КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

Факультет інформаційних технологій

Кафедра інформаційних систем та технологій

Спеціальність 126 – Інформаційних систем та технологій,
програма «Програмні технології інтернет речей»

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему:

«Інформаційно-аналітична модель розумного агро страхування на основі даних з IoT»

Студента 2-го курсу групи ІРма-2

Хом'як Анастасії
(ім'я, прізвище)

(підпис студента)

Науковий керівник:

Доктор технічних наук, доцент
(науковий ступінь, вчене звання)

Олексій Колесніков
(ім'я, прізвище)

(дата) *(підпис)*

Попередній захист:

(Висновок: "До захисту в Державній екзаменаційній комісії")

В.о. завідувача кафедри
інформаційних систем
та технологій

(підпис) *(прізвище, ініціали)* *(дата)*

Київ – 2021

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет інформаційних технологій

Кафедра Інформаційних систем та технологій
Освітньо-кваліфікаційний рівень Магістр
Спеціальність 126 – Інформаційних систем та технологій
Програма «Програмні технології інтернет речей»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
д.т.н., доцент О. Колесніков
_____
"____" _____20___року

З А В Д А Н Н Я
НА ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Студент ___Анастасія ХОМ'ЯК___
Група _____ІРма-2_____

1. **Тема кваліфікаційної роботи** «Інформаційно-аналітична модель розумного агро страхування на основі даних з IoT».
Затверджена протоколом засідання кафедри ІСТ №16/20 від «09» листопада 2020 р.
2. **Строк подання студентом готової роботи** – «20» травня 2021 р.
3. **Цільова установка та вихідні дані до роботи.**

Дослідження в області агро страхування. Програмно-апаратні рішення для оптимізації процесів інтернет речей при агрострахуванні. Дані стану існуючих систем агрострахування.

4. **Зміст роботи**

Постановка задачі та аналіз існуючих рішень. Аналіз існуючих моделей агрострахування. Постановка задачі магістерської роботи.

Розробка архітектури проекту IoT-рішення. Обґрунтування вибору інтелектуальних кінцевих точок IoT. Комунікаційні технології та системи. Хмарні, туманні та граничні обчислення. Методи та засоби обробки даних.

Розробка функціональної схеми. Розробка функціональної системи агрострахування. Розробка електричної принципової схем системи IoT-рішення. Розробка функції моніторингу та сповіщення.

Розробка алгоритму системи агрострахування на основі даних з IoT. Обґрунтування вибору хмарного рішення. Обґрунтування вибору хмарних сервісів та їх налаштування. Аналіз захищеності інформації та методів і способів (протоколів) для її кіберзахисту. Прогнозування економічного ефекту впровадження системи розумного агрострахування.

5. **Перелік графічного матеріалу (слайдів)**

Функціональна схема IoT-рішення. Електрична принципова схема IoT-рішення. Блок-схема алгоритму системи агрострахування на основі даних з IoT.

6. **Календарний план виконання роботи:**

№ з/п	Назва частин роботи	Дати виконання роботи за планом
1.	Аналіз літератури та джерел	до 20.10.2020
2.	Вивчення літературних джерел з предмету дослідження	до 08.11.2020
3.	Збір і вивчення матеріалів досліджуваного об'єкта (підприємства)	до 08.12.2020
4.	Складання розгорнутого плану кваліфікаційної роботи	до 16.12.2020
5.	Ознайомлення наукового керівника з розгорнутим планом кваліфікаційної роботи. Внесення змін.	24.12.2020
6.	Підготовка розділу 1	20.01.2021
7.	Підготовка розділу 2	19.02.2021
8.	Підготовка розділу 3	05.03.2021
9.	Підготовка розділу 4	19.03.2021
10.	Оформлення кваліфікаційної роботи	05.04.2021
11.	Передача кваліфікаційної роботи рецензенту для рецензування	до 14.05.2021
12.	Передача кваліфікаційної роботи науковому керівникові	до 11.05.2021
13.	Попередній захист кваліфікаційної роботи	20.04.2021
14.		
15.		
16.		
17.		

Дата видачі завдання "____" _____ 2021р.

Керівник роботи доцент, Олексій Колесніков
(посада, ім'я, прізвище)

_____
(підпис)

Завдання прийняв до виконання студент групи ІРма-2

Хом'як Анастасія
(ім'я, прізвище)

_____
(підпис)

АНОТАЦІЯ

Тема роботи: «Інформаційно-аналітична модель розумного агро страхування на основі даних з IoT».

Метою кваліфікаційної роботи магістра – є дослідження методів та засобів побудови інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

Об'єкт дослідження. Об'єктом дослідження магістерської роботи виступає технологія Інтернет речей.

Предмет дослідження. Предметом дослідження є розробка інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

Наукова новизна одержаних результатів. Розроблене комплексне рішення для комплексного моніторингу приміщень за допомогою технології Інтернет речей. Розроблена інформаційно-аналітична модель розумного агро страхування на основі даних з IoT.

Методи дослідження. Методологічну основу складають наступні методи наукового пізнання: індукція, дедукція, методи термодинаміки, математичної статистики, програмування.

Практичне значення одержаних результатів. Розроблена інформаційно-аналітична модель розумного агро страхування на основі даних з IoT може бути впроваджена на базі реального підприємства.

Апробація результатів. Основні положення і результати досліджень, викладені у проекті, пройшли апробацію на VI Міжнародній науково-практичній конференції (Київ, 2020) [6], на VII Всеукраїнській науково-практичній конференції молодих науковців у 2020 році [7], на IV Всеукраїнській науково-практичній інтернет конференція студентів та аспірантів «Теоретичні та прикладні аспекти розробки комп'ютерних систем» [5] та на 87 International scientific conference of young scientist and students «Youth scientific achievements to the 21st century nutrition problem solution» [4] (in National University of Food Technologies, Kyiv, 2021).

Кваліфікаційна робота магістра складається зі змісту, вступу, основної частини, яка включає чотири розділи, висновки та списку використаних джерел. Всього 103 сторінки.

КЛЮЧОВІ СЛОВА: IoT, хмарні технології, хмарні сервіси IoT, агрострахування, протокол.

ВЛАСНІ ПУБЛІКАЦІЇ:

1. O. Kolesnikov, A. Biloshchytskyi, V. Gogunskii, A. Khomiak, DEVELOPMENT OF A MARKOV MODEL OF THE INFORMATION ENVIRONMENT AS A COMMUNICATION SYSTEM IN THE SCIENTIFIC SPHERE Scientific Journal of Astana IT University ISSN (P): 2707-9031 ISSN (E): 2707-904X

2. О.Є. Колесніков, А.О. Хом’як, Розумне агрострахування на основі даних з IoT як інструмент управління ризиками. XVII міжнародна науково-технічна конференція, 2021 р.

3. О.Є. Колесніков, А.О. Хом’як Аналіз архітектурних рішень іот-систем УДК 002.6:004

ABSTRACT

Work topic: **"Information-analytical model of smart agro insurance based on IoT data".**

The purpose of the master's qualification work is to study the methods and means of building an information-analytical model of smart agro-insurance based on IoT data.

Object of study. The object of study of the master's thesis is the technology of the Internet of Things.

Subject of study. The subject of the research is the development of an information-analytical model of smart agro insurance based on IoT data.

Scientific novelty of the obtained results. Developed a comprehensive solution for integrated monitoring of premises using the technology of the Internet of Things. An information-analytical model of smart agro-insurance based on IoT data has been developed.

Research methods. The methodological basis is the following methods of scientific knowledge: induction, deduction, methods of thermodynamics, mathematical statistics, programming.

The practical significance of the obtained results. The developed information-analytical model of smart agro insurance based on IoT data can be implemented on the basis of a real enterprise.

Approbation of results. The main provisions and research results presented in the project were tested at the VI International Scientific and Practical Conference (Kyiv, 2020) [6], at the VII All-Ukrainian Scientific and Practical Conference of Young Scientists in 2020 [7], at the IV All-Ukrainian Scientific and Practical Conference. Internet conference of students and graduate students "Theoretical and applied aspects of computer systems development" [5] and at the 87th International scientific conference of young scientist and students "Youth scientific achievements to the 21st century nutrition problem solution" [4] (in National University of Food Technologies, Kyiv, 2021).

The master's qualification work consists of the content, introduction, main part, which includes four sections, conclusions and a list of sources used. A total of 103 pages.

KEY WORDS: IoT, cloud technologies, IoT cloud services, agricultural insurance, protocol.

Зміст

ВСТУП

Актуальність теми. У світі зростає кількість «підключених» пристроїв (за оцінками галузевих аналітиків, їх кількість досягне 20-50 млрд одиниць до 2022 р. І разом з ним - кількість прикладів застосування «Інтернету речей» (Internet of Things, IoT) в економіці: енергетиці, промисловості, житлово-комунальному господарстві, сільському господарстві, транспорті, охороні здоров'я та ін.

У зарубіжній практиці відомі успішні приклади впровадження IoT з ініціативи як держави, так і бізнесу. Наприклад, за підтримки держави в країнах Євросоюзу, Південній Кореї, Китаї та Індії впроваджуються технології «розумного міста», які дозволяють підвищувати ефективність управління енергоспоживанням і транспортними потоками. У Великобританії і США реалізовані масштабні програми з впровадження «розумних лічильників» для віддаленого контролю енергоспоживання в домогосподарствах.

Бізнесу IoT дозволяє отримати конкурентну перевагу за рахунок зниження витрат і розвитку нових джерел доходу. Наприклад, американська компанія GE Aviation виробляє авіадвигуни, на яких встановлені сенсори, що дозволяють віддалено отримувати дані про експлуатацію і на їх основі виявляти оптимальні алгоритми обслуговування літаків, що дозволило в сім разів скоротити витрати на обслуговування.

Промислові IoT-технології лежать в основі «Індустрії 4.0»: за оцінками Німецької академії науки і техніки, їх впровадження підвищить продуктивність німецьких промислових підприємств на 30% на горизонті до 2025 р. Споживчий ринок все більше заповнюють «розумні» технології: наприклад, за результатами опитування PwC в США, пристрій з технологією «розумного будинку» використовує кожен четвертий споживач. «Інтернет речей» стає реальністю.

Постійний обмін даними вимагає розвитку нових сервісів, які повинні з'єднати нас з фізичним світом навколо. Ці сервіси також повинні бути побудовані на повністю нових бізнес-моделях і забезпечити нові фінансові потоки.

