НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет харчових технологій та управління якістю продукції АПК

УДК 006.83:664.7(477.41)

ПОГОДЖЕНО
Декан факультету
харчових технологій та управління якістю продукції АПК
_____ **Баль-Прилипко Л.В.**
«__» _____ 2023 р.

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
Завідувач кафедри
стандартизації та сертифікації сільськогосподарської продукції
_____ **Толок Г.А.**
«__» _____ 2023 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розроблення елементів СУБХП в умовах ФГ "КУЛИНИЧІ", Київська обл.»

Спеціальність: **152 «Метрологія та інформаційно-вимірювальна техніка»**
Освітня програма – **«Якість, стандартизація та сертифікація»**
Орієнтація освітньої програма – **Освітньо-професійна програма**

Гарант освітньої програми
к.т.н., доцент _____ **Слива Ю.В.**

Керівник магістерської роботи
к.т.н., доцент _____ **Слива Ю.В.**

Виконав _____ **Сидоренко О.О.**

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет харчових технологій та управління якістю продукції АПК

ЗАТВЕРДЖУЮ:
Завідувач кафедри
стандартизації та сертифікації
сільськогосподарської продукції,
канд. техн. наук, доц.
Толок Г.А.
«__» _____ 2023 р.

З А В Д А Н Н Я
ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ
Сидоренко Олксандру Олександровичу

Спеціальність: 152 «Метрологія та інформаційно-вимірювальна техніка». Освітня програма – «Якість, стандартизація та сертифікація». Програма підготовки – Освітньо-професійна Тема магістерської роботи: «Розроблення елементів СУБХП в умовах ФГ "КУЛИНИЧІ", Київська обл.» затверджена наказом ректора НУБіП України № 370 «С» від 13.03.2023 року. Термін подання завершеної роботи на кафедру 1 листопада 2023 р.

Вихідні дані до магістерської роботи: 1) Положення про підготовку магістрів у НУБіП України; 2) Положення про підготовку і захист магістерської роботи 3) Міжнародні та національні стандарти; 3) Словникові та довідникові джерела; 4) Навчальна та наукова література; 5) Методичні вказівки про підготовку магістерської роботи; 6) Фахові періодичні видання; 7) Матеріали державної статистики; 8) Електронні ресурси.

Перелік питань, що підлягають дослідженню:

1) **Потенційні ризики цифрового управління безпечністю харчових продуктів**
2) **Практичні дослідження**
3) **Порівняння результатів цифрових систем з традиційними методами**
4) **Аналіз поточної системи управління**
5) **Розробка програмного забезпечення**
6) **Тренінг і навчання персоналу**
7) **Рекомендації щодо управління ризиками та вдосконалення системи управління безпечністю харчових продуктів**

Дата видачі завдання «27» травня 2023 р.

Керівники магістерської роботи _____ Слива Ю. В.

Завдання прийняв до виконання _____ Сидоренко О. О.

РЕФЕРАТ

Магістерська робота складається із вступу, семи розділів, висновків та пропозицій, робота містить 43 літературних джерел, 6 таблиць та 9 рисунків.

Мета роботи Розроблення та діджиталізація елементів СУБХП в умовах ФГ "КУЛИНИЧІ"

У *першому розділі* проведено аналіз основних ризиків, пов'язаних із використанням цифрових систем у харчовій промисловості.

У *другому розділі* проаналізовано результати досліджень і надано висновки щодо ефективності використання цифрових систем управління безпечністю харчових продуктів.

У *третьому розділі* проведено порівняльний аналіз ефективності цифрових систем з традиційними методами управління безпечністю харчових продуктів.

У четвертому розділі було здійснено докладний аналіз поточних систем управління безпечністю харчових продуктів ФГ "КУЛИНИЧІ" і визначенню їх недоліків.

У *п'ятому розділі* наведено процес розробки спеціалізованого програмного забезпечення для моніторингу та відстеження виробництва харчових продуктів. Проведено детальний аналіз функцій та можливостей цього програмного забезпечення.

У шостому розділі розглянуто розробку програми навчання та підготовки персоналу для впровадження цифрових систем управління та висвітлено важливість цього аспекту.

Сьомий розділ містить рекомендації щодо ефективного управління ризиками та покращення системи управління безпечністю харчових продуктів.

Ключові слова: *Діджиталізація, Безпечність, Система менеджменту безпечності*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СМЯ - Система менеджменту якості;

СУЯ - Система управління якості;

ISO - International Organization for Standardization (Міжнародна організація зі стандартизації);

IoT – Інтернет речей (Internet of Things);

ПЗ – Програмне забезпечення

ВСТУП

В сучасному світі динамічного розвитку технологій та глибокої діджиталізації всіх галузей господарства, питання забезпечення безпеки та якості харчових продуктів набуває особливого актуальності та значущості. В умовах цифрового середовища, де дані стають основним ресурсом, а інформаційні технології впроваджуються на всіх етапах виробництва та постачання продукції, аналіз ризиків та розробка стратегій управління ними стають необхідними завданнями для забезпечення безпеки та якості харчових продуктів.

Дана дипломна робота присвячена комплексному дослідженню аспектів цифрового управління безпечністю харчових продуктів. Вона включає в себе аналіз потенційних ризиків, які виникають у зв'язку з впровадженням цифрових рішень у сфері безпечності харчових продуктів, а також розробку стратегій для їхнього управління.

Даний дипломний проект спрямований на розкриття можливостей цифрових технологій у сфері безпечності харчових продуктів та розвиток стратегій для ефективного управління ризиками, пов'язаними з цією галуззю. Результати досліджень та розробок, представлених у цій роботі, можуть сприяти покращенню безпеки та якості харчових продуктів, а також сприяти подальшому розвитку цифрових інновацій у сфері харчової промисловості.

РОЗДІЛ 1. ПОТЕНЦІЙНІ РИЗИКИ ЦИФРОВОГО УПРАВЛІННЯ БЕЗПЕЧНІСТЮ ХАРЧОВИХ ПРОДУКТІВ

У сучасному цифровому світі цифрове управління безпечністю харчових продуктів набуває все більшого значення для галузі харчової промисловості. За допомогою цифрових технологій і систем управління можна ефективно контролювати та моніторити процеси виробництва, забезпечуючи якість та безпеку харчових продуктів. Однак разом з перевагами цифрового управління приходять і ризики, які важливо розглядати та аналізувати для забезпечення безпеки і якості продукції.

Огляд потенційних ризиків цифрового управління

Витоки даних та конфіденційність

Один із основних ризиків цифрового управління безпечністю харчових продуктів - це можливість витоку конфіденційних даних. Зберігання та обробка важливих даних про рецепти, інгредієнти, технологічні процеси, інформацію про клієнтів і партнерів може бути предметом кібератак та порушень конфіденційності.

Витоки даних продовжують домінувати в заголовках у всьому світі. Незважаючи на більшу увагу, що приділяється безпеці даних, хакери постійно знаходять нові способи обійти захист, щоб отримати доступ до цінних корпоративних даних і облікових даних [3].

За допомогою складних методів соціальної інженерії, програм-вимагачів, зловмисних програм чи кібератак сторонніх ланцюжків поставок, хакери намагаються проникнути в конфіденційну інформацію, викрити її та отримати з неї прибуток.

Відповідно до звіту про дослідження безпеки на основі ризиків, протягом перших дев'яти місяців 2019 року було повідомлено про 5183 зломи, що розкрило понад 7,9 мільярда скомпрометованих записів. Порівняно з 2018 роком загальна кількість витоків даних зросла на 33,3%, а загальна кількість розкритих записів зросла більш ніж удвічі – на 112%.

На жаль, це тривожне збільшення витоків даних не корелює з підвищенням організаційної готовності. Насправді багато організацій надзвичайно недостатньо підготовлені та не впроваджують основні заходи безпеки, необхідні для запобігання кібератакам хакерів.

У недавньому дослідженні, проведеному компанією Kaspersky, більше половини отримувачів (57%) сказали, що вони не мають політики кібербезпеки, а це більше ніж дві третини (71%) середніх підприємств (від 250 до 549). співробітники).

Саме таке самовдоволення кібербезпекою наражає організації на значний ризик і піддає їх ретельній перевірці як з боку регуляторних органів, так і з боку їхніх клієнтів, якщо станеться порушення.

Організації повинні повністю усвідомити далекосяжні наслідки, які порушення даних може мати для їхнього бізнесу, якщо вони хочуть зменшити ризик і захиститися від атак [6].

Деякі з найбільш згубних наслідків витоку даних включають:

1. Фінансові втрати

Фінансовий вплив витоку даних, безсумнівно, є одним із найнегайніших і найважчих наслідків, з якими організаціям доведеться мати справу. Згідно з нещодавнім дослідженням Ponemon Institute, вартість витоку даних зросла на

12% за останні п'ять років до 3,2 мільйона фунтів стерлінгів у середньому по всьому світу.

Таблиця 1.1

Топ-15 країн (регіонів світу) за кількістю кіберінцидентів у 2020 р.

Країна / регіон	Кількість випадків, %	Середня загальна вартість втрачених даних, млн дол. США	Причини втрати даних, %		
			Зловмисна атака	Системний збій	Людська помилка
США	12	8,64	54	22	24
Індія	9	2,00	53	26	21
Великобританія	8	3,90	52	23	25
Німеччина	7	4,45	57	24	19
Франція	7	4,01	55	24	21
Японія	6	4,19	51	26	23
Середній Схід	6	6,52	59	24	17
Канада	5	4,50	42	35	23
Південна Корея	5	3,12	50	29	21
АСЕАН	4	2,71	48	22	30
Австралія	4	2,15	57	22	21
Скандинавія	4	2,51	48	30	22
Італія	4	3,19	52	19	29
Латинська Америка	4	1,68	56	26	18
Туреччина	4	1,77	50	25	25

Витрати можуть включати компенсацію постраждалим клієнтам, створення заходів реагування на інциденти, розслідування порушення, інвестиції в нові заходи безпеки та юридичні збори, не кажучи вже про приголомшливі регуляторні штрафи, які можуть бути накладені за невідповідність GDPR (Загальні Регламент про захист даних) [8].

Організації, які порушують GDPR, можуть бути оштрафовані на суму до 4% річного світового обороту або 20 мільйонів євро, залежно від того, що більше. Якщо організації перебувають у будь-якій люзі, що ці фінансові штрафи не будуть виконані, нещодавні штрафи, накладені на British Airways і Marriot, підкреслили, наскільки серйозно ICO має намір сприймати порушення GDPR.

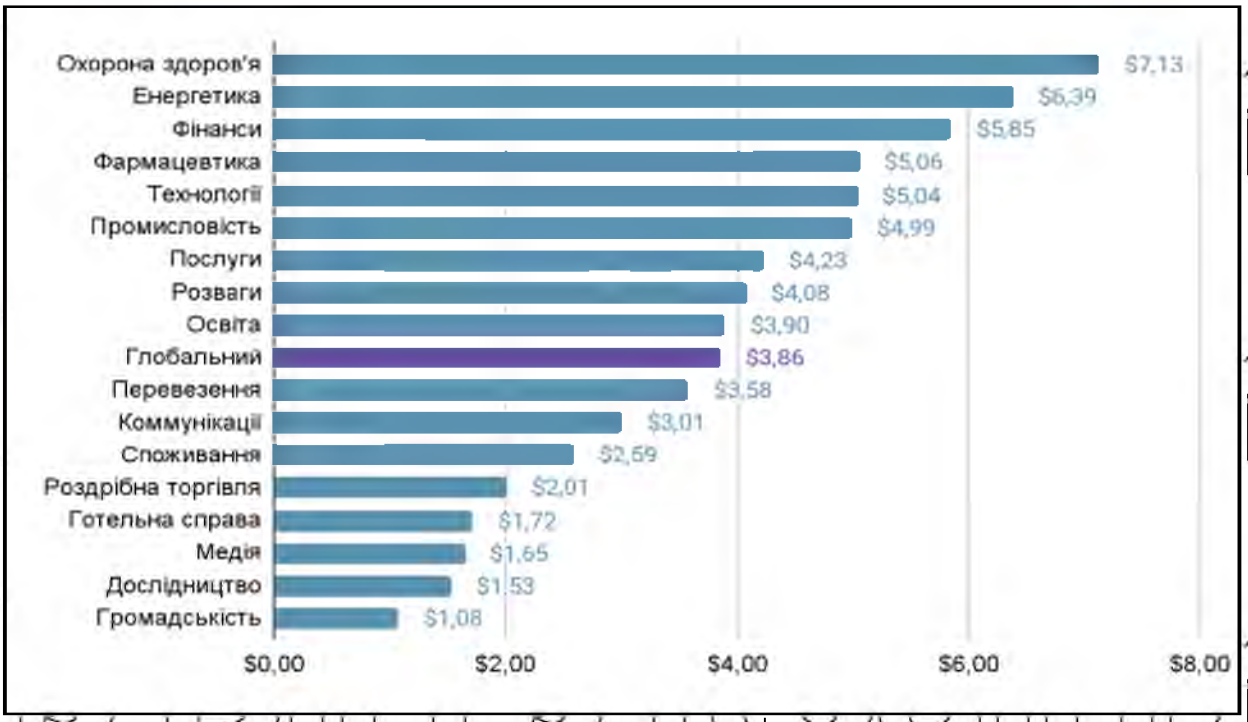

Рисунок 1.1 Середня вартість втрачених даних від кіберінцидентів за сферами економіки

(у млн дол. США)

Порушення також може суттєво вплинути на ціну та оцінку акцій компанії. Це саме те, що сталося з Yahoo після того, як його зламали в 2013 році. Інформацію про злом стало відомо в 2016 році, коли компанію збиралася викупити американська телекомунікаційна компанія Verizon. Придбання відбулося, коли компанія придбала Yahoo за зниженою ставкою 4,48 мільярда доларів, що приблизно на 350 мільйонів доларів менше початкової ціни [7].

2. Шкода репутації

Репутаційна шкода в результаті витоку даних може бути руйнівною для бізнесу. Дослідження показали, що до третини клієнтів у сфері роздрібної торгівлі, фінансів та охорони здоров'я припинять співпрацювати з організаціями, які були зламані. Крім того, 85% розкажуть іншим про свій досвід, а 33,5% звернуться до соціальних мереж, щоб виплеснути свій гнів.

Новини швидко розповсюджуються, і організації можуть стати глобальною новиною протягом кількох годин після розкриття порушення. Ця негативна преса в поєднанні з втратою довіри споживачів може завдати непоправної шкоди компанії, яка порушила правила.

Споживачі дуже усвідомлюють цінність своєї особистої інформації, і якщо організації не можуть продемонструвати, що вони вжили всіх необхідних заходів для захисту цих даних, вони просто підуть і підуть до конкурента, який більш серйозно ставиться до безпеки. Порушення даних може легко призвести до крадіжки особистих даних, коли конфіденційна інформація стає доступною для неавторизованих осіб. Хакери можуть використовувати цю інформацію, щоб викрасти особисті дані людини та вчиняти шахрайські дії, наприклад відкривати нові облікові записи або робити несанкціоновані покупки.

Репутаційна шкода має тривалий характер і також вплине на здатність організації залучати нових клієнтів, майбутні інвестиції та нових працівників у компанію.

