередницькі та інші операції.

Продовження додатку А

4.5. Підприємство є засновником майна, що йому належить. Підприємство здійснює у відповідності з законодавством України володіння, користування і розпорядження майном, що знаходиться у його власності, відповідно до мети власної статутної діяльності та призначення майна.
4.6. Підприємство має право продавати, передавати безкоштовно, дарувати, обмінювати, надавати в оренду юридичним особам і громадянам засоби виробництва, майно та інші матеріальні цінності, або відчужувати їх іншими способами, в порядку, визначеному законом.
4.7. Підприємство може проводити взаєморозрахунки з замовниками, підприємствами, організаціями, громадянами, як в безготівковому порядку, так і за готівку.
4.8. Майно та інші активи підприємства, а також майно, що йому надане у користування, яке знаходиться на території України, не підлягає націоналізації, конфіскації або іншому вилученню за винятком випадків, передбачених законодавством України.
4.9. Підприємство може утворювати філії та представництва, відділення та інші відокремлені підрозділи на території України та за кордоном.
4.10. Філії та представництва діють на підставі положень про них. Положення про філії та представництва затверджуються засновником підприємства згідно із законодавством України.
4.11. Підприємство має товарний знак та знак обслуговування, які реєструються у порядку, встановленому чинним законодавством.
4.12. Підприємство може бути засновником (учасником, акціонером) інших підприємств, господарських товариств, об'єднань та організацій як в Україні, так і на території інших держав.
4.13. Підприємство відкриває в установах банків рахунки в українській та іноземній валюті для розрахункових операцій. Підприємство самостійно обирає банки для здійснення кредитно-розрахункових операцій.
4.14. Підприємство бере участь у міжнародному культурному обміні, проводить і бере участь у проведенні міжнародних виставок, ярмарок, аукціонів.
4.15. Підприємство може направляти за кордон у відрядження, для стажування і на перепідготовку спеціалістів для навчання та ознайомлення з досвідом організації і діяльності фірм, банків, підприємств та кооперативів, збирання інформації, для участі в переговорах, виставках, аукціонах, встановлення ділових контактів.
4.16. Підприємство може придбати і реалізувати продукцію (роботи, послуги) підприємств, об'єднань, організацій, а також іноземних фірм як в Україні, так і за кордоном.
4.17. Підприємство може придбати і орендувати земельні ділянки і користуватися природними ресурсами в порядку, встановленому чинним законодавством України.

5. МАЙНО ПІДПРИЄМСТВА

5.1. Майно підприємства створюється за рахунок:
- статутного капіталу (фонду) підприємства (за рахунок майнового та грошового внеску засновника);
- доходів, одержаних від реалізації продукції, робіт, послуг згідно з метою діяльності підприємства;
- доходів від цінних паперів;
- кредитів банків та інших кредиторів;
- майна, придбаного в інших суб'єктів господарювання, організацій та громадян у встановленому законодавством порядку;
- безоплатних або благодійних внесків, пожертвувань українських та іноземних підприємств, організацій, громадян;
- інших джерел, не заборонених чинним законодавством України.

5.2. Для забезпечення діяльності підприємства засновником створюється статутний капітал (фонд) у розмірі 1000,00 (одна тисяча) гривень.

Статутний капітал (фонд) може бути збільшений за рахунок прибутків від діяльності підприємства, а при необхідності також за рахунок додаткових внесків засновника. Рішення про збільшення Статутного капіталу (фонду) приймається засновником підприємства.

Статутний капітал (фонд) може бути зменшений за рішенням засновника підприємства

5.3. Порядок використання фондів підприємства визначається засновником підприємства згідно з чинним законодавством та цим статутом.
5.4. Вся сума амортизаційних відрахувань, що залишається згідно з чинним законодавством у розпорядженні підприємства, направляється в фонд розвитку підприємства.