За допомогою «Інтернету речей» взаємодія об'єктів, середовища і людей буде багато в чому переплетена, що обіцяє зробити світ «розумним» - більш упорядкованим для людини.

Мета і завдання дослідження. Метою роботи є дослідження методів та засобів побудови інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

Для досягнення поставленої мети вирішуються наступні задачі:

– запропонувати призначення термінології і область застосування;

– навести технічні характеристики інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.;

– провести огляд існуючих рішень і обґрунтування вибору структури інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.;

– розробити та описати структурну та функціональну схеми проектованої інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.;

– здійснити вибір і обґрунтування окремих вузлів інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.;

– розробити і описати принципову схему та алгоритм керуючої програми;

– дослідити інформаційно-аналітичну модель розумного агро страхування на основі даних з IoT.

Об’єкт дослідження – технологія Інтернет речей.

Предмет дослідження – розробка інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

Методи дослідження. Методологічну основу складають наступні методи наукового пізнання: індукція, дедукція, методи термодинаміки, математичної статистики, програмування.

Наукова новизна отриманих результатів.

1) Розроблене комплексне рішення для комплексного моніторингу приміщень за допомогою технології Інтернет речей.

2) Розроблена інформаційно-аналітична модель розумного агро страхування на основі даних з IoT.

Практичне значення отриманих результатів. Розроблена інформаційно-аналітична модель розумного агро страхування на основі даних з IoT може бути впроваджена на базі реального підприємства.

Структура роботи. У своєму складі робота має: вступ, три розділи, висновки, перелік використаної літератури, з 32 літературних джерел. Загальний обсяг роботи становить 103 сторінки.

РОЗДІЛ 1. ПОСТАНОВКА ЗАДАЧІ ТА АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

1.1 Аналіз існуючих моделей агрострахування

Аграрне страхування як спосіб відшкодування ризиків в сільськогосподарському виробництві і, отже, стабілізації фінансової стійкості виробників сільськогосподарської продукції, в тій чи іншій формі використовувалося практично завжди. В останнє десятиліття все більше країн стали приділяти увагу управлінню ризиками в аграрному секторі та розвитку систем аграрного страхування.

Коло різних систем аграрного страхування досить широке. Вважається, що найбільш розвинені системи існують в США, Канаді та Іспанії. Наведемо короткий аналіз існуючих схем страхування за кордоном без опису технічних деталей.

По-перше, агрострахування в усіх країнах буває добровільним і обов'язковим. Обов'язкове страхування практикується лише в невеликій кількості країн. Далі, у агрострахуванні практично завжди бере участь держава, але форми участі різні. Як правило, це дві форми. Перша – коли держава частково бере участь в оплаті страхових премій, а друга – коли за рахунок держави частково компенсує втрати в разі реалізації тих чи інших ризиків. Остання форма держпідтримки поступово скорочується, оскільки її застосування суперечить правилам СОТ.

Далі, існує два види програм – програми страхування врожайності і програми страхування доходів, які гарантують компенсацію втрат виробника сільськогосподарської продукції не тільки від недобору врожаю, а й і від падіння цін на вироблену продукцію.

Як приклад зарубіжних програм страхування наведемо основні програми агрострахування в США.

Мультиризикове страхування врожаю

Ця програма є найдавнішою і найпопулярнішою програмою агрострахування, яка надає захист від падіння врожайності, викликаного цілим рядом ризиків. Для більшості культур ці ризики включають посуху.

перезволоження, заморозки і вимерзання, вітер, повінь, шкоду, завдану шкідниками і хворобами. Страховики можуть пропонувати страхування додаткових ризиків за додаткову плату. Прикладом додаткового страхування є страхування від граду, страхування від неможливості проведення посівних або збиральних робіт через несприятливі погодні умови.

Рівень покриття за даною програмою базується на середній врожайності кожного окремого господарства. Якщо отримана в господарстві врожайність культури менше гарантованої, то застрахованому господарству буде виплачена сума, якої не вистачає до гарантованого рівня.

Мультиризикове страхування є самим дорогим і складним, оскільки при даному виді страхування необхідно проводити моніторинг посівів і врегулювати збитки в кожному господарстві по кожному полю. У структурі тарифу на це йде приблизно 20-30% суми страхової премії.

Страхування доходу від вирощування культури

Існує кілька видів програм такого змісту. Опишемо найпоширенішу програму страхування доходу. Ця програма базується на середній врожайності кожного індивідуального сільськогосподарського виробника і захищає його від зниження доходу в результаті падіння врожайності і / або падіння цін на вироблену продукцію.

Дана страхова програма гарантує певний рівень доходу, який називається повною гарантією. Для розрахунку повної гарантії використовується ціна, яка є максимальною з двох цін – прогнозної весняної ціни на урожай (базової ціни) і осінньої ціни на момент збирання врожаю. Страхова ж премія розраховується виходячи з базової (весняної) ціни. Відшкодування виплачується тоді, коли отриманий дохід (обчислюється виходячи з осінньої ціни в період збирання врожаю) менше повної гарантії на всій застрахованої площі.

Страхування за індексом врожайності

Покриття втрат в цій програмі базується на показниках району, а не індивідуального господарства і виплата застрахованому господарству за цією

програмою здійснюється тоді, коли середня врожайність по району падає нижче гарантованого рівня врожайності.

Компенсація втрат провадиться в однаковому розмірі всім застрахованим господарствам. Конкретний фермер може не отримати компенсацію, якщо у нього врожайність низька, а середня врожайність по району вище гарантованого рівня. Дана програма не влаштовує прогресивні господарства, у яких врожайність найчастіше набагато вище середньої врожайності по району. Основними користувачами даної програми є дрібні і середні ферми а також початківці фермери. Страхові компанії пропонують таким клієнтам кілька років попрацювати за програмою індексу врожайності, після накопичення даних по виробництву даної культури клієнт може вибрати інші програми агрострахування

Страхування за індексом доходу

Це варіант попередньої програми, оскільки базується вона на показниках району, а не на показниках окремого господарства.

За даною програмою клієнти отримують виплату, якщо середньорічний дохід всіх господарств в районі знижується через падіння врожайності і / або ціни на продукцію. Ця програма більш популярна в порівнянні з програмою, заснованою на індексі врожайності. Зауважимо, що і за цією програмою фермер може не отримати компенсацію. якщо показник індексу доходу не були нижче певного рівня.

У деяких країнах індекс врожайності використовується в якості страхування сільгоспвиробників від катастрофічних ризиків і таким чином здійснюється перехід від виплат після катастроф до класичного страхування.

Фахівці відзначають, що програми страхування доходів з виробництва окремих культур і страхування доходів всього сільськогосподарського підприємства найбільш популярні у фермерів.

Структура всіх зібраних страхових премій в США розподіляється наступним чином:

за програмами страхування доходів збирається 60% всіх премій; за програмами страхування врожаю - 20%; за програмами індексу доходу - 10%; за програмами індексу врожайності - 3%.

Решта 7% страхових зборів становлять страхові премії від спеціальних програм з федеральним субсидуванням за окремими видами культур, фруктів, овочів.

Страхування за індексами погоди

Проблемним моментом програм страхування за індексом врожайності і індексу доходу є необхідність отримання офіційних даних від статистичних органів країни, що становить (В США) приблизно 4-6 місяців або навіть більше.

Подібні складності дозволяє обійти страхування за індексами погоди. Дана концепція ґрунтується на тому, що для деяких культур можна спрогнозувати вплив деяких погодних ризиків. Прикладами застосування індексу погоди є страхування фруктових насаджень від вимерзання взимку, від заморозків навесні, страхування якості винограду за сумою ефективних температур. Обґрунтовано страхуються зернові у фазу наливу колоса від посухи і в період збирання від надлишкових опадів.

Виплата страхувальникам за програмами погодного індексу страхування проводиться в мінімальні терміни. Після закінчення договору страхування страхова компанія повинна звернутися в гідрометеорологічну службу і при фіксуванні страхового випадку виплачує відшкодування через 30-45 днів. При цьому огляд посівів культур за даними страхових продуктів не проводиться.

Агрострахування в Іспанії

На думку багатьох фахівців найбільш прийнятною для України може стати модель іспанської системи страхування. З цієї причини наведемо тут основні її положення:

- страхування аграрних ризиків є добровільним;
- покриття ризиків забезпечують приватні страхові компанії на основі солідарної відповідальності;

- держава підтримує, контролює, і розвиває систему агрострахування, виділяє субсидії на страхування, здійснює перестрахування всередині країни;
- сільськогосподарські виробники через свої об'єднання беруть активну участь у прийнятті рішень з питань агрострахування;
- система виключає необхідність надання прямої державної підтримки в разі настання катастрофічних ризиків;
- правила агрострахування закріплені законодавчо і, що важливо, не змінюються.

Аграрному виробнику пропонуються наступні програми страхування:

Індивідуальне страхування від названих ризиків (для кожної культури і для кожного ризику). Інтегральне страхування, що забезпечує покриття всіх погодних несприятливих умов (мультиризик). Для розрахунку тарифів використовуються середні показники по району. Страхування від усіх ризиків, що відрізняється від попереднього тим, що для розрахунку тарифів береться середня врожайність по господарству. Індексне страхування (індекс погоди). Цей вид страхування тільки розвивається. Страхування тваринництва, бджільництва.

Агрострахування на Україні

В останній період перед розпадом СРСР – роками в країні існувала обов'язкова форма страхування в сільськогосподарському виробництві. Існувала одна монопольна страхова організація Держбуд, яка в обов'язковому порядку за своїми правилами страхувала колгоспи і радгоспи по частині культур і частини природних ризиків.

Після розпаду СРСР з 1991 року на території України існує добровільна форма страхування врожаю. У наступний період перерозподілу власності, в тому числі і власності на землю, система страхування врожаю практично не діяла, однак в даний час страхова система в сільському господарстві знаходиться в стадії активного становлення. У правлячих колах дозріло розуміння того, що страхова система є невід'ємною частиною аграрно-

промислового комплексу (АПК) і без неї вирішити проблеми розвитку АПК - одного з пріоритетних напрямків розвитку країни, неможливо. Дозріло також розуміння, що без державної підтримки будь-яка схема страхування в сільському господарстві України, де близько 90% земель є зонами ризикованого землеробства, неможливо.

В даний час існує багато страхових компаній, бажаючих займатися страхуванням в сільському господарстві.