3. Оперативний простій

Бізнес-операції часто будуть серйозно порушені після злому. Організаціям потрібно буде стримати витік даних і провести ретельне розслідування того, як це сталося та до яких систем було здійснено доступ.

Можливо, доведеться повністю припинити роботу, поки слідчі не отримають усі необхідні відповіді. Цей процес може зайняти дні, навіть тижні, щоб виявити вразливі місця, залежно від серйозності порушення. Це може мати величезний додатковий вплив на дохід і здатність організації відновлюватися.

Відповідно до Gartner, середня вартість простою мережі становить близько 5600 доларів США за хвилину. Це приблизно 300 000 доларів США на годину. Це, очевидно, буде відрізнятися залежно від розміру організації та галузі,

на яку це впливає, але очевидно, що це може мати руйнівний вплив і суттєво вплинути на продуктивність бізнесу.

4. Правовий позов

Згідно з правилами захисту даних, організації зобов'язані продемонструвати, що вони вжили всіх необхідних заходів для захисту персональних даних. Якщо безпеку даних буде порушено, навмисно чи ні, особи можуть звернутися до суду з вимогою компенсації.

Як у США, так і у Великій Британії спостерігається величезне збільшення колективних позовів, оскільки жертви вимагають грошової компенсації за втрату витоку даних.

Порушення даних Equifax у 2017 році торкнулося понад 145 мільйонів людей у всьому світі, і компанія виплатила понад 700 мільйонів доларів компенсації постраждалим клієнтам у США. Порушення торкнулося приблизно 15 мільйонів клієнтів у Великій Британії, які зараз подали власний окремий судовий позов до високого суду, вимагаючи 100 мільйонів фунтів стерлінгів компенсації.

Оскільки частота та серйозність порушень продовжують зростати, ми можемо очікувати, що більше таких групових справ буде передано до суду.

2.2. Кібербезпека

Кібербезпека - це ще один ключовий аспект управління ризиками цифрового середовища. Атаки з метою викрадення чи пошкодження даних можуть призвести до серйозних наслідків, які включають в себе можливість контамінації харчових продуктів чи зниження якості продукції.

Таблиця 1.2

Практичне значення кібербезпеки

№ п/п	Ситуація	Опис ситуації
1	Користувач має справу з загрозою «нульового дня»	Процес розробки нових вірусів постійно триває, і в разі, якщо від моменту створення шкідливого програмного забезпечення пройшло дуже мало часу, наприклад, менше доби, розробники захисного програмного забезпечення фактично не встигають належним чином вивчити цю загрозу та розробити відповідний захист або включити її в базу антивірусних сигнатур. В такому випадку користувач залишається майже беззахисним перед хакером.

2	Від моменту створення вірусу пройшо вже певний часовий проміжок, його ще не включили в базу сигнатур.	Цей фактор значно залежить від типу антивірусного програмного забезпечення, його можливостей та потужності. Проте, враховуючи статистику (щороку з'являється близько 90 мільйонів нових варіантів шкідливого програмного забезпечення), включити всі ці 100% загроз до бази антивірусних сигнатур - практично нереалістичне завдання для будь-якого розробника. Цілком зрозуміло, що навіть найсильніше антивірусне програмне забезпечення може не впоратися з таким великим обсягом нових загроз, які постійно з'являються в онлайн-середовищі.
Ситуація		Опис ситуації
3	Антивірус не володіє функцією евристичного аналізу	Для боротьби з вірусами, яких немає в базі сигнатур, використовується метод захисту, відомий як "евристичний аналіз". Це означає, що антивірус вивчає поведінку програм на комп'ютері, шукаючи ознаки, які можуть вказувати на схожість з типовою поведінкою шкідливого програмного забезпечення. Проте цей підхід має свої обмеження: він не підтримується всіма антивірусами, може помилятися, визнаючи безпечні програми як

		потенційно шкідливі, і не завжди гарантує безпечне видалення вірусів і т. д.
4	Антивірус не здатен до самозахисту	Особливо сильні та досконалі віруси можуть самостійно виявляти наявність антивірусного програмного забезпечення на пристрої і вирішувати вимкнути або призупинити його роботу ще до того, як антивірус встигне спрацювати. Вирішення цієї проблеми можливе лише завдяки поєднанню кібергігієни та використання потужного та надійного антивірусного програмного забезпечення.

Впровадження стандарту ISO/IEC 27001:2013 створює цілий спектр можливостей для ефективного управління інформаційною безпекою в підприємствах незалежно від їх власності. Ці можливості включають:

1. Виявлення потенційних ризиків і використання відповідних заходів контролю для мінімізації інформаційних загроз.

2. Здатність підприємства гнучко адаптувати своє управління, відповідаючи змінам у сфері інформаційної безпеки.

3. Забезпечення довіри та інтересів клієнтів у тому, що їхні дані належним чином захищені.

4. Відповідність вимогам сучасності.

Система управління інформаційною безпекою, згідно з ISO/IEC 27001:2013, надає можливість впроваджувати кращі практики для поліпшення захисту даних та усунення загроз інформаційним системам. Ефективне

управління безпекою інформаційних систем досягається завдяки регулярному моніторингу та аудиту системи.

Вплив ISO/IEC 27001:2013 на діяльність компанії або організації проявляється в різних аспектах бізнесу:

1. Репутація: Впровадження процедур для швидкого виявлення порушень інформаційної безпеки сприяє підвищенню репутації компанії.

2. Зацікавлені сторони: Визначення всіх внутрішніх і зовнішніх зацікавлених сторін, які мають відношення до системи управління інформаційною безпекою.

3. Відповідність: Надання основи для ефективного ведення юридичних і нормативних вимог і повідомлення цих вимог іншим зацікавленим сторонам.

4. Управління ризиками: Оцінка ризиків інформаційної безпеки допомагає вчасно виявляти можливі недоліки та реагувати на них.

Розуміння області застосування стандарту ISO/IEC 27001 впливає на процес управління підприємством та інформацією клієнтів. Важливим аспектом є створення культури свідомості про безпеку в компанії, що відповідає вимогам ISO/IEC 27001, що зміцнює довіру клієнтів до здатності компанії захищати їхні дані.

Аварійні ситуації та відмови систем

Системні аварії та відмови в роботі цифрових систем можуть стати значним ризиком для безпеки харчових продуктів. Наприклад, відмови в системах моніторингу чи контролю можуть призвести до невідомих аномалій у виробництві та втрати якості продукції.

3.1. Забруднення та контамінація

Витоки даних, кібератаки та відмови систем можуть призвести до невірного контролю процесів виробництва. Це може призвести до забруднення харчових продуктів шкідливими бактеріями, вірусами, чи іншими забруднювачами[11].

3.2. Втрата якості продукції

Вплив ризиків цифрового управління також відображається на якості харчових продуктів. Невірне управління та моніторинг може призвести до недоліків у продукції, зміни смакових властивостей та погіршення якості.

Аналіз потенційних ризиків цифрового управління безпечністю харчових продуктів вказує на важливість вдосконалення системи кібербезпеки, створення заходів для запобігання витокам даних, та ретельного контролю системних аспектів. Розуміння цих ризиків дозволить розробити ефективні стратегії управління та покращити безпеку та якість харчових продуктів в цифровому середовищі.

1.2 Висновки до розділу 1

У цьому розділі було представлено аналіз потенційних ризиків цифрового управління безпечністю харчових продуктів у сучасній харчовій промисловості. Цей аналіз підкреслив важливість обережного планування та впровадження цифрових технологій для забезпечення безпеки та якості продукції.

Одним із головних ризиків є витік конфіденційних даних, що може виникнути внаслідок кібератак та порушень безпеки даних. Це може призвести до фінансових втрат, шкоди репутації організації та оперативного простою. Організації також повинні бути готові до можливості правових позовів від осіб, чиї дані були втрачені внаслідок порушення.

Важливо підкреслити, що безпека даних та захист від кібератак стають все більш важливими завданнями для підприємств у харчовій промисловості. Проведення аналізу ризиків, розробка стратегій управління та вжиття необхідних заходів є обов'язковими для забезпечення безпеки та якості продукції. На додачу, організації повинні бути готові до негативних наслідків витоку даних та намагатися попередити такі події, вдосконалюючи свої системи безпеки даних та надавати пріоритет цій проблемі.

У цифровому світі, де дані мають велике значення, захист від кібератак та ефективне управління ризиками є важливою частиною стратегії підприємства в харчовій промисловості. Тільки з правильним підходом до цих питань організації можуть забезпечити безпеку та якість харчових продуктів, зберігати довіру споживачів та забезпечити успішну діяльність.

Для успішного управління ризиками в цифровому середовищі, компанії повинні приділяти велику увагу кібербезпеці та безпеці даних. Важливо мати ефективні заходи захисту даних та вдосконалені системи моніторингу та виявлення можливих загроз. Стандарт ISO/IEC 27001:2013 надає цінний фреймворк для забезпечення інформаційної безпеки та контролю ризиків. Впровадження цього стандарту може сприяти збільшенню репутації компанії та покращенню захисту даних.

Додатково, компанії повинні бути готовими до реагування на системні аварії та відмови. Розробка ефективних планів відновлення та резервного копіювання є важливою для забезпечення неперервності виробництва та збереження якості харчових продуктів.

Остаточно, аналіз ризиків цифрового управління безпечністю харчових продуктів визначає, що безпека та якість продукції можуть бути в значній мірі під загрозою в цифровому середовищі. Ретельне планування, вдосконалення

кібербезпеки та системний контроль - це важливі складові для успішного управління цими ризиками та забезпеченням безпеки і якості харчових продуктів. Тільки шляхом поєднання цих заходів компанії можуть ефективно функціонувати в цифровому світі та захищати інтереси своїх клієнтів.

РОЗДІЛ 2: ПРАКТИЧНІ ДОСЛІДЖЕННЯ

2.1. Дослідження впровадження цифрових рішень у компаніях

Дослідження впровадження цифрових рішень у компаніях надає глибоке розуміння того, як ці технології впливають на діяльність підприємств у галузі безпечності харчових продуктів. В цьому підрозділі ми докладно розглянемо кілька ключових аспектів дослідження:

Аналіз реальних прикладів впровадження цифрових рішень. Опис конкретних прикладів компаній, які впровадили цифрові інструменти для контролю якості та безпеки харчових продуктів. Дослідження включає вивчення технологій, які використовуються, витрат та користі, отримані компаніями.

Зв'язуючи концепцію цифрових рішень та контролю якості та безпеки харчових продуктів, важливо відзначити, що інтернет речей (IoT) грає значну роль у вдосконаленні цих процесів в харчовій промисловості. Дозвольте розглянути два приклади компаній, які впровадили цифрові рішення для контролю якості та безпеки продуктів [5].

Приклад 1: Nestlé та IoT виробництво

Компанія Nestlé, один з найбільших світових виробників харчових продуктів, використовує IoT-технології для покращення контролю якості та безпеки своїх продуктів. Вони встановили сенсори на своєму обладнанні та виробничих лініях для моніторингу параметрів виробництва, таких як температура, вологість, тиск і час обробки. Ці дані транслюються в режимі реального часу до центральної системи, де проводиться аналіз та порівняння зі стандартами якості. Якщо будь-який параметр виходить за межі припустимих норм, система сповіщає відповідних операторів, що дозволяє вчасно реагувати на відхилення та виправляти їх. Це призвело до зменшення кількості браку та підвищення якості продукції, що впливає на рентабельність компанії.

Nestlé Purina і QR-коди: Підрозділ компанії Nestlé Purina, що виробляє корм для тварин, використовує QR-коди на упаковці продуктів. Споживачі можуть сканувати коди, щоб перевірити деталі про склад та джерело інгредієнтів [17].

Приклад 2: IBM Food Trust та блокчейн-технології

IBM Food Trust - це ініціатива, яка використовує блокчейн-технологію для забезпечення контролю якості та безпеки харчових продуктів на всьому ланцюжку постачання. Учасники цієї системи, включаючи виробників, перевізників та роздрібних торговців, можуть додавати і перевіряти інформацію про продукти, від початкового виробництва до продажу. Це дозволяє ідентифікувати джерело продуктів та відстежувати умови їх транспортування та зберігання. В разі виявлення проблеми або небезпеки, інформація може бути відразу доступною для вжиття необхідних заходів для видалення продуктів з ризиком. Це допомагає уникнути харчових вибухів та забезпечує безпеку споживачів.

Приклад 3: Walmart і технологія блокчейн

Велика роздрібна мережа Walmart впровадила блокчейн-технологію для відстеження постачання свіжих продуктів, таких як листя салату та куряче м'ясо. Завдяки цьому, споживачі можуть перевірити джерело продуктів, а також отримувати інформацію про умови їх зберігання та транспортування.

Приклад 4: Mars Inc. і IoT для моніторингу виробництва

Mars Inc., виробник популярних продуктів, таких як шоколад і корм для тварин, використовує IoT для моніторингу виробничих процесів. Датчики та зв'язки дозволяють контролювати параметри виробництва, а також надавати відповідну інформацію для підвищення якості продукції.

Приклад 5: Anheuser-Busch InBev і аналітика даних

Виробник пива Anheuser-Busch InBev використовує аналітику даних для моніторингу якості сировини та виробництва пива. Вони аналізують дані з різних джерел, включаючи сенсори та лабораторні тести, для вдосконалення процесів та забезпечення безпеки продукції.

Приклад 6: Tyson Foods і штучний інтелект

Tyson Foods використовує штучний інтелект для виявлення аномалій та дефектів у м'ясній продукції. Штучний інтелект аналізує зображення та датчикові дані для виявлення відхилень від стандартів якості.

Ці приклади демонструють, як різні компанії в харчовій промисловості впроваджують цифрові рішення для забезпечення контролю якості та безпеки продуктів, що призводить до покращення якості продукції та підвищення довіри споживачів.

Цифрові рішення, такі як IoT і блокчейн-технології, відіграють ключову роль у забезпеченні контролю якості та безпеки харчових продуктів для підприємств у харчовій промисловості. Вони допомагають підвищити продуктивність, зменшити витрати та підвищити якість продукції, а також забезпечити безпеку та надійність продуктів для споживачів. Дослідження технологій та їхній вплив на підприємства показують, що цифрові рішення стають важливим інструментом для досягнення успіху в сучасній харчовій промисловості.

Інтернет речей (IoT) - це технологічний концепт, який став популярним в останні роки. IoT передбачає підключення фізичних об'єктів (приладів, машин, сенсорів) до Інтернету, щоб забезпечити збір та обробку даних в режимі реального часу. Цей підхід дозволяє створити "розумні" системи та пристрої, які можуть спілкуватися між собою та з операторами, а також надавати цінну

інформацію для прийняття управлінських рішень. У цьому рефераті розглянемо сутність IoT та його користь для підприємств.

Інтернет речей: сутність і складові

IoT - це система взаємопов'язаних об'єктів, обладнаних сенсорами, програмним забезпеченням та зв'язками, що дозволяє збирати, передавати та аналізувати дані. Сенсори вимірюють фізичні параметри, такі як температура, вологість, рух, а також можуть фіксувати події, такі як включення/вимикання, натискання тощо. Зібрані дані передаються через мережу до облікового центру, де вони обробляються та аналізуються.

Елементи IoT включають:

Сенсори та пристрої збору даних: Датчики, камери, GPS-пристрої та інші засоби для збору інформації.