Продовження додатку А

5.5. Підприємство може використовувати кошти резервного фонду на додаткові витрати по розробці і впровадженню нових перспективних програм, на поповнення власних обігових коштів у разі їх нестачі, на покриття витрат від уцінки продукції та на інші цілі.
За рішенням директора підприємства частина коштів резервного фонду може бути використана на оплату праці з поповненням їх в наступному періоді з прибутку.
5.6. Кошти підприємства зберігаються на розрахунковому рахунку (українська валюта) і валютному рахунку (іноземна валюта) і використовуються ним самостійно, у межах, встановлених чинним законодавством України.
5.7. Майно підприємства може бути вилучене тільки на підставі чинного законодавства.
5.8. Підприємство може об'єднувати частину свого майна і грошових коштів з майном і грошовими коштами державних, кооперативних, колективних та громадських організацій для виконання робіт та надання послуг, в тому числі шляхом організації спільних підприємств.
5.9. Частина майна підприємства може бути передана філіям, представництвам, іншим відокремленим підрозділам підприємства за рішенням і на умовах, визначених засновником підприємства.

6. ПРИБУТОК ПІДПРИЄМСТВА

6.1. Прибуток підприємства після сплати податків та інших обов'язкових виплат (чистий прибуток) надходить у розпорядження засновника. Засновник самостійно визначає напрямок використання чистого прибутку.

7. ЗОВНІШНЬОЕКОНОМІЧНА ДІЯЛЬНІСТЬ

7.1. Підприємство самостійно здійснює зовнішньоекономічну діяльність, тобто співробітництво з іноземними суб'єктами господарської діяльності як в Україні, так і за її межами в порядку та за умов, визначених законодавством.
7.2. При здійсненні зовнішньоекономічної діяльності, підприємство має всі права юридичної особи та учасника зовнішньоекономічних зв'язків в межах, встановлених законодавством України, у тому числі підприємство має право:
7.2.1. У встановленому порядку виступати як учасник зовнішньоекономічних зв'язків.
7.2.2. Здійснювати різного роду угоди та інші юридичні акти з зарубіжними юридичними та фізичними особами, у т.ч. купівлі-продажу, обміну, поставки, підряду, оренди, позики, перевозки, доручення, комісії, схову, спільної діяльності, кредитні, вексельні та інші, а також приймати участь у торгах, конкурсах, надавати гарантії, надавати і набувати права на охоронні документи і їх застосування та інші угоди відповідно законодавству України.
7.2.3. Відповідно встановленому порядку проводити експортно-імпортні, бартерні, лізингові, реекспортні та інші операції безпосередньо.
7.2.4. Створювати спільні підприємства з іноземними юридичними та фізичними особами на території України та за кордоном.
7.2.5. Будувати, набувати, брати і здавати у найм за кордоном необхідне для здійснення своєї діяльності різного роду рухоме та нерухоме майно.
7.2.6. Здійснювати міжнародний туризм, приймати участь у міжнародних спортивних змаганнях, культурних заходах.
7.2.7. Займатися міжнародною рекламою та маркетинговою діяльністю.
7.2.8. Одержувати безкоштовну матеріальну допомогу від своїх іноземних партнерів.
7.2.9. У встановленому порядку відкривати свої валютні рахунки в банках України та за кордоном.
7.2.10. Здійснювати ділові контакти, зв'язуватися у встановленому порядку з питань, пов'язаних з діяльністю підприємства, з іноземними установами, організаціями, підприємствами та їх представниками, а також з іноземними громадянами.
7.2.11. Відряджувати за кордон своїх спеціалістів.
7.2.12. Засновувати свої філії, контори, відділення, представництва та агенства, а також приймати участь у різного роду іноземних і міжнародних організаціях та об'єднаннях.
7.2.13. Формувати за участю іноземних спеціалістів тимчасові творчі та інші колективи для забезпечення діяльності підприємства, рішення його завдань.
7.2.14. Орендувати, купувати у закордонних фірм, підприємств та приватних осіб обладнання, прилади, механізми, будови, споруди, сировину, матеріали, необхідні для виконання завдань і функцій підприємства.