Резюмуючи багато аналітичних роботи з агрострахування, можна перерахувати найбільш важливі проблеми сучасного сільськогосподарського страхування:

1. Відсутність чітких цілей і стратегії розвитку страхування в цій галузі. Зокрема, немає чіткого уявлення про способи участі держави, не визначені навіть види сільськогосподарського страхування. Зазвичай під цим терміном розуміється тільки страхування врожаю, хоча, як показує зарубіжний досвід, страхування доходу вельми популярне серед аграріїв.

2. Недоліки чинного законодавства, оскільки саме існуючі нормативні документи криють в собі всі перераховані вище недоліки.

3. Недосконаліть методичної бази. Зокрема, проблемними є:

- неоптимальні, а точніше, необґрунтовані страхові тарифи;
- вузький перелік культур, що страхуються;
- недосконаліть оцінки впливу випадкових погодних факторів на врожайність;

4. Проблеми фінансово-економічного характеру, що стримують розвиток агрострахування:

важке фінансове становище сільськогосподарських підприємств і, як наслідок, неможливість здійснювати страхування в повному обсязі. Можливо, в даній ситуації може допомогти більш гнучка страхова тарифна політика; відсутність доступу до кредитування для оплати страхових внесків; недостатній розвиток перестрахувального ринку.

Треба сподіватися, що з дозволом перерахованих проблем економічна ефективність страхування на Україні зросте, що дозволить, в свою чергу, прискорити вирішення поставленого завдання розвитку АПК країни.

Організація вітчизняного ринку агрострахування на основі технологій аналізу даних не перший рік залишається предметом дискусій галузевого співтовариства. У той же час концентрація експертної аудиторії на оперативно-технічних деталях і нормативно-законодавчої софістиці обертається ефектом «за деревами не видно лісу», бо загальна концепція рішення виглядає в кращому випадку констатацією недосліджених проблем, що гальмують розвиток всього напряму. Хоча відомої фактури більш ніж достатньо для синтезу цілісної бізнес-платформи «розумного страхування» з урахуванням сучасних можливостей і реальних умов.

Актуальність впровадження «розумного страхування» на Україні забезпечується не тільки появою і поширенням безпрецедентних ІТ-технологій для максимальної автоматизації управління страховими ризиками та операційними процесами. Соціально-економічні фактори роблять ще більший вплив на стан ринку за рахунок швидкого збільшення приватних агропідприємств країни. Стійка тенденція зростання неминуче супроводжується посиленням матеріальних загроз через загальне зниження рівня безпеки і культури учасників агроринку, особливо в непростих умовах економічної чи політичної кризи.

«Гонка озброєнь» страхового бізнесу представляє лише реакцію на первинні загрози його рентабельності, особливо при спостережуваному подорожчання послуг навіть обов'язкового агрострахування. До їх парирування залучаються передові навігаційні, геоінформаційні та інформаційно-аналітичні технології з використанням всіляких каналів і методів збору, передачі, зберігання, обробки і аналізу різнорідних даних з будь-яких типів джерел. ГЛОНАСС і тут з успіхом знаходить своє застосування поряд зі своїми наземними прикладними сегментами, такими, як Інтелектуальні системи і Безпечне місто.

Всі області цифровізації АПК (рис. 1.1) мають певний потенціал для застосування в агрострахування або можуть вплинути на ринок в майбутньому.

Рисунок 1.1. Області цифровізації АПК

Напрямки розвитку цифровізації у агрострахуванні на території України викликано наступними драйверами (рис. 1.2).

Рисунок 1.2. Драйвери впливу на розвиток цифровізації у агрострахуванні

Дієва система агрострахування базується у першу чергу на якісному моніторингу діяльності агропромислового підприємства.

На сьогодні, на ринку програмного забезпечення представлено широкий асортимент програм для забезпечення моніторингу комплексів аграрного призначення.

AGS – система моніторингу комплексом аграрного призначення

Функціональні можливості системи:

– контроль роботи сільгосптехніки в режимі реального часу;

– моніторинг місцеположення транспорту і сільгосптехніки, їх напрямку і швидкості руху;

– моніторинг траєкторії розташування транспорту і сільськогосподарської техніки в режимі on-line. Відображення інформації на електронній карті в режимі реального часу;

– моніторинг за дотриманням технологічної швидкості агрегатів при проведенні польових робіт;

– планування полів, збір інформації для складання паспорта поля, визначення чітких меж полів, вимірювання площі сільгоспугідь, картування врожайності (щільність врожаю та ін.);

– прокладання маршрутів, планування розкладу робіт і контроль його виконання. Виявлення несанкціонованих простоїв техніки з вини працівників;

– урахування кількості рейсів, пройденого кілометражу, робочого часу автомобілів і спецтехніки. Виявлення «приписок» в дорожніх листах;

– моніторинг знаходження об'єкта в межах позначеної ділянки (поля), час входу / виходу на об'єкт;

– моніторинг руху техніки по полю (якість обробки країв при посіві, обробці гербіцидами);

– формування і моніторинг дотримання маршруту руху: знаходження техніки в межах позначеного поля, проходження техніки перевозить зібраний урожай строго на місце розвантаження. Виявлення «лівих» рейсів;

– формування і моніторинг графіка роботи техніки на поле;

– окреслення несанкціонованих простоїв. Зниження кількості простоїв техніки з вини працівників;

– отримання диспетчером або керівником тривожного повідомлення про недотримання маршруту руху, графіка виконання робіт і інших позаштатних ситуаціях.

Головний оператор має можливість зі свого пульта управління дистанційно заблокувати двигун при виході техніки на інше поле або при спробі угону. Забезпечення збереження вантажів, контроль прибуття автомобіля на об'єкт розвантаження, формування інформації про точне місце вивантаження врожаю.

Cropio.

Програмне забезпечення Cropio (рис. 1.3) спрямована на оптимізацію добрива і зрошення ґрунту і таким чином знижується кількість використовуваних добрив і води. Cropio, разом з інформацією про погоду і

даними з супутника, також робить можливим контроль посівів і аналіз врожайності.

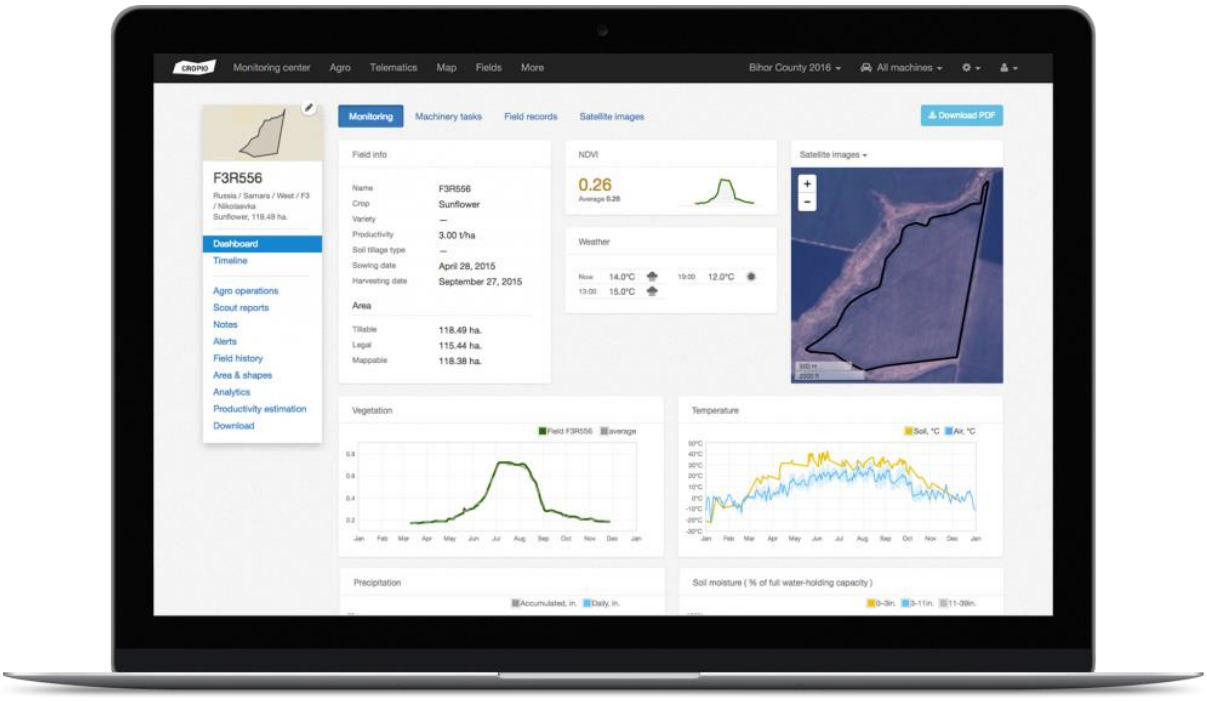


Рисунок 1.3. Програмне забезпечення контролю сільськогосподарських угідь

Cropio – це система дистанційного моніторингу сільськогосподарських угідь, яка включає оперативний контроль стану посівних площ, автодокументування, прогнозування і планування сільськогосподарських операцій.

Програмне забезпечення управління агропідприємством (рис. 1.4)

Програмне забезпечення веде облік активів, планування робіт, GPS-трекінг техніки, контроль вегетації – всі аспекти господарства зібрані в одному місці і доступні з будь-якого пристрою.