Мережеві з'єднання: Забезпечують передачу даних до центральної обробки.

Центральні сервери та хмарові обчислення: Місце обробки та зберігання даних.

Аналітика та програмне забезпечення: Здатність аналізувати та інтерпретувати дані для прийняття рішень.

Користь IoT для підприємств

Підвищення продуктивності: IoT дозволяє віддалено контролювати та моніторити процеси виробництва, що сприяє підвищенню ефективності та зменшенню витрат.

Зменшення витрат: Оптимізація виробничих процесів, моніторинг стану обладнання та попередження відмов дозволяють економити кошти на ремонті та обслуговуванні.

Підвищення якості продукції: Збір та аналіз даних з датчиків дозволяє вчасно виявляти дефекти та покращувати якість продукції.

Розширення нових послуг: IoT дозволяє розробляти нові послуги та продукти, такі як підписка на моніторинг стану обладнання.

Підвищення безпеки: Моніторинг у режимі реального часу та автоматична реакція на аварійні ситуації сприяють зниженню ризику нещасних випадків.

У 2024 році очікується, що кількість "розумних" будинків в США сягне 69,91 мільйона. Протягом наступних років ця цифра буде зростати: у 2025 році до 77,05 мільйона, а в 2026 році до 84,92 мільйона. Прогнозується, що до 2027 року "розумними" пристроями користуватимуться 93,59 мільйона американських домогосподарств.

Згідно з прогнозами, кількість пристроїв Інтернету речей (IoT) у світі майже подвоїться, зростаючи з 15,1 мільярда у 2020 році до понад 29 мільярдів у 2030 році.

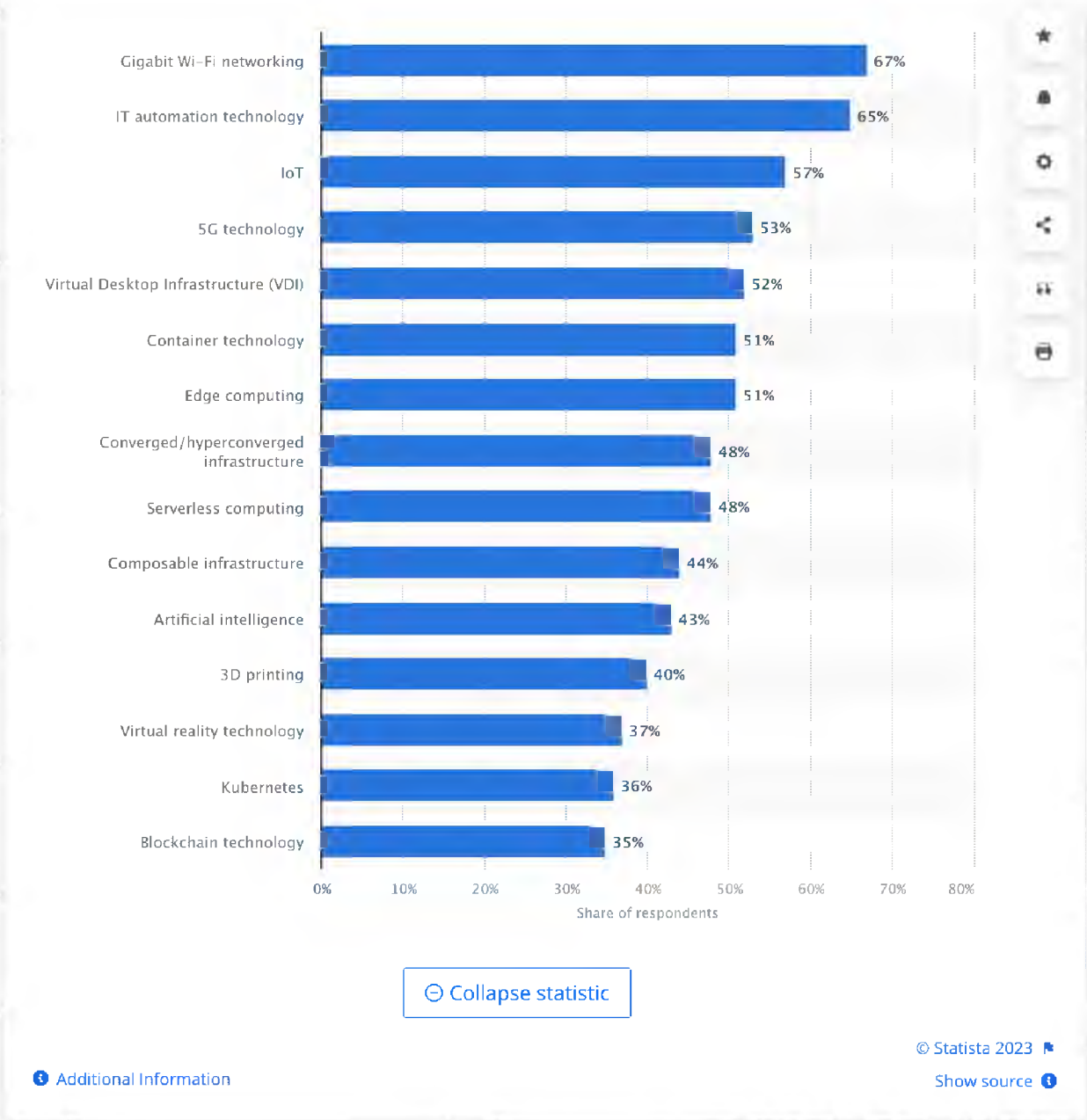

Рисунок 2.1 частка IoT в порівнянні з іншими технологіями

У 2023 році технологія Інтернету речей (Internet of Things) займає третє місце за кількістю впроваджених або запланованих до впровадження технологій в північноамериканських та європейських організаціях. Зараз понад половина

(57%) північноамериканських та європейських організацій вже використовують IoT в своїй діяльності.

У 2021 році близько 41,9% американських домогосподарств були обладнані пристроями розумного дому, і за прогнозами, до 2025 року цей показник зросте до 48,4%.

У 2017 році лише 20% світового населення користувалося мобільним зв'язком. Проте очікується, що найближчими роками ця ситуація зазнає кардинальних змін.

Розмір глобального промислового ринку Інтернету речей становив 320,9 мільярдів доларів США в 2022 році, і передбачається, що до 2032 року він зросте приблизно до 1 562,35 мільярдів доларів США. Прогнозується, що середньорічний темп зростання (CAGR) складатиме 17,2% протягом прогнозованого періоду з 2023 по 2032 рік.

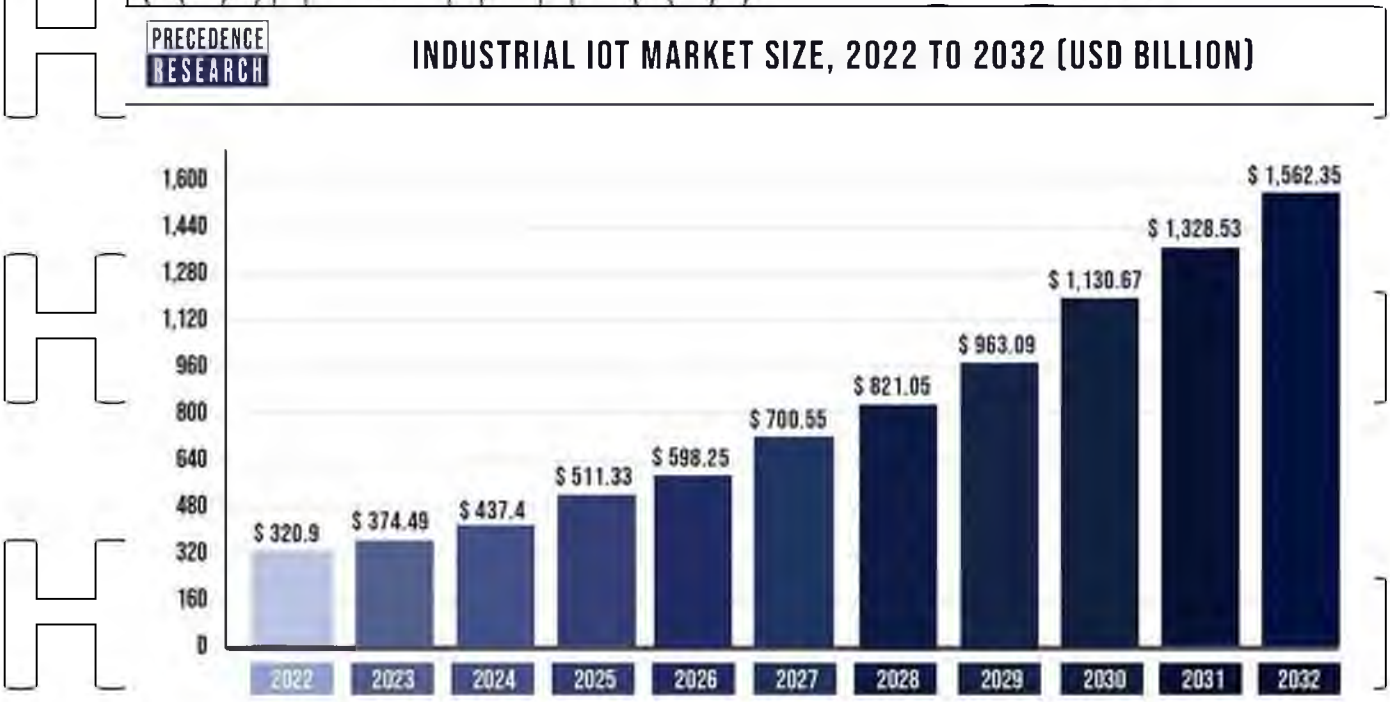

Рисунок 2.2 Промисловий ринок IoT

На момент 2023 року Сполучені Штати, Китай, Японія, Південна Корея і Німеччина визнані п'ятьма провідними країнами в галузі Інтернету речей (IoT). Ці країни виділяються найбільшою кількістю IoT-пристроїв та є ключовими учасниками на ринку IoT.

Інтернет речей має потенціал забезпечити економічну вартість від $4 трлн до $11 трлн до 2025 року, згідно з оцінками McKinsey.

Безпека залишається важливим пріоритетом у сфері Інтернету речей (IoT) як для розробників, так і для користувачів. Це не дивно, оскільки в 2021 році було зафіксовано 1,5 мільярда кібератак на пристрої Інтернету речей.

Згідно з даними IoT Analytics, економія витрат є основним джерелом доходу для понад половини бізнес-проектів, пов'язаних з IoT. Лише 35% таких проектів спрямовані на збільшення прибутку.

За даними IDC, 58% виробників вважають, що Інтернет речей є стратегічно необхідною складовою для цифрової трансформації промислових операцій.

У сфері охорони здоров'я рост інновацій є ключовою перевагою IoT. Інтернет речей використовується у багатьох аспектах, включаючи моніторинг пацієнтів, вимірювання споживаної енергії та медичне обладнання для отримання зображень і рентгенівських променів.

У 2022 році виробничий сектор був домінуючим на ринку промислового IoT. Це пояснюється широким впровадженням рішень IoT та цифрових технологій у виробничому процесі на різних виробничих підприємствах.

Інтернет речей - це перспективна технологія, яка може значно покращити функціонування підприємств у різних галузях. Впровадження IoT дозволяє підприємствам збирати, аналізувати та використовувати дані для підвищення

продуктивності, зменшення витрат та підвищення якості продукції. Поряд із зростанням доступності та розвитком технологій IoT може стати ключовим фактором для конкурентоспроможності підприємств у майбутньому.

Оцінка ефективності цифрового управління: Аналіз результатів, які отримані компаніями внаслідок впровадження цифрових рішень. Виокремлення переваг та недоліків цих ініціатив, враховуючи вплив на якість та безпеку харчових продуктів.

Моніторинг та контроль параметрів виробництва: Дослідження того, як цифрові системи дозволяють компаніям моніторити та керувати параметрами виробництва, такими як температура, вологість, тиск, а також контроль за термінами придатності продуктів.

Автоматизація процесів та зменшення людських помилок: Розгляд автоматизованих систем та їх вплив на зменшення людських помилок у виробництві та контролі за якістю продукції.

2.2 Дослідження впровадження цифрових рішень в конкретних регіонах

В даному розділі досліджується вплив цифрового управління на безпеку та якість харчових продуктів в різних географічних областях.

Регіональні особливості, такі як кліматичні умови, географічне розташування та інфраструктура, можуть впливати на можливість та придатність цифрових рішень для впровадження [16]. Ось деякі приклади:

Кліматичні умови:

Автоматизовані системи зрошення в аридних регіонах: В аридних або пустельних регіонах, де велика вологість є дефіцитною, цифрові системи для

автоматизованого зрошення можуть бути життєво важливими для сільськогосподарської продуктивності. Вони можуть контролювати і регулювати полив, враховуючи конкретні показники вологості та погодні умови.

Прикладом є Ізраїль, де компанія "Netafim" успішно впроваджує цифрові системи зрошення для сільськогосподарських угідь в умовах пустельного клімату.

"Нетафім" використовує сучасні технології, включаючи сенсори для вимірювання рівня вологості грунту, погодних умов та системи зворотного зв'язку для автоматичного регулювання поливу. Це дозволяє точно і ефективно використовувати воду, зменшуючи втрати і забезпечуючи оптимальний полив для рослин.

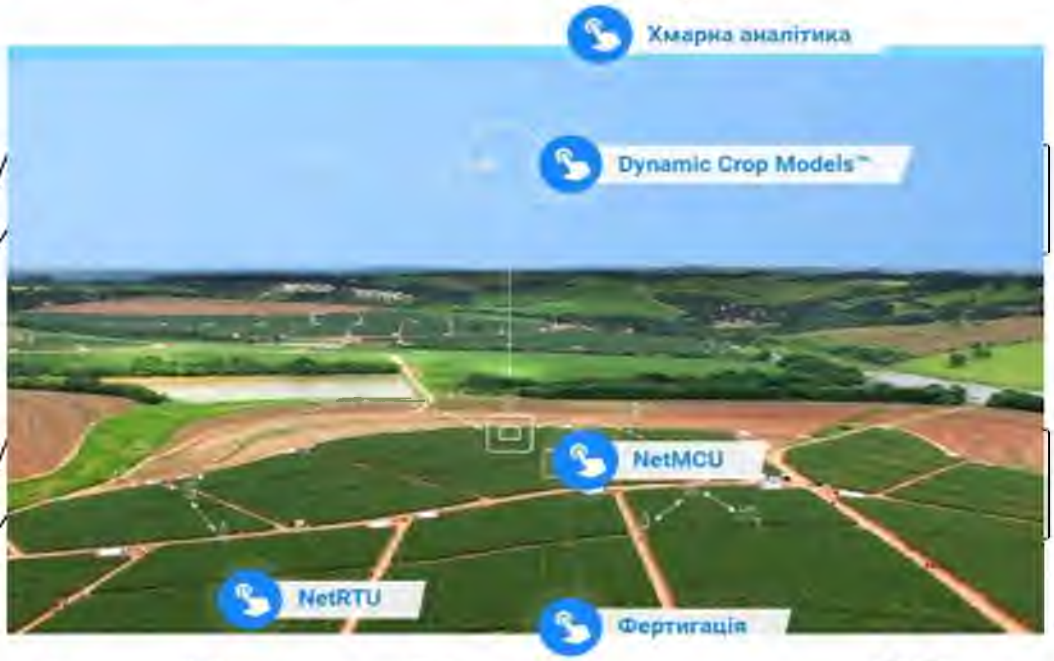

Рисунок 2.3 комплексний підхід NetBeat

Однією за таких ініціатив даної компанії є Netafim, яка надає сільським господарям і агрономам інноваційні рішення для управління системами зрошення та поливу в сільському господарстві. Ця система використовує цифрові

технології та хмарні обчислення для моніторингу та управління поливом різних видів культур.