Продовження додатку А

7.2.15. Володіти, користуватись та розпоряджатись коштами, майном, майновими і немайновими правами та іншими результатами своєї зовнішньоекономічної діяльності.
7.2.16. Брати участь у створенні та роботі міжнародних економічних організацій.
7.2.17. Здійснювати без обмежень посередницькі операції, за яких право власності на товар не переходить до посередника (на підставі комісійних, агентських договорів).
7.2.18. Самостійно підписувати зовнішньоекономічні договори (контракти) всіх видів, крім тих, які прямо заборонені законодавством.
7.2.19. Самостійно визначати форму розрахунків зовнішньоекономічних операцій серед тих, що не суперечать законодавству та відповідають міжнародним правилам.
7.2.20. Безпосередньо брати кредити у чинній на території України та іноземній валюті.
7.2.21. Вільно обирати банківсько-кредитні установи, які будуть вести їх валютні рахунки та розрахунки з іноземними суб'єктами, користуватись їх послугами.
7.2.22. Підприємство може мати інші права, що не суперечать законодавству.
7.3. Підприємство має право здійснювати будь-які види зовнішньоекономічної діяльності, які не заборонені законодавством, зокрема:
7.3.1. Експорт та імпорт товарів, капіталів.
7.3.2. Надання послуг іноземним суб'єктам господарської діяльності з усіх напрямків діяльності підприємства.
7.3.3. Різноманітна кооперація з іноземними суб'єктами господарської діяльності, навчання та підготовка фахівців.
7.3.4. Спільна підприємницька діяльність підприємства та іноземних партнерів відповідно до предмету діяльності підприємства.
7.3.5. Організація та проведення виставок, ярмарок, торгів, аукціонів, конференцій, семінарів та інших заходів спільно з іноземними партнерами.
7.3.6. Товарообмінні (бартерні) операції, інші форми зустрічної торгівлі.
7.3.7. Орендні (лізингові) операції.
7.4. Підприємство веде бухгалтерський та оперативний облік зовнішньоекономічних операцій, а також веде статистичну звітність.
7.5. Ревізія (аудит) зовнішньоекономічної діяльності відображається у річних фінансових звітах підприємства та здійснюється контролюючим органом підприємства або незалежними аудиторськими організаціями.

8. ВІДШКОДУВАННЯ ЗБИТКІВ

8.1. Збитки, яких підприємство може зазнати в процесі своєї діяльності, покриваються за рахунок резервного фонду, а також за рахунок інших фондів за рішенням засновника.

9. ПРАВА ЗАСНОВНИКА

9.1. Засновник підприємства:
- вносить зміни та доповнення до статуту підприємства;
- визначає основні напрями діяльності підприємства, затверджує перспективні річні плани та звіти про їх виконання;
- визначає порядок використання прибутку підприємства;
- призначає та звільняє з посади директора підприємства, укладає з ним контракт;
- приймає рішення про ліквідацію та реорганізацію підприємства.

10. ОРГАНИ УПРАВЛІННЯ ТА КОНТРОЛЮ ПІДПРИЄМСТВА

10.1. Орган управління підприємства представлений директором підприємства.
10.2. Директор підприємства вирішує всі питання діяльності підприємства за винятком тих, які віднесені статутом до компетенції засновника. Директор здійснює керівництво поточною діяльністю підприємства на підставі прав, визначених статутом.
10.3. Директор підприємства, зокрема:
- за згодою засновника підприємства розпоряджається майном підприємства;
- затверджує штатний розклад, визначає форми і системи оплати праці персоналу підприємства, враховуючи принципи розподілу винагород за кінцевими результатами;
- затверджує поточні плани діяльності підприємства та заходи, що є необхідними для вирішення його завдань;

Продовження додатку А

- затверджує щорічний кошторис, штатний розклад та посадові оклади працівників, встановлює показники, розміри та їх преміювання;
- затверджує договірні ціни на продукцію та тарифи на послуги;
- приймає на роботу та звільняє з роботи працівників підприємства, застосовує до них заходи заохочення та накладає стягнення;
- приймає рішення про відрядження працівників;
- організовує ведення бухгалтерського обліку та звітності в підприємстві;
- укладає зовнішньоекономічні угоди в порядку, визначеному чинним законодавством України;
- подає на затвердження засновнику річний звіт та баланс підприємства;
- приймає рішення з інших питань, пов'язаних з поточною діяльністю підприємства.

10.4. Директор підприємства має право:
- без довіреності діяти від імені підприємства, представляти його в усіх установах, підприємствах та організаціях як в Україні, так і за її межами;
- укладати будь-які угоди та інші юридичні акти у порядку, встановленому чинним законодавством України;
- видавати довіреності, відкривати у банках розрахунковий рахунок та інші рахунки;
- здійснювати іншу діяльність для досягнення мети підприємства в межах своєї компетенції.

10.5. Контроль за фінансово-господарською діяльністю підприємства здійснюється ревізійною комісією, яка призначається засновником. Директор підприємства не має права бути членом ревізійної комісії.

10.6. До завдань ревізійної комісії належить щорічна перевірка річного звіту та балансу підприємства.