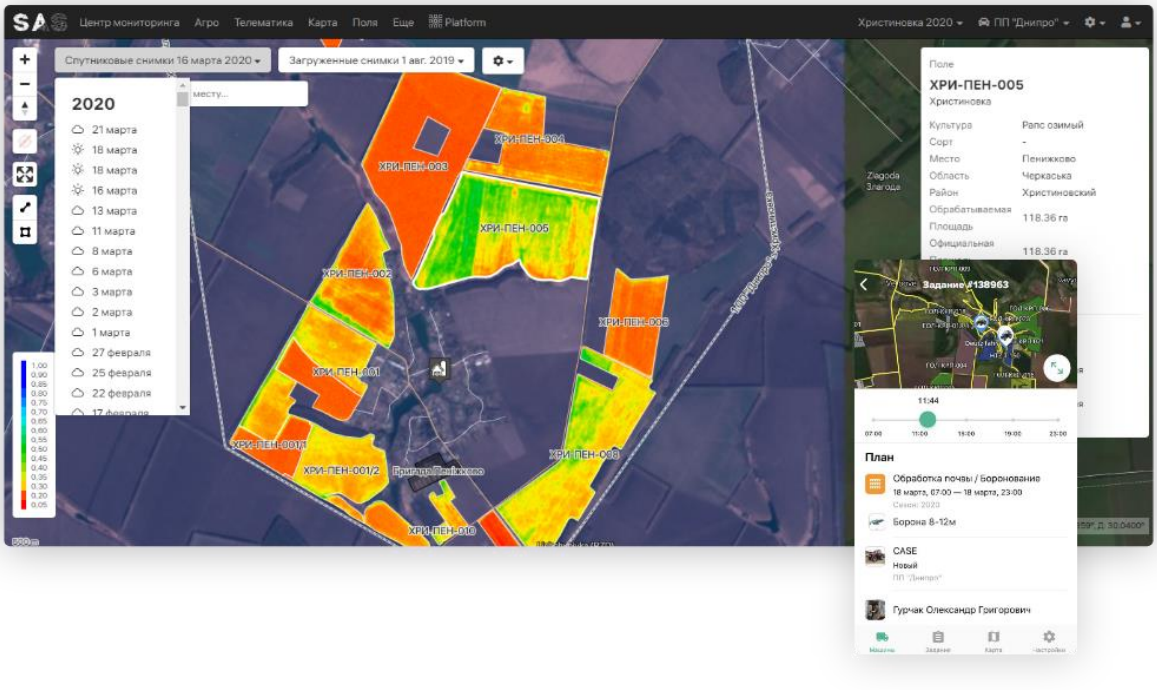


Рисунок 1.4. Програмне забезпечення управління агропідприємством

Програмне забезпечення управління агропідприємством має можливість структурувати та аналізувати супутникові знімки посівів, знаходити проблемні зони на полі. Програма дає прогноз врожайності культур, формуючи дані за поточний сезон та порівнюючи їх з минулим роком.

1.2 Постановка задачі магістерської роботи

Метою даної магістерського роботи є розробка інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

Головними завданнями виступають:

- обґрунтування вибору створення інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;
- розкриття методів та засобів обробки даних;
- розробка проекту IoT-рішення;
- розробка архітектури інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;
- визначення комунікаційний технології та систем;

– аналіз захищеності інформації та методів і способів (протоколів) для її кіберзахисту.

1.3 Висновки

Спостерігається тенденція зростання інвестицій в цифрові технології в страховій галузі. Зростає число стартапів. IT-технології трансформують страхову галузь. Залишаються проблеми, зокрема, в регуляторній сфері.

На сьогодні виникла необхідність формування принципово нової гнучкої нормативної бази для впровадження цифрових технологій в усі сфери життя, потрібно, щоб держава підтримувала компанії, які розробляють компетенції в сфері цифрових технологій, ті, які мають наскрізний галузевий ефект. Це обробка і аналіз великих масивів даних, штучний інтелект і нейротехнології.

Проте, нові IT-технології призводять до появи нових ризиків, до росту кіберризиків. Процес впровадження цифрових технологій в страхових компаніях призведе до скорочення персоналу, часткового заміщенню ряду традиційних професій і підвищення попиту на фахівців з іншими компетенціями, головним чином, в області інформаційних технологій, фахівців з моделювання, обробки та аналізу великих обсягів інформації, актуаріїв. У контексті економічної ефективності впровадження інноваційних інформаційних технологій залишається ще ряд питань і вимагається проведення додаткових наукових досліджень. Головний виграш від процесу діджиталізації отримають клієнти. Їх спілкування зі страховими організаціями обіцяє стати зручнішим, процес врегулювання збитків більш швидким і менш болючим, а персоніфіковані тарифи більш справедливими і привабливими.

РОЗДІЛ 2. РОЗРОБКА АРХІТЕКТУРИ ПРОЕКТУ ІОТ-РІШЕННЯ

2.1 Обґрунтування вибору інтелектуальних кінцевих точок IoT

Завдання інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT полягає у комплексному моніторингу роботи аграрного підприємства та можливості його страхування.

З урахуванням складності IoT має сенс створення архітектури, яка б специфіковані основні компоненти і їх взаємозв'язок. Архітектура IoT може надати такі переваги:

- дати адміністратора мережі або IT-менеджеру корисний контрольний список для оцінки функціональності і повноти пропозицій від різних постачальників;
- служити орієнтиром для розробників в плані того, які функції потрібні в IoT і як вони взаємодіють;
- служити основою для стандартизації, стимулюючи сумісність і скорочення витрат.

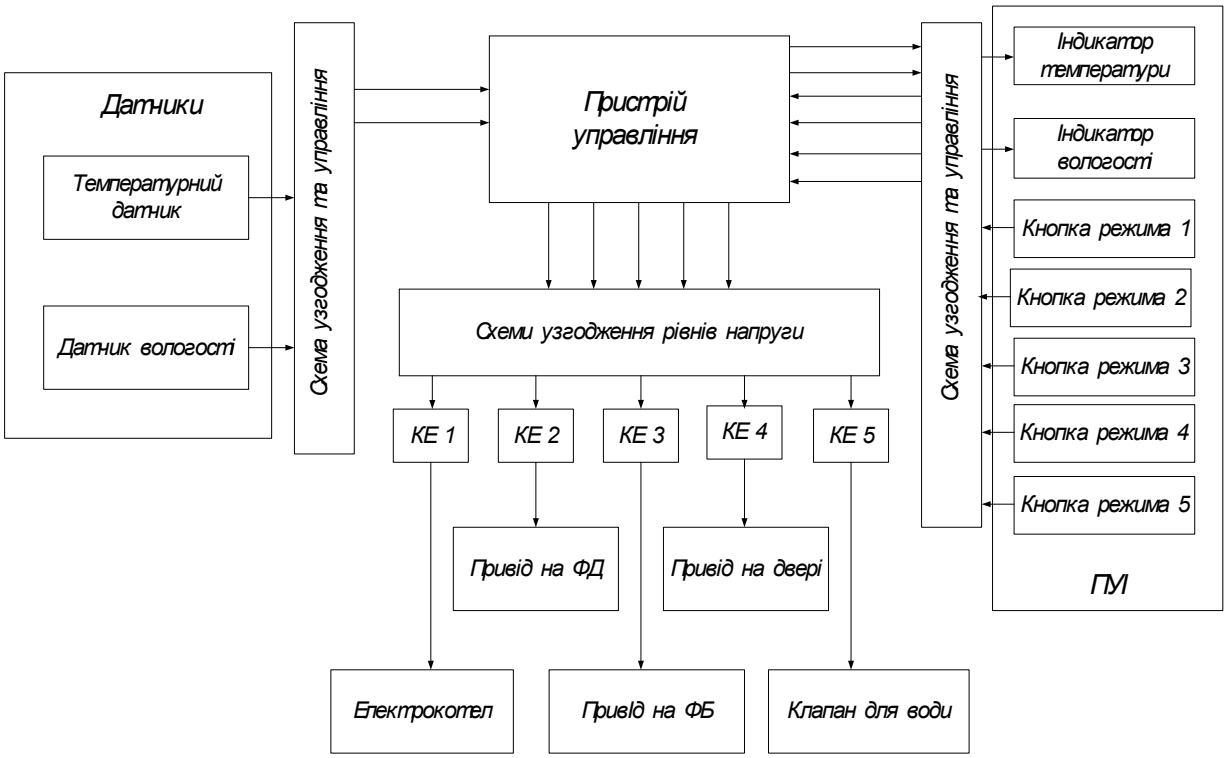
Наведемо огляд інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT, що розробляється.

На відміну від більшості інших моделей і архітектурних моделей, описаних в літературі, модель інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT деталізує фактичні фізичні компоненти екосистеми IoT. Це корисно, тому що висвічує елементи системи IoT, які повинні бути з'єднані, інтегровані, керовані і надані додаткам. Детальна специфікація системи описує вимоги до можливостей IoT.

Один з важливих аспектів, який загострює модель, - той факт, що IoT на ділі не є мережею фізичних речей. Це скоріше мережа пристроїв, що взаємодіє з фізичними речами, разом з прикладними платформами - такими як комп'ютери, планшети і смартфони, - які взаємодіють з цими пристроями.

2.2 Комунікаційні технології та системи

Структурна схема інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT представлена на рис. 2.1.



КЕ – ключовий елемент; ФБ – фрамуга бокова; ФД – фрамуга в даху; ПУІ – пульт управління та індикації

Рисунок 2.1. Структурна схема інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT

Схема взаємодії всіх складових інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT наведена на рис. 2.2

Рисунок 2.2. Схема взаємодії всіх складових інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT

Інтерфейс інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT наведено на рис. 2.3

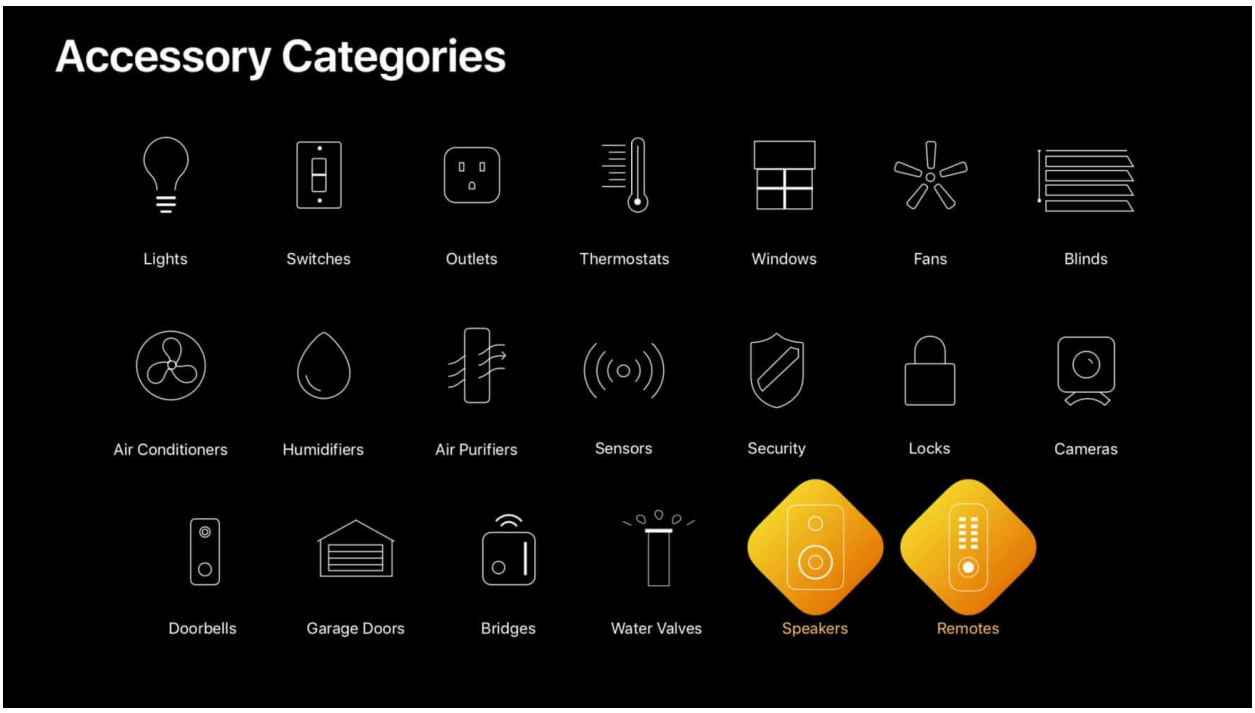


Рисунок 2.3. Інтерфейс інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT

Налаштування інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT

```
[self.homeManager addHomeWithName:@"My Home" completionHandler:^(HMHome *home, NSError *error) {
    if (error != nil) {
        // Failed to add a home
    } else {
        // Successfully added a home
    }
}];
```

```
NSString *roomName = @"Living Room";
[home addRoomWithName:roomName completionHandler:^(HMRoom *room, NSError *error) {
    if (error != nil) {
        // Failed to add a room to a home
    } else {
        // Successfully added a room to a home
    }
}];
```