NetBeat дозволяє сільським господарям отримувати реальний час інформацію про стан рослин, вологості грунту та інші важливі параметри для прийняття обгрунтованих рішень щодо поливу. Вона допомагає оптимізувати використання води та ресурсів, зменшувати витрати та збільшувати врожайність.

Таблиця 2.1

Діяльність NetBeat

Ініціативи, що впроваджує "Netafim"	В чому їх користь ?
Хмарна аналітика	Допомагає сільським господарям ефективно використовувати ресурси, підвищувати врожаї та зменшувати ризики, забезпечуючи доступ до важливих даних в будь-який час та з будь-якого місця.
Dynamic Crop Models	Динамічні моделі рослинництва полегшують прогнозування врожаїв, оптимізацію виробництва та підвищення стійкості сільськогосподарських господарств до зміни клімату, знижують ризики та витрати.
NetMCU	Дає фермерам можливість планувати зрошення, збирати дані з датчиків і отримувати рекомендації в реальному часі. Все, як на долоні.
Ініціативи, що впроваджує "Netafim"	В чому їх користь ?

Ініціативи, що впроваджує "Netafim"	В чому їх користь ?
NetRTU	Надає фермерам швидкий доступ до даних і можливість керувати зрошенням у режимі реального часу.
Фертигація	Фертигація дозволяє точно дозувати добрива та поживні речовини відповідно до потреб рослин. Це зменшує втрати та надлишкове використання добрив, що економить ресурси та забезпечує оптимальний ріст рослин.

Крім того, NetBeat сприяє адаптації сільськогосподарських господарств до зміни клімату та забезпечує стійкість до негоди та екстремальних умов. Ця ініціатива покликана підтримати сільськогосподарський сектор в досягненні сталого розвитку та ефективного використання ресурсів.

Такий підхід є критично важливим для підвищення продуктивності в сільському господарстві в аридних регіонах, де вода обмежена, і землеробство є важливою галуззю економіки. Системи зрошення "Netafim" дозволяють оптимізувати використання води та підвищити врожаї при обмежених ресурсах. Це розкриває важливість цифрових рішень для сталого розвитку сільського господарства в аридних регіонах.

Прогнозування стихійних лиходіть: У регіонах, які часто піддаються природним стихіям, таким як урагани, цунамі чи повені, цифрові системи для прогнозування та реагування на такі події можуть рятувати життя та майно. Наприклад, системи раннього попередження можуть надавати важливу інформацію жителям та органам управління.

Географічне розташування:

Сільські райони та гірські регіони: В гірських регіонах, де доступність до ресурсів та транспорту обмежена, цифрові рішення можуть бути використані для моніторингу земель та ресурсів, розподілу медичної допомоги або навіть для забезпечення зв'язку в умовах відсутності стійкого мережевого підключення.

Сільські райони з обмеженим доступом до освіти: В деяких віддалених сільських районах із низьким рівнем освіти цифрові рішення можуть допомагати у доступі до онлайн-освіти та навчальних матеріалів. Це особливо важливо в умовах пандемії COVID-19.

Інфраструктура:

Розвинена мережа мобільного зв'язку: У регіонах з розвиненою мережею мобільного зв'язку цифрові рішення, такі як мобільні додатки для фінансів чи медицини, можуть швидко поширюватися та надавати важливі послуги жителям.

Відсутність електропостачання: В деяких віддалених сільських районах, де електроенергія обмежена або недоступна, цифрові рішення повинні бути дуже ефективними та економічно доступними, щоб працювати на альтернативних джерелах живлення, наприклад, сонячних батареях або генераторах.

Sistema.bio в Латинській Америці: У Латинській Америці, де сільське господарство важливе для економіки, Sistema.bio використовує цифрові технології для управління біопаливними системами та сприяє збільшенню врожаю та якості грунту.

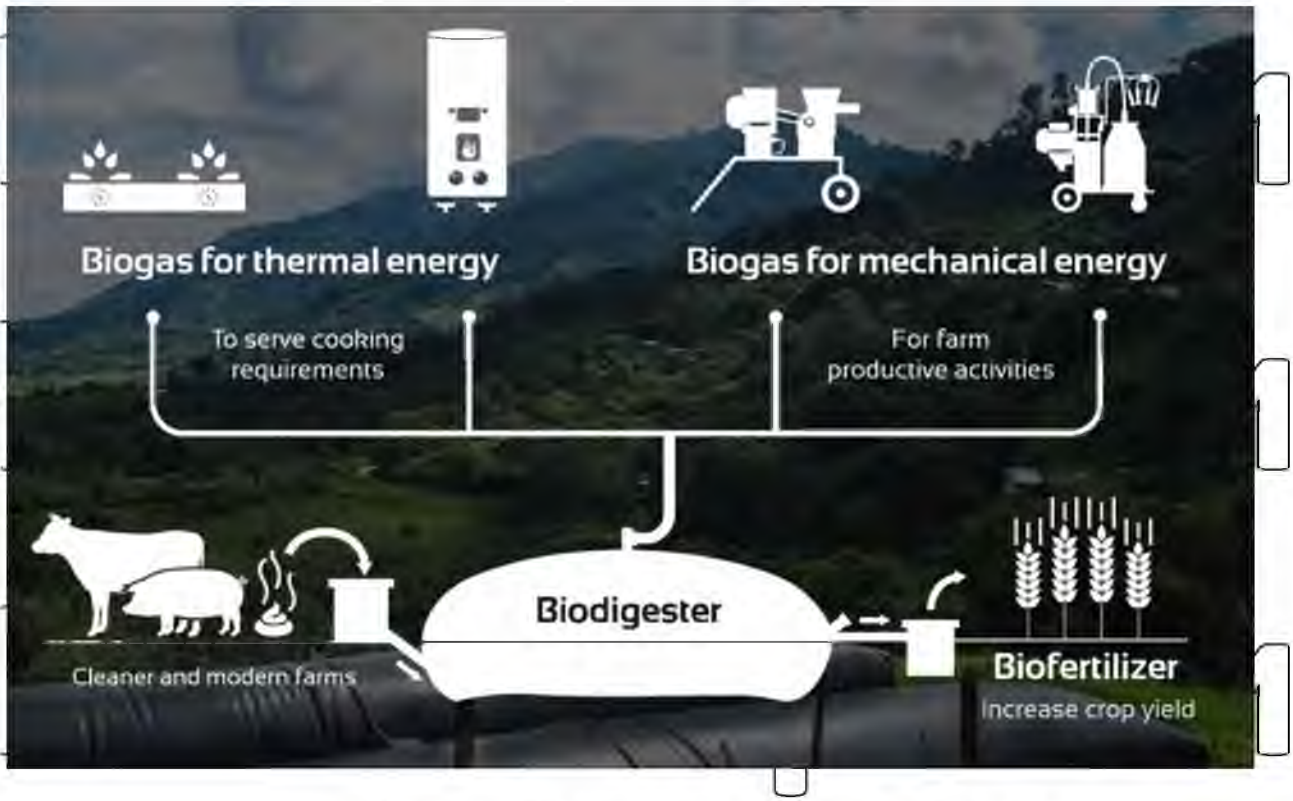

Рисунок 2.4 принцип роботи Sistema.bio

Sistema.bio - це готовий модульний пакет біодайджесторів, який включає повний набір біогазових пристроїв і з'єднань. Прості в установці та використанні, наші запатентовані високоефективні біореактори збирають органічні відходи та перетворюють їх на відновлюваний біогаз і потужне органічне добриво. Sistema.bio - це соціальний проєкт, спрямований на надання інноваційних та сталої ефективності рішень для дрібних сільських фермерів в Латинській Америці та інших регіонах. Головною метою цієї ініціативи є вирішення проблем, з якими стикаються фермери у відходів та покращенні сільськогосподарської продуктивності.

1. Технологія біогазу: Sistema.bio найбільше відома своєю технологією біогазу, яка передбачає встановлення біодайджесторів на фермах. Біодайджестори - це пристрої, які використовують органічні відходи, такі як

залишки культур та тваринний навіс, для виробництва біогазу. Цей біогаз може використовуватися для приготування їжі, обігріву та генерації електроенергії. Процес анаеробного перетворення в біодайджесторах не лише виробляє біогаз, але і дає високоякісне органічне добриво, яке може покращити якість грунту та врожаї.

2. Екологічні переваги: Однією з ключових переваг технології біогазу Sistema.bio є позитивний вплив на навколишнє середовище. Шляхом перетворення органічних відходів на біогаз та органічне добриво ця технологія допомагає зменшити викиди парникових газів та сприяє сталому використанню сільгосвідходів.

3. Сільськогосподарські переваги: Органічне добриво, вироблене біодайджесторами Sistema.bio, багате на поживні речовини та може покращити родючість грунту, що особливо цінно для дрібних сільських фермерів. Це може призвести до збільшення врожаїв та загальної сільськогосподарської продуктивності.

4. Локальне виробництво: Sistema.bio часто виробляє свої біодайджестори на місцях, що допомагає створювати робочі місця в регіонах, де вони працюють. Цей підхід також зменшує витрати на транспортування та підтримує місцеву економіку.

5. Фінансування та підтримка: Sistema.bio надає варіанти фінансування та підтримки дрібним сільським фермерам, дозволяючи їм отримувати та встановлювати біодайджестори на своїх фермах. Вони співпрацюють з різними партнерами та організаціями, щоб зробити ці рішення доступними для більшої кількості людей

6. Вплив: Sistema.bio зробила позитивний вплив в декількох країнах Латинської Америки та за її межами. їхні рішення сприяють розвитку сільських

територій, сталому сільському господарству та зменшенню бідності, надаючи чисту енергію, покращуючи родючість ґрунту та зменшуючи тягар фермерів.

Рисунок 2.5 вплив та користь Sistema.bio

Отже, Sistema.bio зосереджується на сталому сільському господарстві та виробництві чистої енергії за допомогою біодайджесторів. Шляхом пропонування доступних та екологічних рішень для дрібних сільських фермерів, Sistema.bio вирішує екологічні, сільськогосподарські та соціальні проблеми в регіонах, таких як Латинська Америка. Їхні роботи ілюструють потенціал технології та інновацій для створення позитивних змін в сільському господарстві.

Ці приклади показують, що регіональні особливості суттєво впливають на можливість та придатність цифрових рішень для конкретних регіонів і наголошують важливість адаптації технологій до конкретних умов.

Регіональні особливості, такі як кліматичні умови, географічне розташування та інфраструктура, впливають на можливість та придатність цифрових рішень для впровадження. Тому підхід який передбачає діджиталізацію та автоматизацію всіх процесів є найбільш перспективним. Тому,

що враховує конкретні потреби та обмеження кожного регіону, а отже є наразі найбільш обіцяючим в сільському господарстві та інших галузях, оскільки він дозволяє адаптувати технології до конкретних умов і максимально використовувати їх потенціал.

2.3 Висновки до розділу 2

У даному розділі були розглянуті ключові аспекти впровадження цифрових рішень в галузі безпечності харчових продуктів. Аналізуючи приклади компаній, які успішно використовують цифрові інструменти, ми можемо побачити, що ці технології відіграють важливу роль у покращенні контролю якості та безпеки харчових продуктів.

Приклади, такі як використання IoT виробництва компанією Nestlé і впровадження блокчейн-технології за ініціативи IBM Food Trust, свідчать про великий потенціал цих цифрових рішень. Вони допомагають виробникам вдосконалити процеси виробництва, підвищити якість продукції та забезпечити безпеку продуктів для споживачів. Компанії, такі як Walmart, Mars Inc., Anheuser-Busch InBev, Tyson Foods, також успішно використовують технології, які допомагають вдосконалити контроль якості та безпеки своїх продуктів.

Усі ці приклади показують, що цифрові рішення грають важливу роль у покращенні продуктивності, зменшенні витрат та підвищенні довіри споживачів до харчових продуктів. Важливо підкреслити, що цифрові технології стають необхідним інструментом для досягнення успіху в сучасній харчовій промисловості.

Зокрема, Sistema.bio представляє інноваційні та сталі рішення для сільськогосподарських фермерів, зосереджуючись на виробництві біогазу та органічного добрива за допомогою біодайджесторів. Ця технологія має ряд переваг, включаючи позитивний екологічний вплив, підвищення

сільськогосподарської продуктивності та зменшення викидів парникових газів. Sistema.bio також активно співпрацює зі своїми клієнтами, надаючи фінансову підтримку та роблячи свої рішення доступними для дрібних фермерів.

Цей соціальний проєкт не лише вирішує практичні проблеми фермерів, але й сприяє сталому розвитку, створенню робочих місць та зменшенню бідності в регіонах, де він діє. Приклади таких рішень також наголошують на важливості адаптації технологій до конкретних регіональних особливостей, враховуючи кліматичні та інфраструктурні умови, для досягнення максимального впливу та користі.

Sistema.bio виступає яскравим прикладом того, як інновації в сільському господарстві та стале виробництво можуть сприяти покращенню умов життя фермерів та збереженню навколишнього середовища.

Зазначена інформація про IoT свідчить про швидкий розвиток цього технологічного концепту та його розширення у різних сферах діяльності. Висновок продовжує підтверджувати важливість IoT для сучасного світу та його вплив на різні аспекти життя та бізнесу.

Зростання кількості "розумних" пристроїв та систем IoT у приватних домогосподарствах та промисловості свідчить про їх популярність та важливість в щоденному житті та виробництві. Технологія IoT принесла користь у плані підвищення продуктивності, зменшення витрат, покращення якості продукції та безпеки процесів.

Прогнози на майбутнє показують значний ріст використання IoT та поширення цієї технології як в приватних домогосподарствах, так і в бізнесі. Збільшення кількості "розумних" будинків, підприємств та об'єктів підтверджує, що IoT буде грати все більш важливу роль у нашому сучасному світі.

РОЗДІЛ 3. ПОРІВНЯННЯ РЕЗУЛЬТАТІВ ЦИФРОВИХ СИСТЕМ З ТРАДИЦІЙНИМИ МЕТОДАМИ

У цьому розділі проводиться докладний порівняльний аналіз між результатами, отриманими за допомогою цифрових систем управління безпечністю харчових продуктів, та традиційними методами контролю та моніторингу. Переваги та недоліки обох підходів визначаються з точки зору ефективності, витрат та забезпечення безпеки харчових продуктів.

Цифрові системи управління безпечністю харчових продуктів

Цифрові системи управління безпечністю харчових продуктів мають ряд важливих переваг у порівнянні з традиційними методами контролю та моніторингу. **Ось детальніше про ці переваги:**

Спостереження в реальному часі: Цифрові системи надають можливість спостерігати процеси виробництва та постачання харчових продуктів в реальному часі. Це дозволяє виявляти проблеми та негайно реагувати на них. Наприклад, в разі виявлення аномалій у процесі виробництва, система може автоматично сповістити відповідних операторів.