10.7. Ревізійна комісія підприємства:
- здійснює контроль за фінансовою та господарською діяльністю підприємства;
- перевіряє правильність ведення обліку та звітності;
- вимагає від посадових осіб підприємства подання їй усіх необхідних матеріалів, бухгалтерських та інших документів та особистих пояснень;
- направляє результати перевірок засновнику підприємства;
- складає заключення по річному звіту та балансу;
- зобов'язана попередити засновника підприємства, якщо з'явилася загроза інтересам підприємства або виявлені зловживання посадових осіб підприємства.

10.8. Річний звіт та баланс подаються засновнику підприємства тільки із заключенням ревізійної комісії.

10.9. Ревізійна комісія веде протоколи всіх своїх засідань.

10.10. Підприємство за погодженням із засновником та за свій рахунок може запросити спеціалізовану установу для перевірки та підтвердження річного фінансового звіту (зовнішній аудит).

11. ОБЛІК ТА ЗВІТНІСТЬ

11.1. Підприємство здійснює облік результатів господарської діяльності, веде оперативний, бухгалтерський і статистичний облік. Організація документообігу в підприємстві встановлюється директором підприємства.

11.2. Відповідальність за стан обліку, своєчасне надання бухгалетрської та іншої звітності покладається на директора та головного бухгалтера підприємства у відповідності з чинним законодавством.

11.3. Фінансовий рік встановлюється з 1 січня по 31 грудня включно.

11.4. Звітність по операціях підприємства складається в підприємстві у строки, визначені чинним законодавством і подається на затвердження засновнику підприємства.

11.5. Посадові особи підприємства несуть відповідальність за достовірність інформації, що міститься в звітності.

12. ПРАЦЯ ТА ЇЇ ОПЛАТА

12.1. Праця працівників може здійснюватись на підставі трудових договорів, в тому числі контрактів, штатних посад, за сумісництвом, а також на підставі цивільно-правових угод будь-якого виду.

12.2. Директор підприємства має право залучати до роботи українських та іноземних спеціалістів, визначати форми, системи, розміри оплати праці згідно з чинним законодавством України.

Продовження додатку А

12.3. Загальний розмір виплат за результатами праці окремих працівників підприємства не обмежується.
12.4. У разі необхідності для виконання робіт та послуг підприємство має право залучати громадян та їх колективи на основі угод, у тому числі: угод підряду, доручення, трудових угод, контрактів та інших форм угод, передбачених цивільним законодавством, з оплатою праці на договірній основі.
12.5. Штатні працівники підприємства підлягають соціальному та медичному страхуванню і соціальному забезпеченню в порядку і на умовах, встановлених чинним законодавством.

13. КОМПЕТЕНЦІЯ ТА ПОВНОВАЖЕННЯ ОРГАНІВ ТРУДОВОГО КОЛЕКТИВУ

13.1. Трудовий колектив підприємства становлять усі громадяни, які своєю працею беруть участь у його діяльності на основі трудового договору (контракту, угоди), а також інших форм, що регулюють трудові відносини працівника з підприємством.
13.2. Органом самоврядування трудового колективу підприємства є збори трудового колективу підприємства (надалі - збори).
13.3. Трудовий колектив підприємства на зборах:
- розглядає і затверджує проект колективного договору з підприємством;
- розглядає і вирішує питання самоврядування трудового колективу;
- визначає і затверджує перелік і порядок надання працівникам підприємства соціальних пільг.
13.4. Регулювання взаємовідносин між трудовим колективом та засновником підприємства або уповноваженим ним органом визначається у колективному договорі.
13.5. У період між зборами трудового колективу його функції виконує рада трудового колективу підприємства, повноваження якої визначаються на зборах трудового колективу.