Протокол делегатів управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT та додати властивості браузера до інтерфейсу класу.

```
@interface EditHomeViewController () <HMAccessoryBrowserDelegate>

@property HMAccessoryBrowser *accessoryBrowser;

@end
```

Здійснити налаштування інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

```
self.accessoryBrowser = [[HMAccessoryBrowser alloc] init];
self.accessoryBrowser.delegate = self;
```

знайти аксесуари управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

```
[self.accessoryBrowser startSearchingForNewAccessories];
```

Сформувати колекцію управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

```
- (void)accessoryBrowser:(HMAccessoryBrowser *)browser didFindNewAccessory:(HMAccessory *)accessory {
    // Update the UI per the new accessory; for example, reload a picker view.
    [self.accessoryPicker reloadAllComponents];
}
```

Послуги для аксесуарів інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT наведено на рис. 2.4.

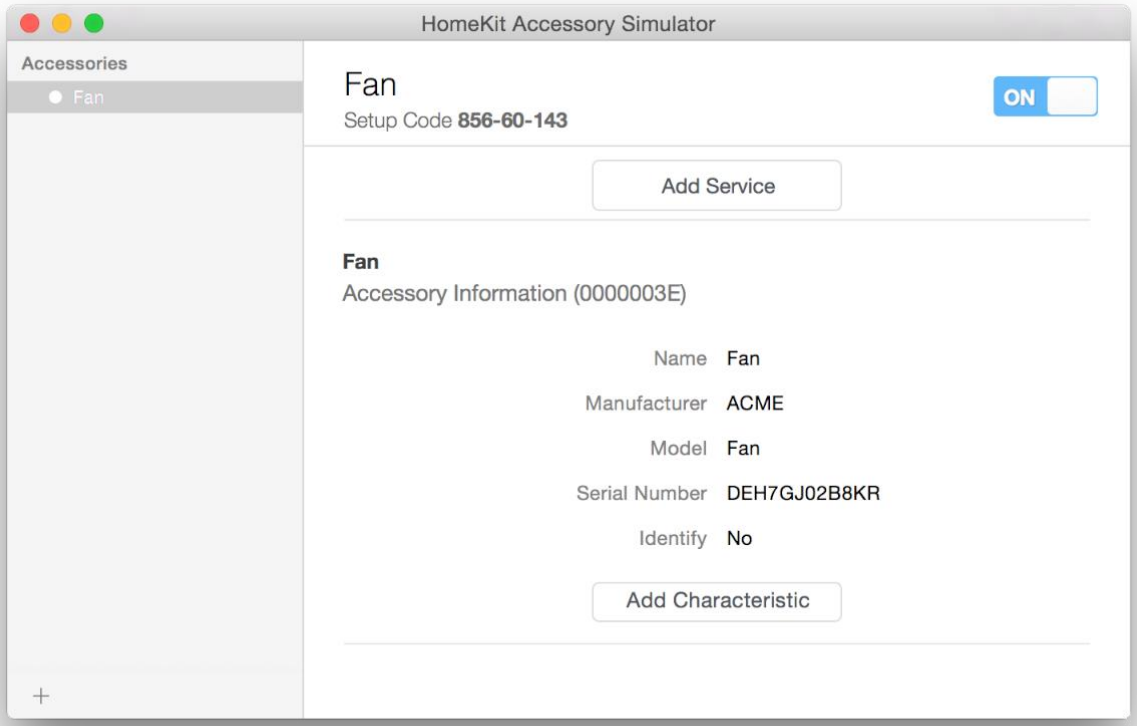


Рисунок 2.4. Послуги для аксесуарів інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT

Сформувати перехід до другої моделі управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT

```
- (void)viewWillDisappear:(BOOL)animated {
    [self.accessoryBrowser stopSearchingForNewAccessories];
}
```

Зупинити пошук аксесуарів інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

Характеристики аксесуарів системи розумного агро страхування на основі даних з IoT наведено на рис. 2.5.

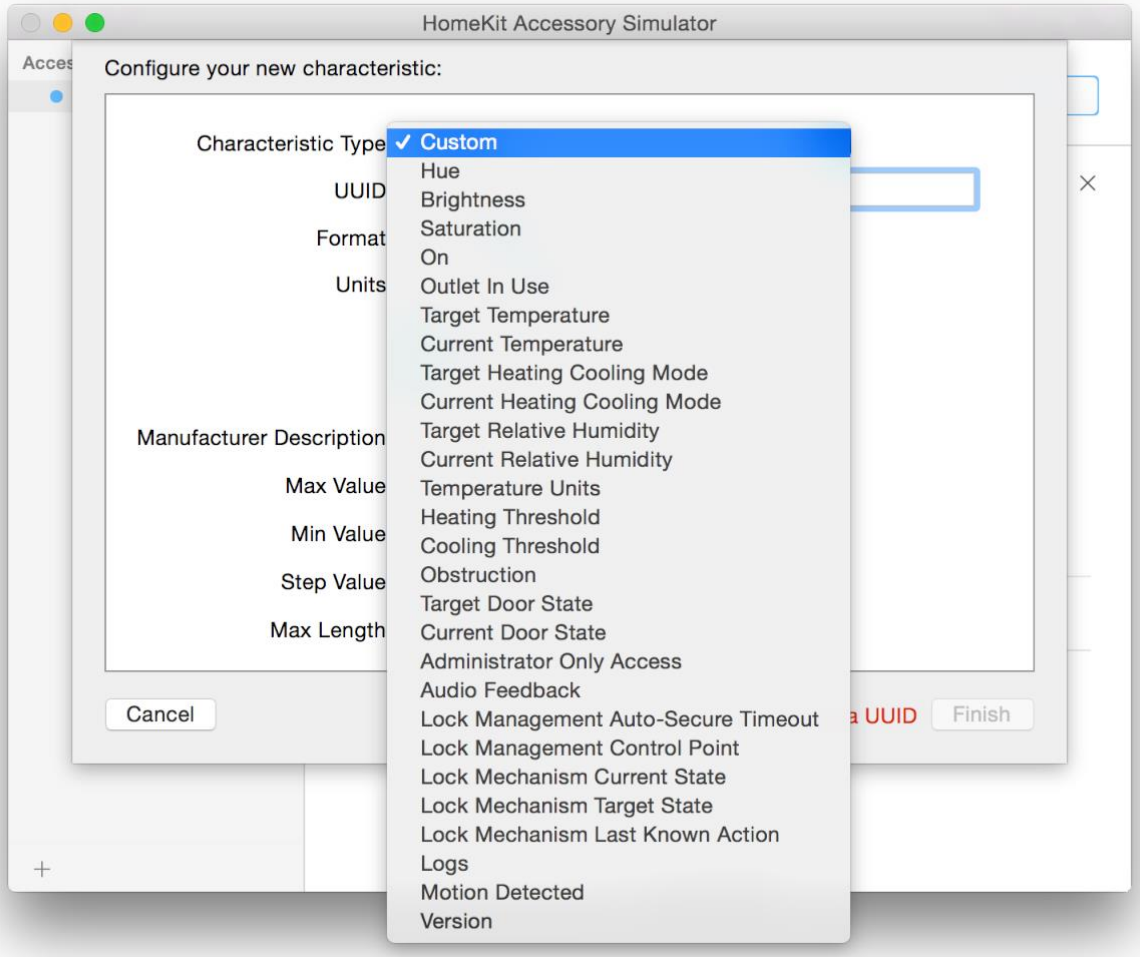


Рисунок 2.5. Характеристики аксесуарів системи розумного агро страхування на основі даних з IoT

Переваги створеної системи системи розумного агро страхування на основі даних з IoT:

– дозволяє здійснити моніторинг всієї системи розумного агрострахування з урахуванням розташування датчиків інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– відкрита гетерогенна архітектура управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– об'єднана розподілена база даних управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– інтерфейси між процесами управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– масштабовані рішення управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