Автоматизація та оптимізація: Цифрові системи можуть автоматизувати багато аспектів контролю та моніторингу, такі як вимірювання температури, вологості, тиску, якість повітря, тощо. Це дозволяє знизити витрати праці та ресурсів. Більше того, системи можуть надавати оптимальні рекомендації щодо налаштувань процесів виробництва та поліпшення продуктивності.

Відстежування продуктів: Цифрові системи відстеження та трасування можуть точно визначити джерело можливих загроз безпеці харчових продуктів і дозволяють відстежувати шлях продуктів від виробництва до споживача. Це допомагає у виявленні ізольованих випадків зараження чи інших проблем у постачанні.

Збільшення ефективності і зниження витрат: Цифрові системи допомагають підвищити ефективність виробництва та знизити витрати, оскільки вони дозволяють точно керувати процесами та ресурсами. Наприклад, системи автоматичного поливу можуть зменшити витрати води та покращити якість поливу.

Підвищення стійкості та безпеки: Завдяки цифровим системам можна забезпечити постійний моніторинг та автоматичну реакцію на потенційні загрози безпеці харчових продуктів. Це допомагає уникнути інцидентів та забезпечити безпеку споживачів.

Інтеграція та звітність: Цифрові системи можуть легко інтегруватися з іншими системами управління та надавати детальні звіти та аналізи процесів виробництва та безпеки харчових продуктів.

Загалом, цифрові системи управління безпечністю харчових продуктів надають більше можливостей для забезпечення безпеки та якості харчових продуктів

Незважаючи на численні переваги, цифрові системи управління безпечністю харчових продуктів також мають свої недоліки:

Висока вартість впровадження: Впровадження цифрових систем може бути високою вартістю, особливо для малих сільськогосподарських підприємств чи галузей з обмеженими ресурсами. Це включає в себе витрати на обладнання, програмне забезпечення, навчання персоналу та технічну підтримку.

Спеціалізована експертиза: Використання цифрових систем вимагає наявності технічної експертизи для налагодження та обслуговування системи. Це може становити трудність для галузей з обмеженими технічними ресурсами чи у виробничих підприємствах без великих ІТ-відділів.

Залежність від інфраструктури та енергопостачання: Робота цифрових систем вимагає доступу до стійких мереж Інтернету та енергопостачання. У регіонах з недостатньою інфраструктурою це може бути проблемою.

Загрози кібербезпеці: Цифрові системи піддаються загрозам кібербезпеці. Хакери можуть намагатися вторгнутися у систему та спричинити втрати даних або викликати проблеми у виробництві.

Необхідність оновлень та підтримки: Цифрові системи потребують постійного оновлення та підтримки для забезпечення їхньої працездатності та безпеки. Це може бути витратним та часомістким завданням.

Навчання та адаптація персоналу: Впровадження цифрових систем може вимагати навчання та адаптації персоналу до нових технологій та робочих процесів.

Загалом, недоліки цифрових систем управління безпечністю харчових продуктів пов'язані з вартістю впровадження, технічною складністю та залежністю від інфраструктури. Вибір між цифровими та традиційними методами повинен враховувати конкретні потреби та можливості кожної ситуації.

Традиційні методи контролю та моніторингу

Традиційні методи контролю та моніторингу безпеки харчових продуктів також мають свої переваги, особливо в деяких сферах і контекстах. Ось детальніше основні аспекти, які можна виділити в якості переваг:

Експертність і досвід: Традиційні методи спираються на експертність та досвід фахівців у галузі контролю якості та безпеки харчових продуктів. Експерти можуть точно визначати показники якості та безпеки продуктів і виявляти потенційні загрози, що базується на знаннях і досвіді.

Низькі початкові витрати: Впровадження традиційних методів контролю та моніторингу може бути менше витратним у порівнянні з цифровими системами. Багато з таких методів вимагають обладнання, яке є доступним та відомим на ринку.

Зручність у використанні: Традиційні методи контролю, такі як візуальний огляд чи збір проб, можуть бути зручними для застосування на підприємствах без значних технічних можливостей. Вони не вимагають складної технічної інфраструктури чи навчання персоналу.

Спеціалізована експертиза: Деякі традиційні методи контролю можуть використовувати спеціалізовані апарати чи методи, такі як хроматографія або спектроскопія, що дозволяють точно визначати хімічний склад продуктів та виявляти забруднення.

Наявність інфраструктури: В деяких регіонах та ситуаціях інфраструктура для використання традиційних методів може бути доступною, що робить їх привабливими варіантами для контролю та моніторингу.

Спрощення процесу контролю: Традиційні методи можуть бути менше складними у використанні та розумінні, що дозволяє швидко виявляти проблеми та вживати відповідних заходів.

Загалом, традиційні методи контролю та моніторингу відзначаються своєю доступністю, низькими витратами впровадження та використанням експертної експертизи. Вони можуть бути особливо корисними в контекстах, де висока точність та швидкість реакції не є критичними.

Традиційні методи контролю та моніторингу безпеки харчових продуктів мають свої недоліки, які варто враховувати:

Обмежена точність та об'єктивність: Традиційні методи можуть бути менш точними та об'єктивними порівняно з сучасними цифровими системами. Вони можуть піддаються впливу людського фактору та індивідуальних оцінок операторів.

Затримки в виявленні проблем: Традиційні методи не завжди здатні виявити проблеми в реальному часі. Вони можуть вимагати часу на збір та аналіз зразків, що може призвести до затримок у реакції на потенційні загрози.

Велика витратність праці та часу: Збір проб та їх аналіз може бути витратним за ресурсами та часом завданням, особливо при великих обсягах продукції.

Обмежені можливості моніторингу в реальному часі: Традиційні методи не завжди здатні забезпечити моніторинг в реальному часі, що може бути важливим для виявлення наглих проблем чи відстеження якості продуктів в процесі виробництва.

Залежність від людського фактору: Традиційні методи піддаються людському фактору, і якщо оператори не відповідають вимогам або допускають помилки, це може призвести до невірних результатів.

Відсутність інтеграції та аналітики: Традиційні методи зазвичай не надають можливостей для інтеграції з іншими системами та проведення аналітики даних, що може ускладнити збір та аналіз інформації.

Відсутність трасування та історії продукту: Традиційні методи можуть не забезпечувати можливість трасування шляху продукту від початкової фази виробництва до споживача, що може бути важливим для виявлення проблем та відкликання продукції в разі необхідності.

3.2 Висновки до розділу 3

У підсумку, традиційні методи контролю та моніторингу можуть бути менш точними, вимагати більше ресурсів та часу, а також бути менше підходящими для виявлення проблем в реальному часі. Однак вони все ще залишаються важливими в деяких виробничих сферах та контекстах, особливо коли враховувати вартість впровадження та наявність експертизи. Цифрові системи управління безпечністю харчових продуктів, в свою чергу, мають переваги у сфері моніторингу в реальному часі, автоматизації та відстежуванні, але вимагають великих витрат на впровадження та технічної підготовки. Традиційні методи спираються на досвід, надійність та низькі початкові витрати, але можуть бути менше ефективними та схильними до помилок. Вибір між цими підходами повинен враховувати конкретні потреби та можливості кожного сценарію.

З іншого боку, традиційні методи включають у себе візуальну перевірку, збір зразків для лабораторних аналізів, та інші ручні операції. Це може бути більш часо- та працезатратним процесом, а також менш точним і піддається людським помилкам.

У сучасному світі діджиталізація та використання цифрових рішень, зокрема Internet of Things (IoT), стають все більш привабливими для підприємств, особливо для тих, які мають велику мережу філіалів та комплексну виробничу діяльність. До яких якраз і відноситься ФГ "КУЛИНИЧІ". З врахуванням потреб сучасного бізнесу та вимог ефективності, існують вагомі причини, які обгрунтовують впровадження цифрових рішень.

По-перше, для великих підприємств з численними філіалами та розподіленими структурами традиційні методи контролю та моніторингу можуть бути надто повільними та ресурсоємкими. Впровадження цифрових систем

дозволить здійснювати моніторинг в реальному часі та отримувати дані з різних локацій без зайвих затрат на пересилання та аналіз інформації. Це сприяє швидкій реакції на потенційні проблеми та підвищує загальну ефективність виробничих процесів.

По-друге, діджиталізація допомагає спростити процес розширення бізнесу. Це можливо завдяки наявності готової цифрової інфраструктури та програмного забезпечення, яке легко масштабувати та адаптувати до нових філіалів чи напрямків діяльності. Це робить розвиток підприємства більш швидким та ефективним.

По-третє, важливо враховувати, що впровадження нового програмного забезпечення вимагатиме фінансових витрат та навчання персоналу. Однак, з часом ці витрати виправдаються завдяки підвищенню ефективності, зменшенню витрат та можливості швидко реагувати на зміни на ринку. Крім того, цифрові рішення надають можливість збирати та аналізувати дані, що сприяє прийняттю обґрунтованих рішень та оптимізації бізнес-процесів.

За всіма цими причинами, впровадження цифрових рішень, зокрема IoT, стає важливим кроком для великих підприємств, які прагнуть забезпечити ефективність та конкурентоспроможність у сучасному бізнес-середовищі. Спрощення моніторингу, реагування в реальному часі та можливість легко розширювати бізнес роблять цифрові рішення незамінними для досягнення успіху в глобальному економічному середовищі.

РОЗДІЛ 4: АНАЛІЗ ПОТОЧНОЇ СИСТЕМИ УПРАВЛІННЯ

Розгляд і аналіз існуючої системи контролю та управління безпечністю харчових продуктів на підприємстві є важливим кроком в оцінці ефективності та потреби у впровадженні інноваційних підходів. В даному контексті ми дослідимо, як функціонує поточна система управління на підприємстві, які методи та процедури використовуються для забезпечення безпечності та якості продукції.

Цей аналіз дозволить нам зрозуміти, де можуть бути слабкі місця чи потенційні ризики в існуючій системі контролю та управління безпечністю харчових продуктів на підприємстві.

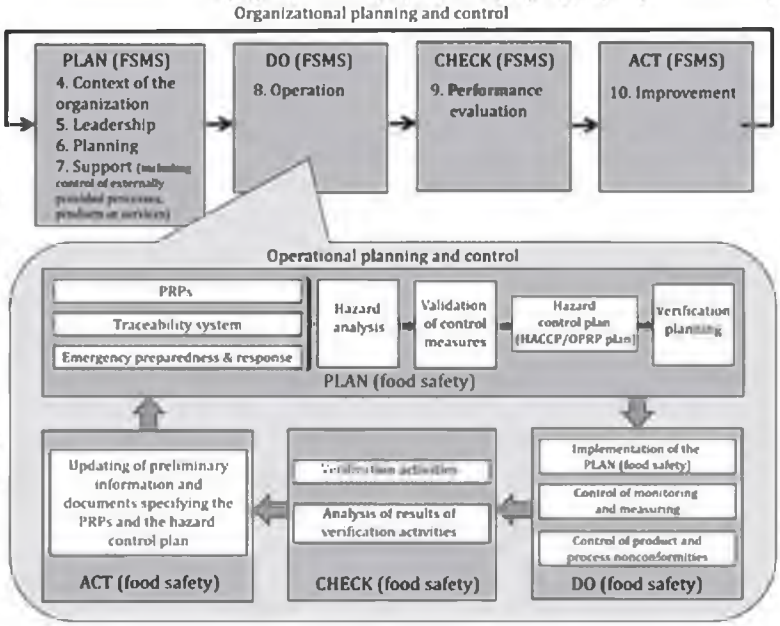

Рисунок 4.1 Ілюстрація циклу Plan-Do-Check-Act

На основі цього аналізу ми зможемо визначити, які саме аспекти потребують поліпшення та де можна впровадити інноваційні підходи для підвищення ефективності та безпечності продукції. На основі принципів HACCP (системи аналізу критичних контрольних точок) та стандарту ISO 22000:2018,

фермерське господарство "Кулиничі" підтримує поточну систему контролю та управління безпечністю харчових продуктів.

Щоб відповідати вимогам ISO 22000:2018 , організація планує та здійснює дії щодо усунення організаційних ризиків. Усунення ризиків створює основу підвищення результативності СМБХП, досягнення поліпшених результатів і запобігання негативних наслідків [1].

Таблиця 4.1 Політика безпеки харчових продуктів ФГ "Кулиничі".

Напрям політики	Сутність
Розробка політики	Фермерське господарство розробляє політику безпеки харчових продуктів, яка визначає загальні принципи та цілі в галузі безпеки продукції. Ця політика визначається керівництвом господарства та відображає їхнє зобов'язання забезпечувати безпеку та якість продукції.
Забезпечення відповідності стандартам	У політиці безпеки харчових продуктів визначається зобов'язання господарства дотримуватися вимог міжнародних стандартів, таких як ISO 22000:2018 та HACCP (система аналізу критичних контрольних точок).
Цілі та завдання	У цьому розділі політики визначаються конкретні цілі та завдання з покращення безпеки та якості продукції. Наприклад, це може включати зниження ризиків захворювань, збільшення терміну придатності продукції, забезпечення відповідності стандартам якості.

Напрям політики	Сутність
Залучення персоналу	У політиці безпеки визначається важливість залучення персоналу до досягнення цілей. Персонал повинен бути свідомим важливості безпеки та якості продукції і дотримуватися відповідних процедур та стандартів.
Оновлення та перегляд	Політика безпеки регулярно оновлюється та переглядається для відповідності змінам в ситуації, новим вимогам та внутрішнім потребам господарства.

Ця ініціатива є ключовою для забезпечення безпеки та якості продукції, яку надає підприємство на ринок. Для кращого розуміння та оцінки впровадження цих стандартів, ми розглянемо систему контролю та управління, яка базується на вищезазначених принципах, і детально проаналізуємо її ефективність та можливість впровадження інноваційних підходів для забезпечення вищих стандартів безпеки та якості продукції на фермерському господарстві "Кулиничі" [2].

Ризик-орієнтований підхід в контролі та управлінні безпечністю харчових продуктів є фундаментальною складовою системи, яка базується на принципах HACCP та ISO 22000:2018. Цей підхід дозволяє фермерському господарству "Кулиничі" систематично та об'єктивно оцінювати та керувати ризиками, пов'язаними з безпечністю харчових продуктів, з метою забезпечення їхньої безпеки та якості.

Детальніше розглянемо основні аспекти ризик-орієнтованого підходу:

Ідентифікація ризиків. Перший крок - ідентифікація потенційних ризиків та небезпек, які можуть впливати на безпеку та якість харчових продуктів на

кожному етапі виробництва. Це можуть бути фізичні, хімічні або біологічні фактори, які мають потенціал створити загрозу продуктам.

Оцінка ризиків: Після ідентифікації ризиків проводиться оцінка їхнього потенціалу впливу та ймовірності виникнення. Ця оцінка дозволяє визначити, наскільки критичними є ці ризики для безпеки та якості продукції [4].

Управління ризиками: Наступний крок - розробка та впровадження стратегій та процедур для зменшення або усунення ідентифікованих ризиків. Це може включати в себе впровадження контрольних точок, моніторинг параметрів виробництва, використання заходів безпеки, навчання персоналу та багато іншого.