14. РЕОРГАНІЗАЦІЯ ТА ЛІКВІДАЦІЯ ПІДПРИЄМСТВА

14.1. Реорганізація підприємства (злиття, приєднання, розподіл, виділення, перетворення) здійснюється за рішенням засновника підприємства.
14.2. Ліквідація підприємства проводиться за рішенням засновника підприємства або за рішенням суду чи господарського суду у випадках, передбачених чинним законодавством України.
14.3. Ліквідація підприємства здійснюється ліквідаційною комісією, призначеною засновником підприємства, судом чи господарським судом.
14.4. Ліквідаційна комісія публікує в офіційній пресі за місцем знаходження підприємства інформацію про ліквідацію підприємства.
14.5. З моменту призначення ліквідаційної комісії до неї переходять усі повноваження по управлінню справами підприємства.
14.6. Порядок і строки ліквідації підприємства встановлюються засновником підприємства або судом (господарським судом). Строк для заяви претензій кредиторів не може бути менше 2 місяців з моменту повідомлення про ліквідацію підприємства.
14.7. Ліквідаційна комісія:
- оцінює наявне майно підприємства;
- виявляє дебіторів і кредиторів підприємства і проводить розрахунки з ними;
- проводить заходи по сплаті боргів підприємства третім особам та засновнику;
- складає ліквідаційний баланс і представляє його засновнику підприємства.
14.8. Залишки підприємства після розрахунків з бюджетом, оплати праці робітників підприємства, розрахунків з кредиторами, використовуються за рішенням засновника.
14.9. Підприємство вважається реорганізованим або ліквідованим з моменту виключення його з Єдиного державного реєстру.
14.10. Ліквідаційна комісія несе відповідальність за збитки, заподіяні підприємству, його засновнику та третім особам, за нормами цивільного законодавства.
14.11. При ліквідації (реорганізації) підприємства документи по особовому складу передаються на зберігання правонаступнику або державному архіву.

Статут складено з 14 статей на 8 аркушах.

Засновник приватного підприємства «СЦ СЕРВІС-МАЙСТЕР» _____

Іванов Валерій Володимирович

UNICHECK

Ім'я користувача:
Аудиту Іванова Лариса

ID перевірки:
1015423806

Дата перевірки:
05.06.2023 10:34:01 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
05.06.2023 10:35:54 EEST

ID користувача:
100005737

Назва документа: **Мельник Д.О._Організація інформаційної безпеки системи обліку та внутрішнього контрол...**

Кількість сторінок: **62** Кількість слів: **14403** Кількість символів: **118289** Розмір файлу: **135.69 KB** ID файлу: **1015086053**

5.05%
Схожість

Найбільша схожість: **0.65%** з Інтернет-джерелом (https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/9367/1/%D0%9C%D0%

2.77% Джерела з Інтернету	221	Сторінка 64
4.8% Джерела з Бібліотеки	585	Сторінка 66

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

УДК 657.6

Мельник Д.О.,
студент ф-ту ОПМ, 4 курсу, спец. 071 «Облік і оподаткування»,
Київський національний економічний університет імені Вадима Гетьмана,
Науковий керівник — Кошець О.В. — к.е.н.,
професор кафедри аудиту

СИСТЕМИ ОБЛІКУ ТА ВНУТРІШНЬОГО КОНТРОЛЮ НА ПІДПРИЄМСТВІ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Системи обліку та внутрішнього контролю є невід'ємною частиною діяльності будь-якої компанії. Ці процеси допомагають забезпечити ефективне використання корпоративних ресурсів і дотримання нормативних актів. У сучасних умовах, із зростанням рівня кіберзагроз та кібератак, інформаційній безпеці систем обліку та внутрішнього контролю слід приділяти особливу увагу.

Однією з основних проблем, що виникають у контексті інформаційної безпеки, є забезпечення конфіденційності, цілісності та доступності даних. У зв'язку з цим суб'єкти господарювання повинні забезпечити належний рівень захисту інформації в системах обліку та внутрішнього контролю [1].

Поточний стан систем обліку та внутрішнього контролю підприємства може відрізнятися залежно від конкретної компанії та її бізнес-процесів. Але в цілому можна виділити наступні тенденції:

- Автоматизація. Більшість підприємств використовують автоматизовані системи обліку та внутрішнього контролю, які дозволяють ефективно управляти бізнес-процесами та отримувати регулярну звітність.
- Забезпечення захисту інформації. Більшість компаній дуже серйозно ставляться до захисту своєї інформації, особливо завдяки використанню різних технологій безпеки, таких як антивірусні програми, брандмауери, шифрування даних тощо.
- Недостатня увага до ризику. У деяких підприємствах процеси оцінки ризиків, пов'язані з системою обліку та внутрішнього контролю, можуть не існувати або бути неповними. Це може призвести до підвищення вразливості системи та збільшення ризику кібератак.
- Недостатня кваліфікація персоналу. Захист інформації від кіберзагроз залежить від кваліфікації персоналу компанії та культури безпеки. Недостатня кваліфікація персоналу перешкоджає досягненню належного рівня інформаційної безпеки.
- Використання застарілого обладнання та програмного забезпечення. Застаріле апаратне та програмне забезпечення вразливе до кібератак, тому компанії повинні забезпечити постійне оновлення та модернізацію своїх систем.