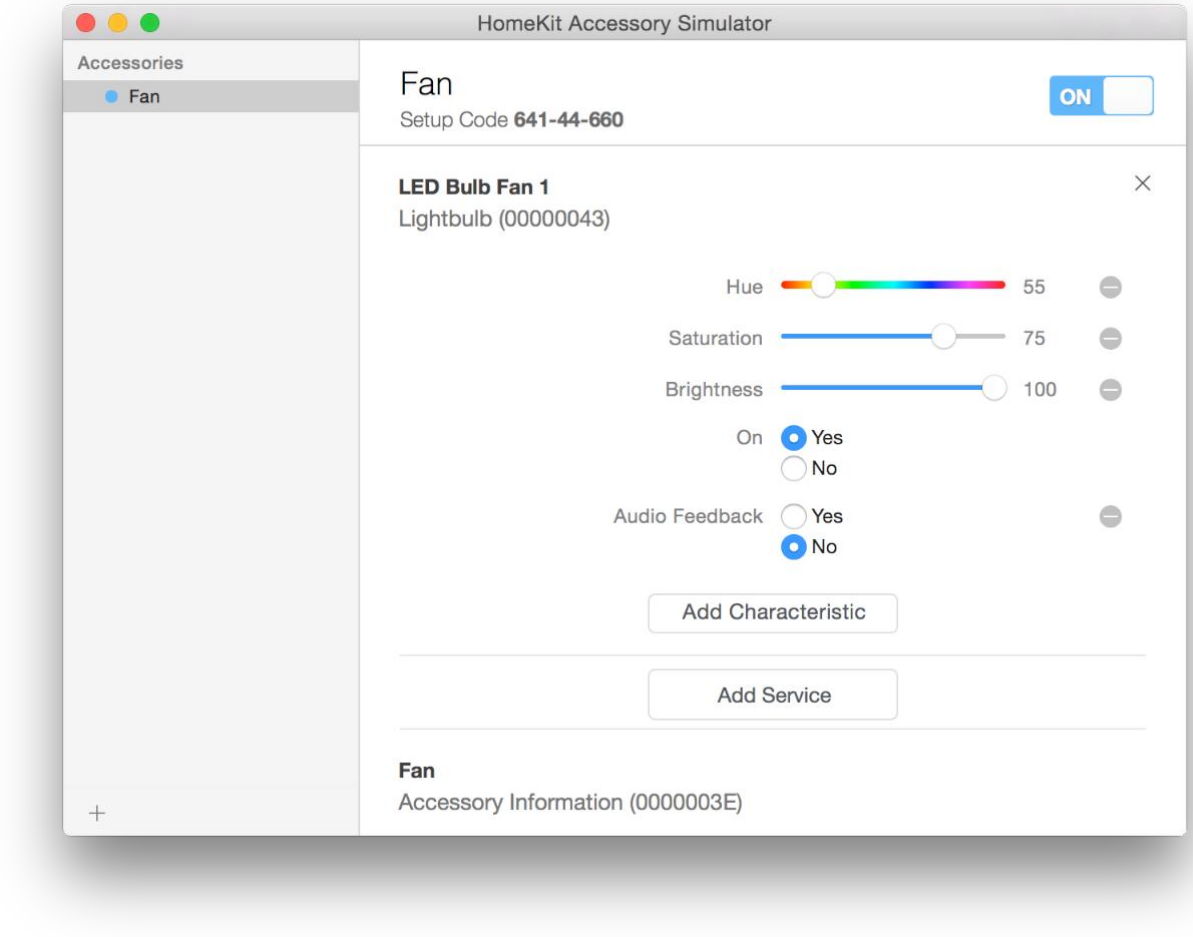


Рисунок 2.6. Управління аксесуарами системи розумного агро страхування на основі даних з IoT

– модульна технологія, можливості для етапного впровадження інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– проста інтеграція існуючих і майбутніх систем і інтерфейсів управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– база управління, що настроюється інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– автоматизований аналіз подій управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– автоматичне управління аварійними ситуаціями управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

2.3 Хмарні, туманні та граничні обчислення

«Хмара» - це система, що складається з декількох пристроїв, комп'ютерів і серверів, з'єднаних між собою через Інтернет. Така система обчислення може бути образно розділена на дві частини:

- зовнішній інтерфейс – пристрої клієнта (комп'ютери, планшети, мобільні телефони);
- внутрішній інтерфейс – зберігання даних і обробні системи, які можуть бути віддалені від пристроїв клієнта і самої хмари.

Ці дві частини системи безпосередньо взаємодіють один з одним за допомогою бездротових з'єднань.

Технологія хмарних обчислень надає різні види послуг, які діляться на три групи:

- послуги інфраструктури (IaaS) – віддалений центр обробки даних з такими ресурсами як: місткість зберігання даних, обчислювальна потужність, і мережі;
- платформа як послуга (PaaS) – розвиток платформи з пристроями і компонентами для створення, тестування і запуску додатків;
- послуги програмного забезпечення (SaaS) – готове програмне забезпечення, відповідне виробничими потребами.

Доступність – це головна перевага. Крім того, немає необхідності підтримувати місцеві послуги та переживати через час простою.

Інтеграція інтернету речей з хмарою – це вигідне рішення в бізнесі. Віддалені сервери забезпечують необхідну місткість і гнучкість для

управління та аналізу зібраних даних з підключених пристроїв, в той час як спеціалізовані платформи, такі як Asure IoT, Suite, IBM Watson, AWS, Google Cloud для IoT, дають розробникам створювати якісні програми без величезних вкладень в програмне забезпечення і ОЗУ.

Так як підключення пристрою обмежують місткість і обчислювальну потужність, інтеграція з хмарними обчисленнями допоможе забезпечити:

- поліпшення роботи (швидкий зв'язок між датчиками інтернету речей і системами обробки даних);
- місткість (добре масштабується і необмежене місце для зберігання в змозі об'єднати, з'єднати і розподілити величезний обсяг даних);
- можлива обробка (віддалені центри обробки даних забезпечують необмежені віртуальні можливості обробки на вимогу);
- зменшення витрат (ліцензійні збори нижче, ніж вартість обладнання на початковому рівні, і його безперервне обслуговування).

Недоліки використання хмарних обчислень:

- високий час очікування (додатки інтернету речей все більше вимагають, щоб час очікування був якомога нижче, але хмара не може цього гарантувати через відстані між пристроями клієнта і центрами обробки даних);
- час простою (технічні проблеми і збої в мережах можуть статися з будь-якої причини в будь-якій системі, що використовує Інтернет, і дані клієнта можуть постраждати при відключенні електрики; щоб уникнути проблем, багато компаній використовують кілька каналів зв'язку з автоматизованою відмовостійкістю;
- безпека і особиста інформація (особиста інформація передана через глобально пов'язані канали разом з тисячею гігабайтів інформації інших користувачів, не дивно, що система стає вразливою для втрати даних або кібератак; проблема може бути частково вирішена

за допомогою гібридної хмари або створення особистого хмарного сховища).

Термін туманні обчислення (або затуманення) був придуманий CISCO в 2014 році, тому він є новим для більшості людей. Туманні і хмарні обчислення взаємопов'язані між собою. У природі туман ближче до землі, ніж хмари, в світі технологій відбувається те ж саме, туманні обчислення ближче до кінцевого користувача, передаючи можливості хмарних обчислень кінцевому користувачеві.

Ухвала може звучати так: туманне обчислення – це розширення хмарних обчислень, що складається з декількох граничних вузлів, безпосередньо підключених до фізичних пристроїв.

Такі вузли фізично набагато ближче до пристроїв в порівнянні з централізованими центрами обробки даних, тому вони здатні забезпечувати миттєві з'єднання. Значна обчислювальна потужність периферійних вузлів дозволяє їм самостійно виконувати обчислення великого обсягу даних, не відправляючи їх на віддалений сервер.

Туманні обчислення також включають хмарні обчислення – невеликі і досить потужні центри обробки даних, розташовані на граничному сегменті мережі. Їх метою є підтримка ресурсоємних додатків інтернету речей, які вимагають низького часу затримки.

Основна відмінність між туманними і хмарними обчисленнями полягає в тому, що хмара являє собою централізовану систему, а туман являє собою розподілену децентралізовану інфраструктуру.

Туманні обчислення є посередником між обладнанням і віддаленими серверами. Туманні обчислення визначають, яка інформація буде відправлена на сервер, і яку інформацію можна буде редагувати локально. Таким чином, туман – це інтелектуальний шлюз, який розвантажує хмару, забезпечуючи більш ефективну, обробку та аналіз даних.

Слід зазначити, що туманна мережа не є окремою архітектурою і не замінює хмарні обчислення, а скоріше доповнює їх, максимально наближаючись до джерела інформації.

Нова технологія, можливо, надасть найбільший вплив на інтернет речей, вбудовані рішення штучного інтелекту і 5G, оскільки вони, як ніколи раніше, вимагають швидкої і безперебійної роботи.

Переваги туманних обчислень:

- низький час відгуку (туман географічно ближче до користувачів і здатний забезпечити миттєвий відгук);
- немає проблем з пропускною спроможністю (частина інформації агрегується в різних точках, а не відправляється в один центр по одному каналу);
- неможливість втрати з'єднання (через безліч з'єднаних каналів);
- високий рівень безпеки (так як дані обробляються величезною кількістю вузлів в складній розподіленій системі);
- покращений інтерфейс користувача (миттєвий відгук і відсутність простоїв радують користувачів);
- енергетична ефективність (периферійні вузли використовують в роботі високоефективні протоколи, такі як Bluetooth, Zigbee або Z-хвиля).

Недоліки туманних обчислень:

- система туманних обчислень більш складна (туман - додатковий шар в системі обробки і зберігання даних);
- додаткові витрати (компанії повинні купувати периферійні пристрої-роутери, маршрутизатори, шлюзи);
- обмежений масштаб (на відміну від хмари).

Концепції туманних і хмарних обчислень дуже схожі. Але все ж між ними є різниця по деяким параметрам. Розглянемо точкове порівняння туманних і хмарних обчислень:

У хмарних обчисленнях обробка даних відбувається у віддалених центрах обробки даних. Обробка і зберігання туманних обчислень здійснюється на граничному сегменті мережі, близького до джерела інформації, що має вирішальне значення для контролю в режимі реального часу.

Хмара є більш функціональною, ніж туман щодо обчислювальних ресурсів і можливостей зберігання.

В туманних обчисленнях виконується короткостроковий аналіз на граничному сегменті мережі через миттєвий відгук, в той час як в хмарних обчисленнях буде довгостроковий глибокий аналіз через більш повільний відгук.

При туманних обчисленнях час затримки – низький, при хмарних обчисленнях – високий.

Хмарна система може зруйнуватися при збоях мережі Інтернет. Туманні обчислення використовують різні протоколи і стандарти, тому ризик збою набагато нижче.

Туман є більш безпечною системою, ніж хмара з-за його розподіленої архітектури.

Нові вимоги до сучасних технологій є рушійною силою розвитку інформаційних технологій. Інтернет речей – це постійно зростаюча індустрія, яка вимагає більш ефективних способів управління передачею інформації і обробкою даних.

Туманні обчислення є одним з рішень в роботі з пристроями інтернету речей, так як вони можуть задовольнити потреби постійно зростаючого числа підключених пристроїв. Вони використовують локальні, а не видалені комп'ютерні ресурси, що робить продуктивність більш ефективною і потужною, і зменшуються проблеми з пропускною спроможністю.

Компанії повинні порівнювати хмарні і туманні обчислення, щоб використовувати по максимуму доступні можливості, і використовувати високий потенціал.