Систематичність і постійний моніторинг: Ризик-орієнтований підхід передбачає систематичний моніторинг ризиків та ефективності управління ними. Він базується на принципі постійного вдосконалення та коригування стратегій з урахуванням нової інформації та змін у виробничих процесах [43].

Ризик-орієнтований підхід є ефективним інструментом для забезпечення безпечності та якості харчових продуктів, оскільки він дозволяє ідентифікувати, оцінювати та управляти ризиками на кожному етапі виробництва. Такий підхід допомагає гарантувати високі стандарти безпеки та якості продукції на фермерському господарстві "Кулиничі".

Документація та процедури: Фермерське господарство розробляє та підтримує документацію, яка включає в себе процедури, інструкції та записи, що стосуються безпеки та якості харчових продуктів. Ця документація допомагає систематизувати процеси та забезпечити відповідність стандартам.

Моніторинг та вимірювання: Фермерське господарство проводить моніторинг та вимірювання параметрів, які впливають на безпеку та якість

харчових продуктів. Це може включати збір зразків для аналізу, вимірювання температурних режимів, вологості, а також моніторинг виробничих процесів.

Управління постачальниками: Фермерське господарство співпрацює з постачальниками сировини та інших матеріалів для забезпечення їхньої відповідності стандартам безпеки та якості. Від них вимагається відповідна документація та зобов'язання щодо безпеки продукції.

Навчання та підвищення кваліфікації персоналу: Фермерське господарство забезпечує навчання та підвищення кваліфікації свого персоналу, щоб забезпечити їхню компетентність у питаннях безпеки та якості харчових продуктів.

4.2 Висновки до розділу 4

Таким чином робимо висновок, що фермерське господарство "Кулиничі" активно впроваджує систему контролю та управління безпечністю харчових продуктів на основі принципів HACCP (системи аналізу критичних контрольних точок) та стандарту ISO 22000:2018. Ця ініціатива дозволяє господарству відповідати високим вимогам та стандартам щодо безпеки та якості продукції, що надається на ринок.

Головною метою даного проєкту є діджиталізація та автоматизація існуючих процесів на фермерському господарстві "Кулиничі". Це означає впровадження сучасних цифрових технологій та систем для покращення управління безпечністю харчових продуктів. А саме програмного забезпечення на базі IoT. Діджиталізація дозволить оптимізувати процеси контролю, моніторингу та аналізу ризиків, зробить їх більш ефективними та доступними. Автоматизація спростить виконання процедур та забезпечить їхню послідовність, що важливо для виконання стандартів [35].

РОЗДІЛ 5: РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

5.1 Розробка спеціалізованого програмного забезпечення для моніторингу та відстеження виробництва харчових продуктів

Розробка спеціалізованого програмного забезпечення для моніторингу та відстеження виробництва харчових продуктів є ключовим етапом цифрової трансформації в галузі безпеки та якості продукції. Ця система має на меті поліпшити контроль, безпеку та якість продукції на підприємствах, а також забезпечити відстеження та попередження можливих ризиків.

Процес розробки спеціалізованого програмного забезпечення включає наступні кроки:

Аналіз вимог: Спочатку необхідно провести детальний аналіз вимог щодо моніторингу та відстеження виробництва харчових продуктів. Це включає в себе визначення функціональних, технічних та безпекових вимог.

Загальний опис системи

Даний додаток є інтегрованою системою, спрямованою на відстеження та контроль процесів виробництва та якості харчових продуктів. Додаток складається з двох ключових частин: клієнтської та серверної. Кожна з частин виконує свої функції та має власні функціональні та нефункціональні вимоги. Основна задача даного програмного забезпечення полягає в задоволенні вимог представлених в таблиці 5.1. Додаток має забезпечити оперативний контроль показників безпечності, таких яких температура робочих поверхонь, таймерів строку придатності продукції, вологості повітря та ін., також необхідно максимально інтегрувати данне ПЗ у вже існуючу екосистему виробничого обладнання.

В результаті аналізу функціональних вимог до розроблюваного програмного продукту було виявлено, що найбільш оптимальною архітектурою для цього проєкту є клієнт-серверна архітектура. У цій архітектурі серверний модуль відповідає за взаємодію з базою даних і зовнішніми ресурсами, а також за агрегацію та збір даних показників обладнання, тоді як клієнтський модуль відповідає за реалізацію користувацького інтерфейсу.

Таблиця 5.1

Вимоги для розробки програмного забезпечення для моніторингу виробництва харчових продуктів

Вимоги до ПЗ	Поставлене завдання
Функціональні	Відстеження постачання сировини та матеріалів для виробництва харчових продуктів. Моніторинг усіх процесів виробництва, включаючи температуру, тиск, часові параметри тощо. Контроль якості продукції, включаючи вимірювання параметрів якості та відповідність стандартам. Автоматизований аналіз даних для виявлення аномалій та відхилень в процесі виробництва. Відстеження партій продукції та можливість виведення інформації про виробництво конкретної партії.

Вимоги до ПЗ	Поставлене завдання
Технічні	Вибір технологій та платформи розробки, що відповідають потребам галузі та забезпечують ефективну роботу системи. Інтеграція з існуючими системами виробництва та обробки даних. Забезпечення високої доступності та надійності системи для запобігання відмовам та втратам даних.
Безпекові	Захист конфіденційності даних про процеси виробництва та продукцію. Захист від несанкціонованого доступу до системи та можливість ведення журналів подій. Захист від атак і загроз, які можуть вплинути на безпеку та якість продукції.
Зручність користування	Розробка інтерфейсу, який спрощує роботу користувачів та забезпечує їхню можливість швидко та ефективно користуватися системою. Підтримка навчання та підтримки користувачів.
Документація	Розробка документації, яка описує функціональні можливості, інструкції користувача та технічну документацію для системи.
Відповідність нормативам та стандартам	Забезпечення, що система відповідає всім вимогам галузевих стандартів і нормативів, таких як HACCP, ISO 22000

Вибір мови програмування

При виборі мови програмування для реалізації серверної частини програми, були поставлені наступні вимоги:

- Підтримка неблокуючого паралельного виконання програми.
- Наявність жорсткої типізації.
- Наявність бібліотек для розробки серверних додатків.
- Активність користувацького співтовариства цієї мови програмування.
- Можливість використання об'єктно-орієнтованого підходу.

Вибір мови програмування, яка відповідає цим критеріям, дозволитьрозробити прототип програмного продукту в найкоротший термін.

Python

Обрання мови програмування для реалізації серверної частини програми є критичним завданням, і мова Python відповідає багатьом вимогам, які були поставлені. Ось основні переваги Python для реалізації серверноної частини програми:

1. **Інтерпретованість:** Python є інтерпретованою мовою програмування, що означає, що ви можете розробляти і тестувати програми без необхідності компіляції. Це полегшує та прискорює процес відлагодження.
2. **Кросплатформеність:** Python підтримується на багатьох популярних платформах, включаючи Windows, Linux та macOS, що робить його ідеальним вибором для розробки кросплатформеного програмного забезпечення.

3. **Об'єктно-орієнтованість:** Python базується на об'єктно-орієнтованому програмуванні, що дозволяє зручно використовувати об'єктно-орієнтований підхід під час розробки програм.

4. **Інтегровність та розширюваність:** За допомогою багатьох сторонніх модулів, доступних на Python Package Index (PyPI), Python може інтегруватися з іншими платформами та мовами програмування з легкістю.

5. **Відкритість вихідного коду:** Python - це вільно розповсюджувана мова, і її сирцевий код доступний у відкритому доступі, що сприяє гнучкості та розвитку спільноти.

6. **Багата стандартна бібліотека:** Python має розширену стандартну бібліотеку, яка містить багато корисних модулів і функцій для полегшення розробки програм.

7. **Доступність сервісів та фреймворків:** Існує велика кількість фреймворків і сервісів для розробки серверних додатків на Python, такі як Django, Flask, і багато інших.

8. **Спільнота користувачів та джерела інформації:** Python має велику та активну спільноту користувачів, що дозволяє легко знаходити інформацію та відповіді на будь-які питання стосовно розробки на цій мові.

Вибір мови Python для розробки серверної частини програми дозволить розробити прототип програмного забезпечення в найкоротший термін, використовуючи багато переваг цієї мови програмування [20].

C#

C# - це строго типізована об'єктно-орієнтована мова програмування, розроблена компанією Microsoft, і спрямована на роботу з платформою .NET.

.NET - це кросплатформене середовище з відкритим вихідним кодом, яке дозволяє розробляти різноманітні застосунки.

Основні переваги мови C# включають:

- Об'єктна орієнтованість: C# надає інструменти для зручної реалізації об'єктно-орієнтованого програмування.
- Статична типізація: Мова використовує статичну типізацію, що дозволяє мінімізувати помилки, пов'язані з типами даних.
- Багата стандартна бібліотека: C# має велику кількість вбудованих модулів та компонентів.
- Збирач сміття: Мова підтримує автоматичне управління пам'яттю завдяки збирачу сміття (garbage collector).
- Велика спільнота розробників: C# має активну спільноту розробників, що дозволяє отримувати підтримку та ресурси для розвитку.

Платформа ASP.NET Core, розроблена також компанією Microsoft, використовується для створення веб-додатків. Особливістю ASP.NET Core є її кросплатформеність, оскільки вона може працювати як на операційних системах Windows, так і на Unix-подібних системах, таких як macOS і Linux.

У цьому розділі ми провели аналіз популярних мов програмування і розглянули технології та інструменти для розробки серверної частини веб-додатків.

На основі цього аналізу ми прийняли рішення обрати мову програмування C# для реалізації серверної частини програмного забезпечення. Ця мова відповідає всім вимогам, які були визначені, і не має відомих недоліків у

порівнянні з іншими розглянутими мовами. Результати дослідження внесено до таблиці 5.2

	Python	C#
Неблокуючий паралелізм виконання програми	+	+
Жорстка типізація	-	+
Об’єктноорієнтованість	+	+
Бібліотеки для розробки серверних додатків	+	+
Активна спільнота розробників	+	+

При виборі технології для розроблення клієнтської частини було враховано наступні вимоги:

- Структурованість: Технологія повинна надавати можливість створення структурованих і організованих клієнтських додатків.
- Реалізація MVC: Технологія повинна підтримувати патерн Model-View-Controller (MVC), що дозволить ефективно розділити логіку додатку.
- Вичерпна кількість стандартних модулів та/або бібліотек: Вибрана технологія повинна мати багатий набір стандартних модулів і бібліотек для полегшення розробки.
- Компонентний підхід до архітектури: Технологія має підтримувати компонентний підхід до створення клієнтських додатків.

Ці вимоги були враховані при виборі технології для розроблення клієнтської частини.

React

React є JavaScript-бібліотекою, спрямованою на створення швидких, простих та масштабованих користувацьких інтерфейсів для односторінкових та мобільних додатків. Основні характеристики React включають:

- Використання віртуального DOM: Зміни відразу ж відображаються в віртуальному DOM. Він порівнюється з поточним станом, і зміни в реальному DOM вносяться мінімальними операціями для покращення ефективності.
- Підтримка збірки у bundle та tree-shaking: Ця функція допомагає мінімізувати завантаження ресурсів для кінцевого користувача шляхом об'єднання і оптимізації файлів.
- Візуалізація на стороні сервера (SSR): SSR дозволяє рендерити клієнтську частину на сервері, що покращує продуктивність та індексацію.
- Використання мови JSX: JSX - це синтаксичний цукор JavaScript, який дозволяє швидко прототипувати динамічні веб-сторінки з використанням React.js.

Основні обмеження React включають:

- Відсутність реалізації MVC: React не включає реалізацію структури Model-View-Controller (MVC), і для її створення може знадобитися використання додаткових бібліотек.
- Погана документація: Швидкий розвиток React і велика кількість бібліотек можуть призвести до недостатньої документації та уроків.

- Часті оновлення: React постійно змінюється, і розробники повинні бути в курсі останніх змін [25].

Vue.js

Vue.js - це JavaScript-фреймворк з відкритим вихідним кодом для побудови веб-інтерфейсів. Цей фреймворк є одним із найновіших серед розглянутих і стрімко набирає популярність. Основні характеристики Vue.js включають:

- Використання віртуального DOM: Vue є дуже продуктивним інструментом.
- Простота використання: Vue легко вивчати, що робить його привабливим як для початківців, так і для досвідчених розробників.
- Чудова документація: Vue має високоякісну документацію, що полегшує розробку.
- Проста інтеграція проєкту: Vue можна швидко впровадити в ваш проєкт.

Основні обмеження Vue.js включають:

- Мала спільнота: На відміну від React або Angular, Vue має меншу спільноту, і це може призвести до обмеженого обсягу доступних ресурсів.
- Обмежена інтеграція з мовою програмування TypeScript: Інтеграція Vue.js з TypeScript може бути менш прямою, порівняно з іншими фреймворками [26].

Після проведеного аналізу та порівняння основних технологій розробки користувацького інтерфейсу, було прийнято рішення вибрати React.js. Основні чинники, що вплинули на цей вибір, включають легкість навчання та високу продуктивність, порівняно з альтернативним фреймворком Vue.js. Результати було внесено до таблиці 5.3.

Таблиця 5.3

Порівняння технологій для розроблення клієнтської частини

	React	Vue.js
Структурованість	+	+
Реалізація MVC	-	-
Вичерпна кількість стандартних модулів та/або бібліотек	+	-
Компонентний підхід до архітектури	+	+

Результатом цього процесу є спеціалізована система моніторингу та відстежеиня, яка дозволяє контролювати процеси виробництва харчових продуктів в режимі реального часу, а також аналізувати дані для виявлення ризиків і покращення якості продукції.

5.2 Функції та можливості програмного забезпечення

Програмне забезпечення для забезпечення безпеки та якості харчових продуктів через цифрову трансформацію включає різноманітні функції та можливості, які допомагають покращити процеси контролю та моніторингу на

підприємствах харчової промисловості. До основних функцій цього програмного забезпечення належать:

Моніторинг параметрів виробництва: Програмне забезпечення здатне відстежувати різні параметри виробництва, такі як температура, вологість, тиск, час та інші. Це дозволяє операторам в режимі реального часу спостерігати за усіма аспектами виробництва та вчасно реагувати на будь-які аномалії.