Щоб забезпечити належний рівень інформаційної безпеки в системах обліку та внутрішнього контролю, підприємства повинні вживати заходів щодо забезпечення конфіденційності, цілісності та доступності даних [2]. До таких заходів належать:

- Оцінка ризику. Компанії повинні проводити регулярну оцінку ризиків, пов'язаних із системами обліку та внутрішнього контролю, щоб визначити потенційні загрози та ризики.
- Регулярне оновлення програмного та апаратного забезпечення. Компанії повинні забезпечити постійне оновлення апаратного та програмного забезпечення, щоб зменшити ризик кібератак.
- Захист від шкідливих програм. Компанії повинні забезпечити захист від шкідливих програм, таких як віруси, хробаки та троянські програми. Це може включати використання антивірусного програмного забезпечення та застосування політики безпеки щодо використання електронної пошти, Інтернету та USB-накопичувачів.
- Правильно організувати доступ до даних. Компанії повинні забезпечити належний рівень контролю доступу до даних, щоб уникнути несанкціонованого доступу до конфіденційної інформації.
- Резервне копіювання даних. Підприємства повинні забезпечити резервне копіювання даних, щоб їх можна було відновити у разі проблем із системами обліку та внутрішнього контролю.
- Навчання та підвищення кваліфікації персоналу. Організації повинні навчати та вдосконалювати персонал щодо заходів із забезпечення інформаційної безпеки та культури безпеки в цілому.
- Аудит систем захисту інформації. Підприємства повинні проводити регулярні аудити системи інформаційної безпеки, виявляти можливі порушення та недоліки та вживати заходів щодо їх усунення.

Підприємству важливо розуміти загрози і ризики інформаційної безпеки, планувати та вживати заходи для їх уникнення та управління ними. Крім того, необхідно пам'ятати про постійний розвиток та оновлення засобів захисту інформації, оскільки кіберзлочинці постійно знаходять нові способи атак і проникнення в системи [3].

Підсумовуючи, системи обліку та внутрішнього контролю підприємств мають бути захищені від можливих кібератак та забезпечувати конфіденційність, цілісність та доступність даних. Для цього потрібна регулярна оцінка ризиків, оновлення програмного забезпечення, надійні паролі, захист мережі та резервне копіювання даних. Організаційний персонал також повинен бути навчений і знати про культуру безпеки та практику інформаційної безпеки.

Список використаних джерел:

1. Вітер С. А., І. І. Світлишин. Захист облікової інформації та кібербезпека підприємства. Економіка та суспільство. *2017. № 11. С. 497–502.*
URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf (дата звернення 07.05.2023).

2. Ілляшенко К.В. Інформаційна безпека сучасного бухгалтерського обліку. Науковий вісник Міжнародного гуманітарного університету. 2019. № 40. С. 179–183. URL: http://vestnik-econom.mgu.od.ua/journal/2019/40-2019/25.pdf (дата звернення 07.05.2023).

3. Данилюк І.В., Зорій Н.М. Оцінка обліку та системи внутрішнього контролю як інструменти безпеки бізнесу. Глобальні та національні проблеми економіки. 2016. № 9. С. 765-770. URL: http://global-national.in.ua/archive/9-2016/157.pdf (дата звернення 07.05.2023).

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

СЕРТИФІКАТ

ПІДТВЕРДЖУЄ, ЩО

МЕЛЬНИК Дмитро

взяв(ла) участь у роботі платформи

«Інноваційні та digital-технології обліку, аналізу та аудиту для забезпечення післявоєнного відновлення та розвитку України»

в межах ЮВІЛЕЙНОЇ 90-ОЇ ЩОРІЧНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ
«ІННОВАЦІЙНІ ПРОЄКТИ ДЛЯ ПІСЛЯВОЄННОГО ВІДНОВЛЕННЯ
ТА РОЗВИТКУ УКРАЇНИ»

Проректор з наукової роботи
д.е.н., професор

Лариса Антонюк

17 КВІТНЯ - 20 ТРАВНЯ 2023 РОКУ
М.КИЇВ, УКРАЇНА