2.4 Методи та засоби обробки даних

Розглянемо метод розподіленої обробки даних для Інтернету Речей який використовує хмарні обчислення і безліч сенсорів для даних. Зокрема, спосіб реалізації розподіленого виконання алгоритмів обробки даних.

Всі пристрої IoT, використані в проекті, мають відносно середні характеристики і недорогі в ціні.

В останні роки, мережі і сенсорні технології стали швидко розвиватися, і сприймають все більше даних [4]. Подальші дослідження розширюють можливості машинного навчання, включаючи глибоку взаємодію безпосередньо з Інтернетом Речей.

Рівні інтеграції системи управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT представлено на рис. 2.7.

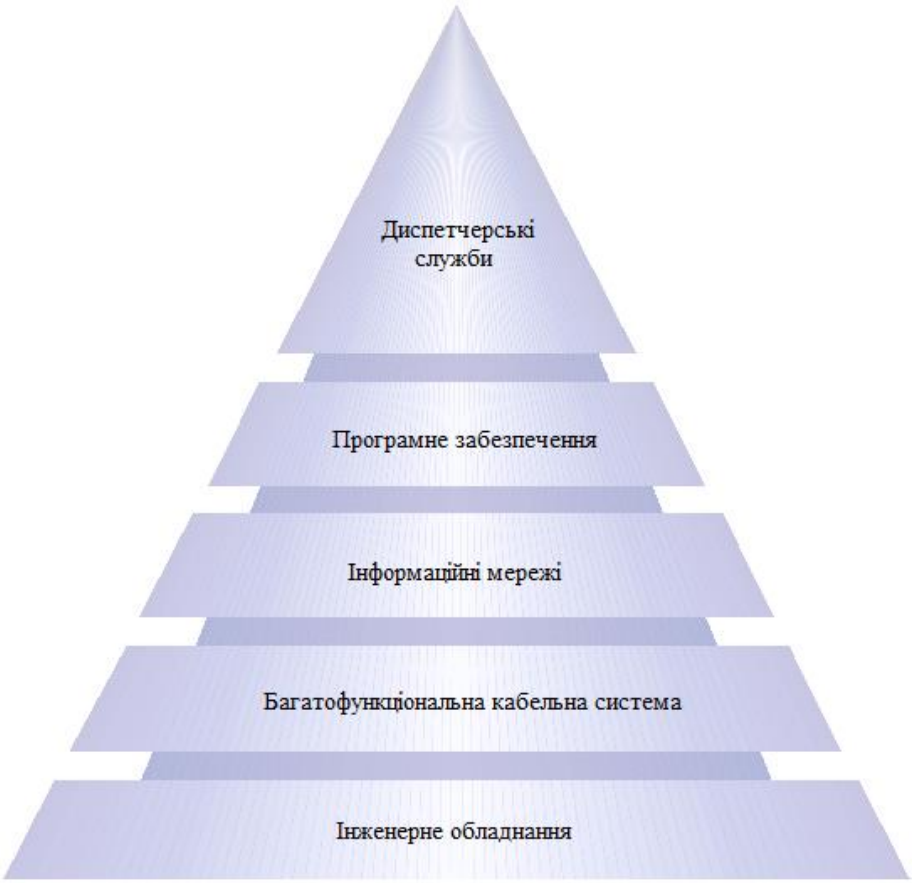
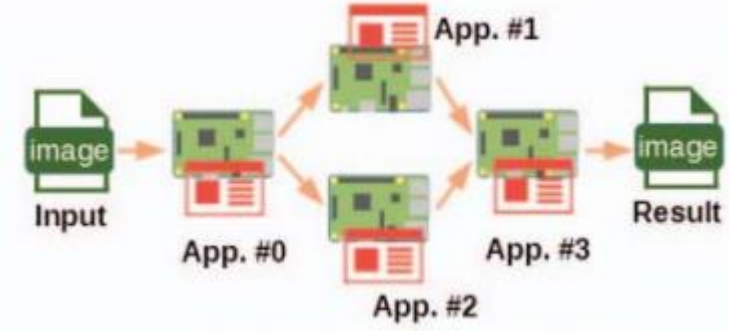


Рисунок 2.7. Рівні інтеграції системи управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT

а)



б)

Рисунок 2.8. Одно ланкова (а) та багатоланкова (б) структура засобів

У багатьох традиційних вбудованих пристроях програмне забезпечення реалізовано на одному апаратному засобі і одна задача запускається на незалежному пристрої (рис. 2.8, а).

Відповідно до еволюції технології LSI, недавно випущені пристрої Інтернет Речей є багатофункціональними, виконуючи функції отримання і передачі даних. Проте, через обмежене енергоспоживання і низьку вартість, можливості по обробці даних на IoT-пристроях складають від ¼ до 1/100 від можливостей сучасних комп'ютерів. Паралельні обчислювальні системи, що використовують залізо з низькими характеристиками, можуть використовувати методу високошвидкісної передачі даних, протее необхідна програмна модель такого алгоритму, яка має на увазі роздільну програмну розробку для кожного пристрою (рис. 2.8, б). У більшості випадків програми для паралельної системи обробки складні. Крім того, через довгий період розробки, налагодження і високі витрати, реалізація паралельної системи обробки даних була утруднена.

2.5 Висновки

У межах другого розділу розкрито функціональне призначення інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT, проведено проектування системи та описано принципи проектування інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT. Розглянуто варіанти організації доступу до сервісів корпоративної мережі з Інтернет інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

РОЗДІЛ 3. РОЗРОБКА ФУНКЦІОНАЛЬНОЇ СХЕМИ

3.1 Розробка функціональної системи агрострахування

Інформаційно-аналітична модель розумного агро страхування на основі даних з IoT, що розробляється є багаторівневою. Інтерфейс RS– 485 використано як інтерфейс зв'язку. Інтерфейс RS– 485 широко використовується в промисловій автоматиці, а так само мережа Ethernet. Загальна структурна схема інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT, що розробляється показана у додатку А на рис. А.1.

3.2 Розробка електричної принципової схем системи IoT-рішення

Електрична принципова схема управління комплексом аграрного призначення наведена у додатку Б на рис. Б.1.

Впровадження системи управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT передбачає:

– інтеграцію інженерних систем у інформаційно-аналітичу модель розумного агро страхування на основі даних з IoT;

– створення системи управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– інтеграцію системи управління інженерним обладнанням у систему управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

3.3 Розробка функції моніторингу та сповіщення

Технології, які використовуються для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне і гальванічне збудження. Приклади кожної з них:

- Радіочастотні: радіочастотні ідентифікаційні (RFID) -біркі, або радіопозначки.

- Інфрачервоні: інфрачервоні мітки, використовувані в середовищах, де потрібно відстежувати розташування і переміщення персоналу.
- Оптичні: штрих-коди і QR-коди можуть служити прикладами ідентифікаційних носіїв даних, які зчитуються оптично.

Останнім типом пристроїв є пристрої загального призначення. Вони володіють можливостями обробки даних і зв'язку, які можуть бути інтегровані в IoT. Хорошим прикладом є технологія «розумного будинку», яка може інтегрувати практично будь-який пристрій в будинку в мережу для централізованого або дистанційного керування.

Вимоги до шлюзів IoT, які зазвичай розпадаються на три категорії:

- Шлюз підтримує різні технології доступу до пристроїв, дозволяючи пристроїв обмінюватися даними один з одним і з мережею - Інтернетом або корпоративною мережею, що містить додатки IoT. Такі схеми доступу можуть, наприклад, включати ZigBee, Bluetooth і Wi-Fi.
- Шлюз підтримує необхідні мережеві технології як для локальних, так і для глобальних мереж. Ці технології можуть включати в себе Ethernet і Wi-Fi на території організації, а також стільниковий зв'язок, Ethernet, DSL і кабельний доступ до Інтернету і глобальним корпоративним мережам.
- Шлюз підтримує взаємодію з додатками, управління мережею і функції безпеки.

Дві перших вимоги включають в себе трансляцію протоколів між різними мережевими технологіями і стеками протоколів. Третя вимога зазвичай називається функцією IoT-агента . По суті, IoT-агент надає функціональність високого рівня від імені IoT-пристроїв, таку як організація або резюмування даних з декількох пристроїв для передачі в IoT-додатки, забезпечення протоколів і функцій безпеки і взаємодія з системами управління мережею.

Тут слід зазначити, що термін «мережа зв'язку» прямо не визначається в серії IoT-стандартів Y.206x. Мережа (або мережі) зв'язку підтримує зв'язок між пристроями і може безпосередньо підтримувати прикладні платформи. Вона може мати розміри невеликого IoT, такого як домашня мережа «розумних»

пристроїв. У більш загальному сенсі мережу (або мережі) пристроїв з'єднується з корпоративними мережами або Інтернетом для зв'язку з системами додатків і серверами, на яких розташовані бази даних, пов'язані з IoT.

Перша можливість - зв'язок між пристроями через шлюз. Наприклад, за допомогою шлюзу сенсорний або виконавчий пристрій з підтримкою Bluetooth може здійснювати зв'язок з пристроєм збору даних або пристроєм загального призначення, що використовують Wi-Fi.

Друга можливість - зв'язок по мережі зв'язку без шлюзу. Наприклад, якщо всі пристрої в мережі «розумного будинку» підтримують Bluetooth, вони можуть управлятися з комп'ютера, планшета або смартфона з підтримкою Bluetooth.

Третя можливість - прямий зв'язок пристроїв між собою за окремою локальною мережею, в той час як зв'язок із зовнішньою мережею здійснюється через шлюз LAN.

Кожна фізична річ в інтернеті речей може бути представлена в інформаційному світі однією або декількома віртуальними речами, але при цьому віртуальна річ може існувати без відповідної фізичної речі. Фізичні речі зіставлені віртуальним речам, що зберігаються в БД і інших структурах даних. Додатки обробляють віртуальні речі і працюють з ними.

Рівень мережі виконує дві базові функції. Можливості мережі відносяться до взаємодії пристроїв і шлюзів. Транспортні можливості відносяться до транспорту інформації служб і додатків IoT, а також інформацією управління і контролю IoT. Грубо кажучи, ці можливості відповідають мережевому і транспортному рівням OSI.

Рівень підтримки послуг і підтримки додатків надає можливості, які використовуються додатками. Багато різноманітні додатки можуть використовувати загальні можливості підтримки. До прикладів належать спільне опрацювання даних і управління БД. Спеціалізовані можливості підтримки - це конкретні можливості, які призначені для задоволення потреб конкретної підмножини додатків IoT.