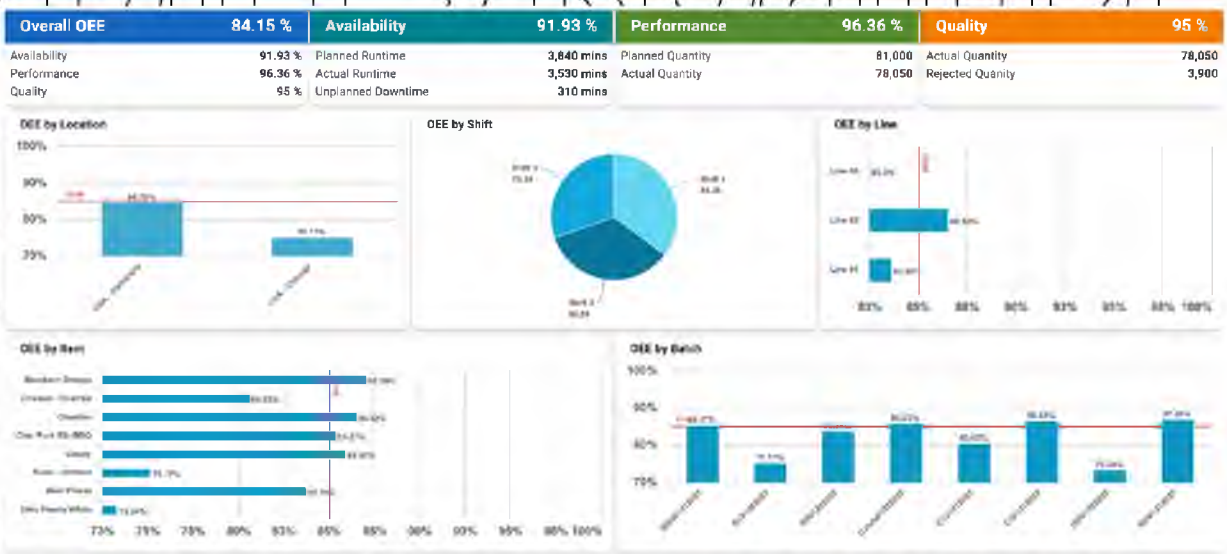

Рисунок 5.1 Приклад користувацького інтерфейсу для моніторингу параметрів виробництва

Аналіз даних та виявлення аномалій: Програмне забезпечення проводить аналіз накопичених даних і може виявляти аномалії або незвичайні зміни в параметрах виробництва. Наприклад, воно може автоматично виявити відхилення від заданих стандартів безпеки та якості продукції.

Ось докладніше, як ця система працює:

- Збір даних: Програмне забезпечення здійснює збір даних з різних джерел у виробничому процесі. Це може включати в себе датчики для вимірювання температури, тиску, вологості, часових параметрів і багато інших показників.

- Збереження даних: Зібрані дані зазвичай зберігаються в централізованій базі даних, де їх можна легко аналізувати та використовувати для подальших операцій.
- Аналіз даних: Програмне забезпечення використовує різні аналітичні методи та алгоритми для виявлення аномалій. Це може включати в себе порівняння поточних даних з історичними даними, побудову статистичних моделей або використання машинного навчання.
- Виявлення аномалій: Якщо програмне забезпечення виявляє будь-які відхилення або незвичайні зміни в параметрах виробництва, воно може сповістити операторів або автоматично вжити певні заходи для вирішення проблеми. Наприклад, воно може вимкнути обладнання, що працює з порушеннями безпеки або змінити параметри процесу для виправлення якості продукції.
- Запис журналу подій: Програмне забезпечення також може вести журнал подій, де фіксується інформація про виявлені аномалії, прийняті заходи та інші події, що стосуються безпеки та якості продукції. Це корисно для подальшого аудиту та аналізу.

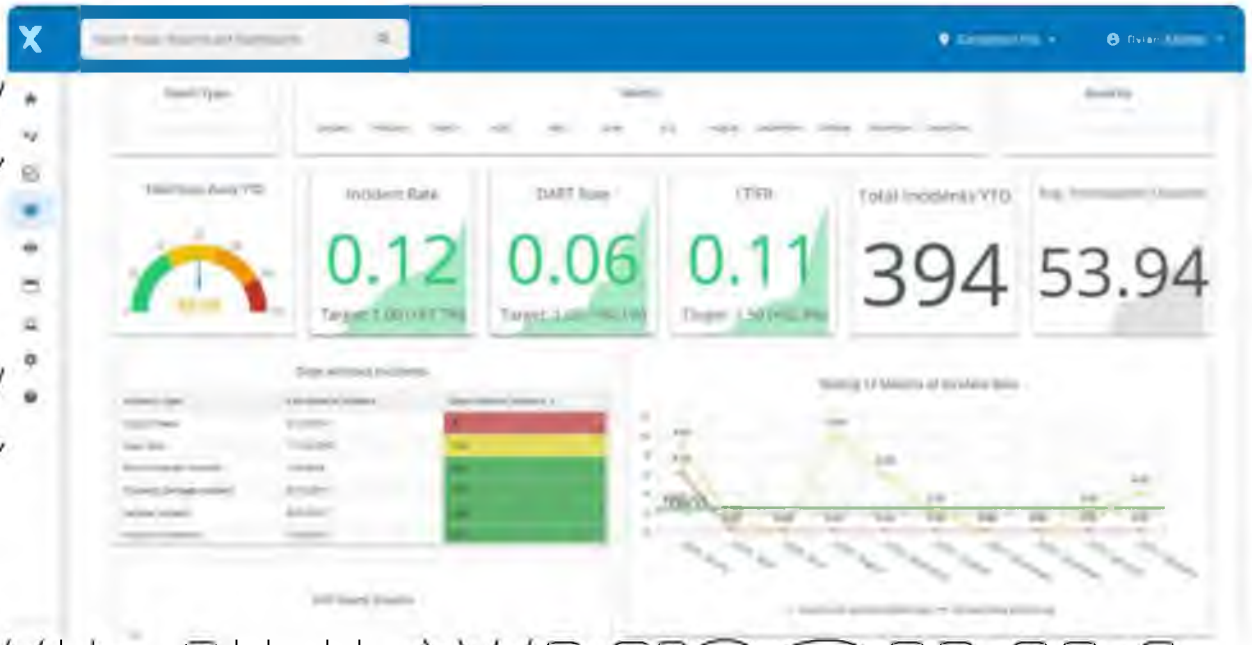

Рисунок 5.2 Сторінка перегляду аналітики показників

У результаті використання такого програмного забезпечення підприємство може досягти вищого рівня безпеки виробництва та якості продукції, а також зменшити ризики та витрати, пов'язані з незапланованими відмовами та відхиленнями. Приклад сторінки перегляду аналітики вказано на рисунку 5.2.

Запис та зберігання даних: Система забезпечує збір та зберігання всіх даних про виробництво та якість продукції в електронному вигляді. Це дозволяє зберігати історію виробництва та швидко визначити в разі необхідності. Також дане ПЗ включає в себе модуль для відстеження постачальників та якості сировини. Це дозволяє перевіряти якість і походження сировини, що використовується в виробництві харчових продуктів. В разі виявлення серйозних аномалій або відхилень від стандартів, програмне забезпечення може надсилати автоматичні сповіщення операторам або навіть запускати автоматичні заходи для виправлення ситуації.

Забезпечення дотримання нормативів і стандартів: Програмне забезпечення може допомагати підприємствам дотримуватися вимог стандартів та регулювань щодо безпеки та якості харчових продуктів.

Ця програмна система стає невід'ємною частиною цифрової трансформації підприємств харчової промисловості, допомагаючи підвищити якість продукції, забезпечити безпеку їжі та ефективно контролювати виробничі процеси. Вона сприяє покращенню реакції на потенційні ризики та забезпечує впровадження цифрових рішень для досягнення високих стандартів безпеки та якості харчових продуктів.

5.3 Висновки до розділу 5

У цьому розділі була розглянута розробка спеціалізованого програмного забезпечення для моніторингу та відстеження виробництва харчових продуктів. Перед розробкою програмного продукту був проведений аналіз вимог, який включав в себе функціональні, технічні, безпекові, вимоги до зручності користування, документаційні вимоги та вимоги до відповідності нормативам та стандартам.

Спеціалізоване програмне забезпечення для моніторингу та відстеження виробництва харчових продуктів розроблено на основі архітектури клієнт-сервер та складається з серверної та клієнтської частин. Серверна частина відповідає за взаємодію з базою даних та іншими ресурсами, виконання аналізу даних та забезпечення безпеки, тоді як клієнтська частина надає користувачам зручний інтерфейс для взаємодії з системою.

При виборі мови програмування для реалізації серверної частини програмного забезпечення була обрана мова C#, яка відповідала всім технічним вимогам та надавала можливість реалізації неблокуючого паралельного виконання.

Для клієнтської частини було обрано React.js, оскільки цей фреймворк надавав легкість навчання та високу продуктивність, порівняно з конкуруючим Vue.js.

Результатом цього етапу розробки є спеціалізована система, яка дозволяє виробникам харчових продуктів моніторити та відстежувати процеси виробництва в режимі реального часу, виявляти аномалії та ризики, а також покращувати якість та безпеку продукції. Вибір оптимальних технологій та підходів до розробки дозволив створити ефективну та функціональну систему, яка відповідає всім вимогам та стандартам галузі безпеки та якості продукції.

Були представлені функції та можливості програмного забезпечення, спрямованого на забезпечення безпеки та якості харчових продуктів через цифрову трансформацію виробничих процесів.

Основні функції програмного забезпечення включають:

- Моніторинг параметрів виробництва: Програмне забезпечення дозволяє в режимі реального часу спостерігати за різними параметрами виробництва, такими як температура, вологість, тиск тощо.
- Аналіз даних та виявлення аномалій: Система здатна аналізувати дані і виявляти аномалії або незвичайні зміни в параметрах виробництва, допомагаючи операторам реагувати на будь-які відхилення від стандартів.
- Запис та зберігання даних: Програмне забезпечення забезпечує збір та зберігання всіх даних про виробництво та якість продукції, що дозволяє вести історію виробництва і виявляти несправності у виробничому процесі.

- Забезпечення дотримання нормативів і стандартів: Система допомагає підприємствам дотримуватися вимог стандартів та регулювань щодо безпеки та якості харчових продуктів.

Ця програмна система стає ключовою складовою цифрової трансформації підприємств харчової промисловості, допомагаючи підвищити якість продукції, забезпечити безпеку харчових продуктів та ефективно контролювати виробничі процеси. Вона дозволяє підприємствам зменшити ризики та витрати, пов'язані з незапланованими відмовами та відхиленнями виробництва, та забезпечити дотримання всіх необхідних стандартів та нормативів. Таким чином, програмне забезпечення допомагає забезпечити якість та безпеку харчових продуктів на підприємствах харчової промисловості.

РОЗДІЛ 6: ТРЕНІНГ І НАВЧАННЯ ПЕРСОНАЛУ

7.1. Розробка програми навчання та підготовки персоналу

У цьому розділі описано процес розробки навчальної програми для навчання користувачів нашого ПЗ. Навчання є важливою частиною впровадження будь-якого нового програмного продукту, оскільки воно допомагає користувачам розібратися з інтерфейсом, функціоналом та іншими аспектами додатка. У цьому розділі буде розглянуто весь процес розробки навчальної програми, включаючи визначення цілей, адаптацію для цільової аудиторії, розробку навчального контенту та інші ключові аспекти.

Програма навчання та підготовки персоналу для впровадження цифрових систем управління безпечністю харчових продуктів є критично важливою для забезпечення успішного переходу до цифрового управління та збереження високого стандарту безпеки та якості продукції. Ця програма повинна бути ретельно розроблена і враховувати основні аспекти навчання та підготовки персоналу.

Оцінка потреб: Першим кроком є оцінка потреб у навчанні. Це включає в себе визначення, який персонал буде працювати з цифровими системами, і які саме аспекти цифрового управління їм необхідно освоїти. Наприклад, це може бути технічний персонал, менеджери, які відповідають за моніторинг процесів, або робітники, що проводять контроль якості.

Розробка модулів навчання

На основі потреб персоналу розробляються модулі навчання для кожної категорії працівників. Кожен модуль повинен включати в себе такі ключові елементи:

Модуль 1. Основи цифрового управління

Ціль: Вивчити основні принципи цифрового управління та зрозуміти, як ваше програмне забезпечення допомагає в цьому процесі.

1.1. Теоретичний матеріал:

- Визначення цифрового управління.
- Роль та відповідальності персоналу у цифровому управлінні.
- Огляд ключових функцій та можливостей вашого програмного забезпечення.

1.2. Практичні навички:

- Встановлення та налаштування програмного забезпечення.
- Ознайомлення з інтерфейсом та основними опціями.
- Виконання простих завдань у програмі.

1.3. Контрольні завдання:

- Тестування на засвоєння теоретичного матеріалу та навичок.

Модуль 2. Технічне навчання

Ціль: Навчити технічний персонал робити більше технічно орієнтовану роботу у вашому програмному забезпеченні.

2.1. Теоретичний матеріал:

- Огляд технічних аспектів вашого програмного забезпечення.
- Робота з апаратурою та програмними інструментами, які використовуються для моніторингу та автоматизації процесів.

2.2. Практичні навички:

- Робота з технічними компонентами програмного забезпечення.
- Вирішення технічних завдань та виправлення недоладок.

2.3. Контрольні завдання:

- Тестування на засвоєння теоретичного матеріалу та навичок.

Модуль 3: Спеціальні навички

Ціль: Навчити персонал специфічних навичок, які можуть бути необхідні для певних завдань чи індивідуальних ролей.

3.1. Теоретичний матеріал:

- Специфічні вимоги та завдання, які вимагають особливих навичок.

3.2. Практичні навички:

- Практичне навчання виконання завдань, що вимагають спеціалізованих навичок.

3.3. Контрольні завдання:

- Оцінка професійних навичок та вмінь у виконанні спеціальних завдань.

Модуль 4: Система оцінки та підтримки

Ціль: Переконатися, що персонал реально засвоїв матеріал та готовий до роботи з вашим програмним забезпеченням.

4.1. Система оцінки:

- Встановлення процедур оцінки успішності навчання.
- Визначення критеріїв успіху.

4.2. Підтримка:

- Можливість звертання за підтримкою під час навчання.
- Додаткові ресурси та матеріали для підтримки.

Модуль 5: Навчання в практичних умовах

Ціль: Навчити персонал працювати з програмним забезпеченням в реальних виробничих умовах.

5.1. Практичні вправи:

- Відтворення реальних виробничих процесів на навчальному обладнанні.
- Робота під наглядом інструкторів

Залучення експертів: Для ефективного навчання персоналу важливо залучити експертів у галузі цифрових систем управління безпечністю харчових продуктів або здійснити партнерство зі спеціалізованими навчальними закладами.

Ця програма навчання та підготовки персоналу гарантує, що всі співробітники мають необхідну компетенцію для ефективної роботи з цифровими системами управління безпечністю харчових продуктів. Вона також сприяє забезпеченню високого стандарту безпеки та якості продукції.

6.2 Важливість навчання та підготовки персоналу для впровадження цифрових систем управління

Персонал відіграє критичну роль у процесі цифрової трансформації та забезпеченні безпеки та якості харчових продуктів через впровадження цифрових систем. Нижче подано докладніше про важливість цього аспекту:

Збільшення свідомості: Важливо забезпечити, що персонал повністю розуміє переваги та важливість цифрових систем управління безпечністю харчових продуктів. Це включає в себе усвідомлення того, як ці системи

допомагають виявляти ризики, забезпечувати відповідність стандартам безпеки та якості та покращувати продуктивність.

Розвиток навичок і компетентностей: Персонал повинен бути наділений необхідними навичками та компетентностями для використання цифрових систем. Це включає в себе навички роботи з програмним забезпеченням, інтерфейсами, сенсорами, технологіями IoT тощо. Компетентний персонал може забезпечити ефективну експлуатацію систем та надійний контроль параметрів виробництва.

Усвідомлення ролі в безпеці та якості продукції: Персонал повинен розуміти свою роль у забезпеченні безпеки та якості харчових продуктів. Це включає в себе правильну обробку продуктів, забезпечення відповідності стандартам гігієни та безпеки, а також реагування на аномалії та ризики.

Забезпечення відповідності стандартам та регуляторним вимогам: Персонал повинен бути наділений знаннями щодо стандартів безпеки та якості харчових продуктів, а також регуляторних вимог. Вони повинні дотримуватися цих вимог та впроваджувати їх у щоденну практику.

Підготовка до виявлення аномалій та реагування на них: Персонал повинен бути навчений виявляти аномалії в процесах виробництва, параметрах якості продукції та безпеці. Вони також повинні знати, як реагувати на ці аномалії, вживаючи необхідні кроки для запобігання ризиків та виправлення проблем.

Важливість змін в організаційній культурі: Перехід до цифрових систем може вимагати змін в організаційній культурі, включаючи підвищену відкритість до інновацій та навчання, а також збільшену відповідальність за якість та безпеку продукції.

Постійне навчання та оновлення: Цифрові технології швидко розвиваються, тому персонал повинен мати можливість постійного навчання та оновлення своїх знань. Це може включати в себе участь у тренінгах, вебінарах, онлайн-курсах та інших формах навчання.

Важливо враховувати, що успішна цифрова трансформація вимагає не лише інвестицій у технології, але й інвестицій у навчання та підготовку персоналу. Компетентний та добре підготовлений персонал є ключовим фактором для забезпечення безпеки та якості харчових продуктів у цифровому середовищі.

6.3 Висновки до розділу 6

У висновку можна відзначити, що розробка модулів навчання для персоналу важлива для ефективного впровадження цифрових систем управління безпечністю харчових продуктів. Кожен модуль навчання має включати в себе теоретичний матеріал, практичні навички та контрольні завдання, щоб забезпечити повноцінне засвоєння матеріалу та розвиток необхідних компетенцій.

Важливо, що навчання не обмежується лише технічними аспектами, але також враховує специфічні вимоги та завдання, які можуть виникати для певних категорій працівників. Система оцінки та підтримки допомагає переконатися, що персонал дійсно засвоїв матеріал та готовий до роботи з цифровими системами управління.

Залучення експертів та постійне навчання є важливими компонентами успішного навчання персоналу. В організаційній культурі також слід розвивати відкритість до інновацій та відповідальність за якість та безпеку продукції.

Враховуючи вищезазначені аспекти, навчання та підготовка персоналу гарантують не лише впровадження цифрових систем управління, але і забезпечення високого стандарту безпеки та якості харчових продуктів.

РОЗДІЛ 7. РЕКОМЕНДАЦІЇ ЩОДО УПРАВЛІННЯ РИЗИКАМИ ТА ВДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕЧНІСТЮ ХАРЧОВИХ ПРОДУКТІВ

Як було показано у попередніх розділах, цифрові технології та інновації відіграють важливу роль у забезпеченні безпечності та якості харчових продуктів, а також у вдосконаленні управління ризиками на підприємствах харчової промисловості.

В цьому розділі ми розглянемо конкретні рекомендації та підходи, які допоможуть підприємствам ефективно управляти ризиками та підвищити безпеку та якість своєї продукції в умовах цифрової трансформації. Дослідження та аналіз, представлені в цьому розділі, стануть корисними як для фахівців у галузі безпечності харчових продуктів, так і для керівників підприємств, що прагнуть покращити свої практики управління ризиками та забезпечити високий стандарт безпечності та якості своєї продукції.

Впровадження інтегрованих систем управління

У контексті цифрової трансформації підприємства рекомендується впроваджувати інтегровані системи управління, які об'єднують управління якістю та безпечністю харчових продуктів з управлінням ризиками. Ця інтеграція дозволяє компанії визначити потенційні ризики та розробити стратегії їх управління. Інтегровані системи дозволяють спростити процес впровадження нових цифрових технологій та забезпечують єдність підходів у системі управління.

Стандартизація та впровадження найкращих практик

Однією з ключових рекомендацій є стандартизація процесів управління якістю та безпечністю харчових продуктів в умовах цифрової трансформації. Розробка і впровадження стандартів та найкращих практик допомагають

спростити процес впровадження нових технологій та забезпечують використання ефективних методів управління безпечністю.

Стратегічне партнерство з технологічними компаніями

Для успішної цифрової трансформації рекомендується розробити стратегічне партнерство з компаніями, що постачають цифрові технології та рішення для галузі безпечності харчових продуктів. Ці партнери можуть мати досвід у розробці та впровадженні цифрових рішень для підприємств харчової промисловості.

Аналіз та вдосконалення поточних процесів

Для досягнення високих стандартів безпечності та якості харчових продуктів, рекомендується систематично аналізувати та вдосконалювати поточні процеси управління безпечністю харчових продуктів. Важливо виявляти слабкі місця та проводити їхнє подальше вдосконалення.

Оцінка та забезпечення кібербезпеки

З огляду на зростаючі загрози кібербезпеці, рекомендується розробити та впровадити стратегії для захисту від кіберзагроз, які можуть вплинути на безпеку харчових продуктів. Забезпечення кібербезпеки стає надзвичайно важливим аспектом в контексті цифрової трансформації.

Освіта та навчання персоналу

Розробка програми навчання та підготовки персоналу є надзвичайно важливою рекомендацією. Програма має охоплювати всі аспекти цифрової трансформації та управління ризиками у сфері безпечності харчових продуктів. Персонал повинен отримувати постійне навчання та перепідготовку для успішного впровадження цифрових систем управління.

Моніторинг та аналіз результатів

Рекомендація полягає впровадженні систем моніторингу та аналізу результатів цифрового управління. Це допомагає підприємству постійно вдосконалювати процеси та стратегії, забезпечуючи безпеку та якість харчових продуктів на високому рівні.

Співробітництво з регуляторами та експертами

Пошук і збереження партнерських стосунків з регуляторними органами та експертами у сфері безпечності харчових продуктів є ключовим чинником успіху в управлінні ризиками. Залучення висококваліфікованих фахівців може сприяти розробці більш дієвих стратегій управління ризиками та допомагати вирішувати ефективно проблеми, пов'язані з безпечністю та якістю харчових продуктів.

Моніторинг новітніх цифрових розробок

Для постійного оновлення та впровадження новітніх цифрових технологій рекомендується активно вивчати та моніторити ринок цифрових розробок у сфері безпечності харчових продуктів. Це дозволить підприємству завжди бути на крок попереду та використовувати передові рішення для управління ризиками.

Внутрішні аудити та регулярна оцінка

Важливим елементом управління ризиками є проведення внутрішніх аудитів та регулярна оцінка виконання стратегій та програм у сфері безпечності харчових продуктів. Це допомагає виявляти можливі недоліки та прогалини в системі управління та негайно вживати відповідні заходи.

Інновації та постійне вдосконалення

Останнім, але найважливішим елементом є постійні інновації та вдосконалення системи управління ризиками. Світ цифрових технологій постійно змінюється, тому підприємство повинно бути готовим до адаптації та

вдосконалення стратегій та процесів управління безпечностю та якістю харчових продуктів.

Усі ці рекомендації спрямовані на створення високоефективної системи управління ризиками та безпечністю харчових продуктів в умовах цифрової трансформації. Вони допоможуть підприємству досягти високих стандартів безпечності та якості своєї продукції та забезпечити конкурентну перевагу на ринку харчових продуктів.

ВИСНОВКИ

Ця дипломна робота досліджувала сучасні підходи до управління безпечністю харчових продуктів в умовах цифрової трансформації харчової промисловості. В ході дослідження були розглянуті потенційні ризики та виклики, пов'язані з впровадженням цифрових технологій у цей сектор, а також їх вплив на якість та безпеку харчових продуктів. Досліджено практичні дослідження впровадження цифрових рішень у компаніях і в конкретних регіонах, порівняно результати цифрових систем з традиційними методами та оцінено їхню ефективність у забезпеченні безпеки харчових продуктів.

У результаті аналізу існуючих систем управління були виявлені проблеми та слабкі місця, які можуть призвести до загроз для безпеки та якості продукції. Для вирішення цих проблем було розроблено та впроваджено цифрові інструменти та технології, спеціалізове програмне забезпечення для моніторингу та автоматизованого контролю процесів виробництва. Вони дозволили не лише підвищити рівень безпеки та якості продукції, але й покращити управління ризиками виробництва.

Однак важливо враховувати, що впровадження цифрових систем вимагає підготовки та навчання персоналу. Розроблена програма навчання та підготовки персоналу є ключовим елементом успішної цифрової трансформації підприємств у сфері харчової промисловості. Правильно підготовлений персонал здатен ефективно впроваджувати та використовувати цифрові інструменти для досягнення найвищих стандартів безпеки та якості.

Загальним результатом цієї роботи є набір рекомендацій щодо управління ризиками та вдосконалення системи управління безпечністю харчових продуктів в умовах цифрової трансформації. Ці рекомендації можуть бути корисними для підприємств та фахівців у галузі безпечності харчових продуктів, які прагнуть

покращити свої практики та досягти високих стандартів безпеки та якості у цьому важливому секторі господарства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Офіційний сайт ISO 22000: ISO 22000 Системи менеджменту безпеки харчової продукції [Електронний ресурс]. – Режим доступу: https://www.iso.org/ru/iso-22000-food-safety-management.html
2. М. Хараламбус Впровадження систем управління безпечністю харчових продуктів на малих підприємствах на Кіпрі: Дослідницький архів репозиторію тез - 2011, с. 53
3. Duret et al (2017) Quantitative risk assessment of norovirus transmission in food establishments: evaluating the impact of intervention strategies and food employee behavior on the risk associated with norovirus in foods. Risk Anal 37:1–27
4. Food Safety Mag. June/July. See: https://www.foodsafetymagazine.com/magazine-archive1/junejuly-2019/the-need-for-a-glove-use-management-system-in-retail-foodservice/
5. https://www.techtitute.com/pdf/nutrition/postgraduate-certificate/quality-management-system-digitalization-food-industry
6. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: Проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018. №1. С.75-86.
7. The Global Risks Report 2021. WEF. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (дата звернення 10.12.2021)
8. BM Security. Cost of a Data Breach Report. 2020. URL:https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
9. Bronk Ch. Hacking the Nation-State: Security, Information Technology and Policies of Assurance. Information Security Journal: A Global Perspective. 2008. Vol.17, № 3. pp.132-142.
10. basedsecurity.com/2021/12/06/data-breach-quickview-november-2021/
11. Створення глобальної культури кібербезпеки. Резолюція ГА ООН №57/239 від 20 грудня 2001 р. URL: https://undocs.org/ru/A/RES/57/239
12. Fritze, M. P., Eisingerich, A. B., & Benkenstein, M. (2019). Digital transformation and possession attachment: examining the endowment effect for consumers' relationships with hedonic and utilitarian digital service technologies. Electronic Commerce Research, 19(2), 311–337.
13. https://doi.org/10.1007/s10660-018-9309-8 Furr, N., & Shipilov, A. (2019).
14. Digital Doesn't Have to Be Disruptive The best results can come from adaptation rather Than reinvention. Harvard Business Review, 94–104.
15. https://cases.media/article/cikava-statistika-ta-fakti-pro-internet-rechei-iot-rozmir-rinku-vikoristannya-ta-prognozi

16. https://aws.amazon.com/partners/success/?partner-case-studies-cards.sort-by=item.additionalFields.sortDate&partner-case-studies-cards.sort-order=desc&awsf.partner-case-studies-filter-audience=*all&awsf.partner-case-studies-filter-content-type=*all&awsf.partner-case-studies-filters-locations=*all&awsf.partner-case-studies-filter-industry=*all&awsf.partner-case-studies-filter-use-case=*all&awsf.partner-case-studies-filter-partner-type=*all
17. https://www.nestle.ua/
18. International Journal of Information Management, Volume 63, April 2022, 102466
19. https://smartfoodsafe.com/digital-environment-for-food-safety-inspections/ https://www.researchgate.net/publication/342596828_Digital_Technology_to_Enable_Food_Safety_Management_Systems
20. What is Python: [Електронний ресурс]. – Режим доступу до ресурсу: https://www.pythonforbeginners.com/learn-python/what-is-python/
21. Best Programming Language to Learn in 2020 (for Job & Future): [Електронний ресурс]. — Режим доступу: https://hackr.io/blog/bestprogramming-languages-to-learn-2020-jobs-future
22. Advantages and Disadvantages of Python Programming Language [Електронний ресурс]. — Режим доступу: https://medium.com/@mindfiresolutions.usa/advantages-anddisadvantagesof-python-programming-language-fd0b394f2121/
23. The Python Package Index (PyPI) [Електронний ресурс]. — Режим доступу: https://docs.python.org/3/distutils/packageindex.html
24. TypeScript [Електронний ресурс]. — Режим доступу: https://www.typescriptlang.org/
25. React [Електронний ресурс]. — Режим доступу: https://reactjs.org/
26. Vue.js [Електронний ресурс]. — Режим доступу: https://vuejs.org/
27. Строгая типизация для приложений Vue.js на TypeScript [Електроний ресурс] — Режим доступу: https://habr.com/ru/post/351216/
28. GitLab CI/CD [Електронний ресурс]. — Режим доступу: https://docs.gitlab.com/ee/ci/
29. https://smartfoodsafe.com/digital-environment-for-food-safety-inspections/
30. https://www.netafim.com.ua/digital-farming
31. https://sistema.bio/blog/q3-2023-sistema-bio-news/
32. Remote monitoring and alerting for iot [електронний ресурс]. – 2020. – режим доступу до ресурсу: https://cloud.google.com/solutions/remote-monitoring-andalerting-for-iot.
33. Петін В. А. Arduino и raspberry pi в проектах internet of things / Віктор А. Петин. – санкт-петербург: «бхв-петербург», 2018. – 432 с.

34. Интернет вещей, iot, m2m мировой рынок [електронний ресурс]. – 2020. - режим доступу до ресурсу: https://www.tadviser.ru/index.php/статья:интернет_вещей,_iot,_m2m_(мировой_рынок)
35. Howling Pixel. Інтернет речей [Електронний ресурс] / Howling Pixel //
36. Інтернет речей URL: https://howlingpixel.com/i-uk/Інтернет_речей
37. IT Strategy Headquarters. «E-Japan Strategy» January 22, 2001 URL: https://japan.kantei.go.jp/it/network/0122full_e.html
38. https://intercert.com.ua/newsnews-of-standartization/667-iso-22000-2018-new-standart
39. Україну чекає "революція" з інтернетом і зв'язком: що зміниться //електрон. текст. дані URL:https://www.obozrevatel.com/ukr/tech/5g-v-ukraini-perevagi-ta-terminivvedennya.htm
40. Шаповал М.І. Менеджмент якості. Київ : Центр учбової літератури, 2005. 256 с.
41. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7374378/
42. Webpack- https://en.wikipedia.org/wiki/Webpack
43. Міжнародний стандарт ISO 22000:2018. Система менеджменту харчової безпеки. Вимоги до будь-якої організації, яка бере участь у ланцюзі створення харчової продукції. Для навчальних цілей / Переклад здійснений спеціалістами громадської організації «СФЕРО». 51 с. URL : https://sfero.org.ua/wp-content/uploads/2020/04/ISO-22000-2018-2_sfero.pdf