Рівень додатку складається з усіх додатків, взаємодіючих з IoT-пристроями.

Рівень можливостей управління охоплює традиційні функції управління мережею, тобто управління несправностями, управління конфігурацією, управління обліком, управління показниками роботи і управління безпекою.

Можливості управління:

- управління пристроями: приклади включають виявлення пристроїв, аутентифікацію, дистанційну активацію і деактивацію пристроїв, конфігурацію, діагностику, оновлення прошивки і / або ПЗ, управління робочим статусом пристрою;
- управління топологією локальної мережі: прикладом є управління конфігурацією мережі;
- управління трафіком і перевантаженнями: наприклад, виявлення умов перевантаженості мережі і реалізація резервування ресурсів для термінових і / або життєво важливих потоків трафіку.

3.4 Висновки

У рамках третього розділу розкрито інноваційні механізми застосування системи розумного агро страхування на основі даних з IoT.

Система управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT призначена для забезпечення комфортних умов, захисту матеріальних цінностей, людей, що знаходяться в приміщенні, яке підлягає захисту.

РОЗДІЛ 4. РЕАЛІЗАЦІЯ АРХІТЕКТУРИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ МОДЕЛІ

4.1 Розробка алгоритму системи агрострахування на основі даних з IoT

Інформаційно-аналітична модель розумного агро страхування на основі даних з IoT призначена для створення комфортних умов, захисту матеріальних цінностей, людей, що знаходяться у комплексі аграрного призначення, що захищається, забезпечує виконання наступних функцій:

– аналіз сигналів тривог відкриття та злому;

– формування мікроклімату у всіх приміщеннях;

– подання сповіщення про наявність і місце виникнення тривожної / аварійних ситуацій на пульт сигналізації і зовнішній світлозвуковий оповіщувач;

– відключення кульових кранів подачі гарячої та холодної води;

– моніторинг стану елементів системи і її складових частин;

– формування сповіщення про не типову ситуацію в охоронні структури через термінал;

– формування сповіщення про не типову ситуацію, інших подій дзвоном і за допомогою SMS власнику і / або в охоронні структури [25].

Розглянемо приміщення двоповерхове, окремо стояче.

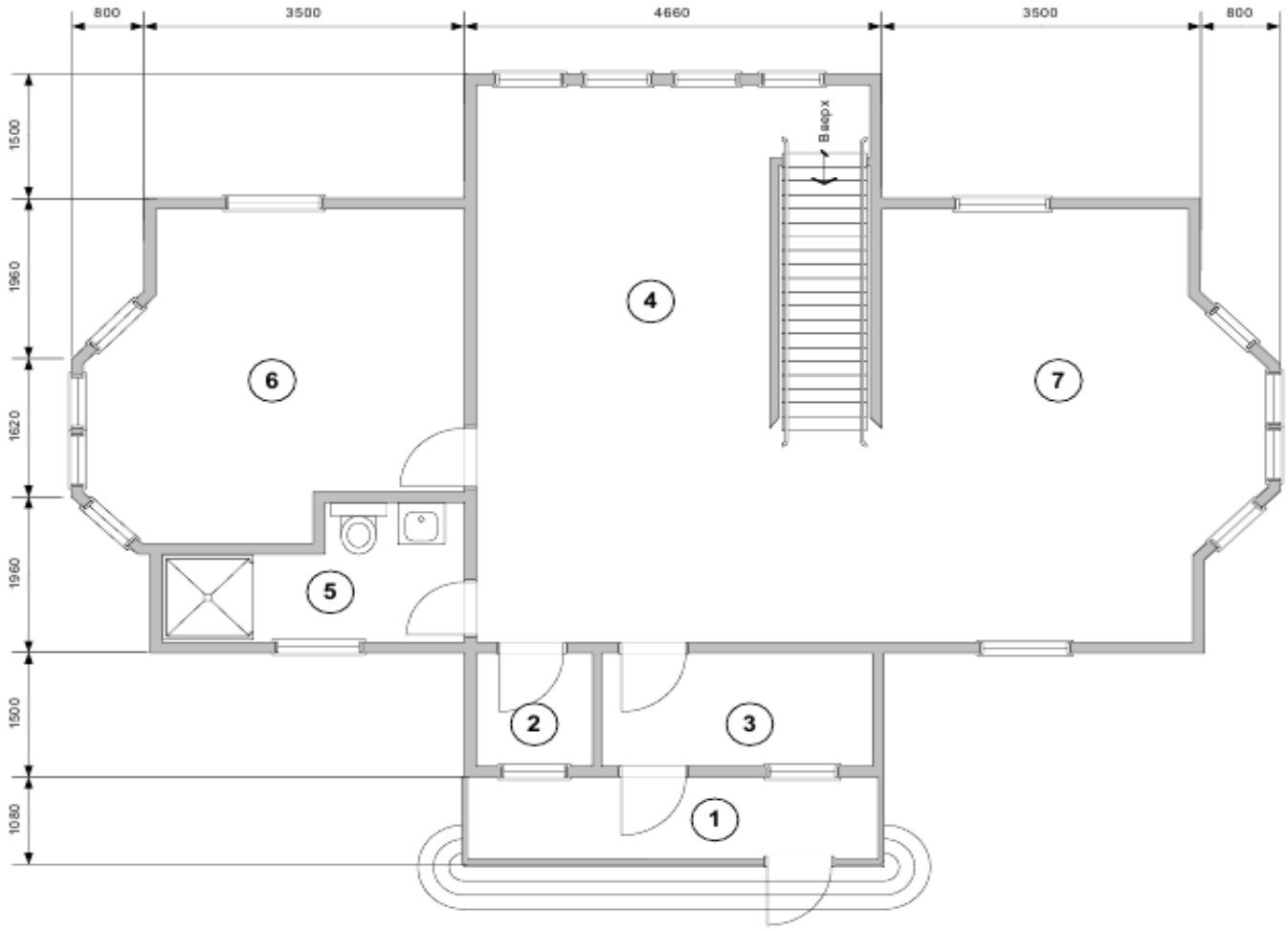
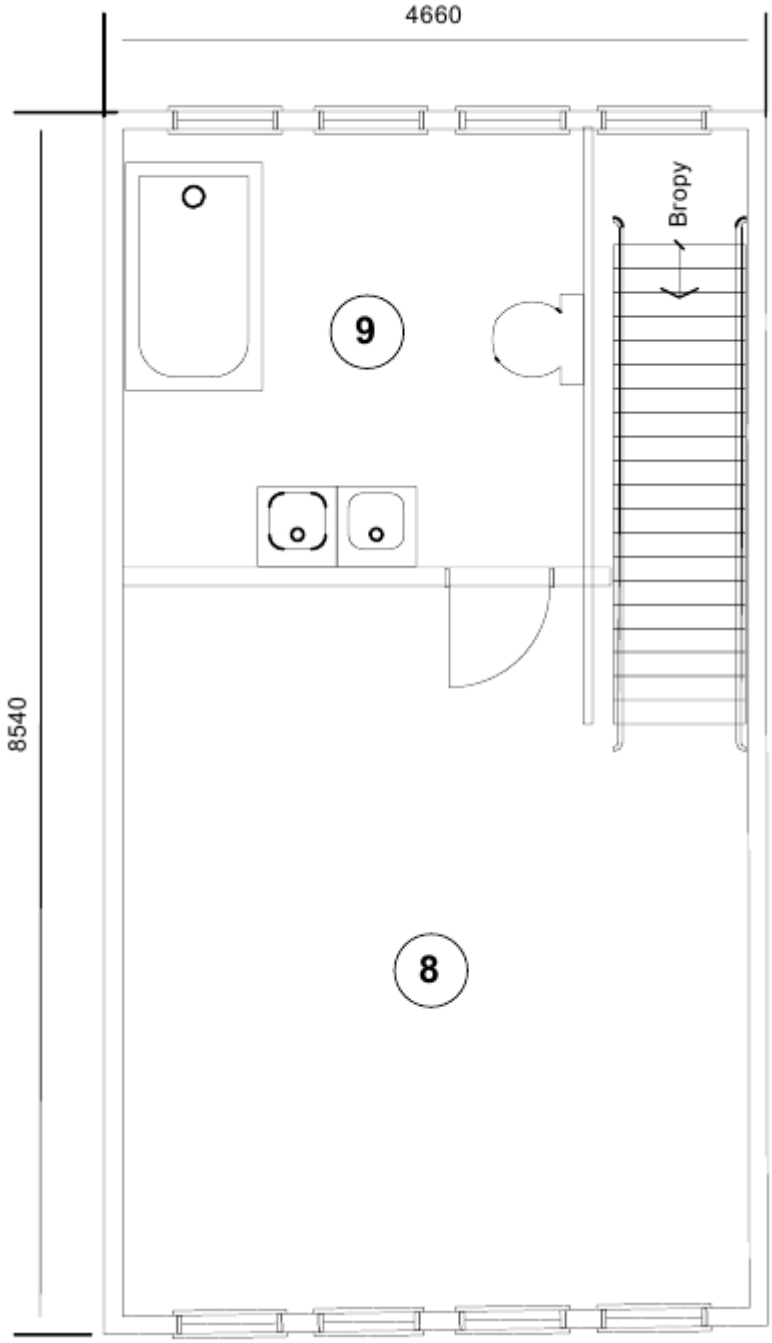


Рисунок 4.1. План будівлі, яка підлягає встановленню системи розумного агро страхування на основі даних з IoT

План першого поверху



Продовження рисунку 4.1. План будівлі, яка підлягає встановленню системи розумного агро страхування на основі даних з IoT. План другого поверху

Експлікація агроприміщень запропонована в таблиці 4.1.

Таблиця 4.1 – **Експлікація агроприміщень**

№ п.п	Найменування	Площа, м^2
1	**2**	**3**
	Перший поверх агроприміщення	
1	Тераса відкрита агроприміщення	4,36
2	Господарське приміщення для інвентарю притирального агроприміщення	1,69
3	Тамбур закритий агроприміщення	4,23
4	Приймальня агроприміщення	25,67
5	Санвузол	4,43
6	Склад	14,41
7	Виробниче приміщення агроприміщення	19,31
	Другий поверх агроприміщення	
8	Бухгалтерія	20,96
9	Санвузол	9,81

Алгоритм роботи моделі розумного агро страхування на основі даних з IoT представлений у додатку В на рис. В.1.

4.2 Обґрунтування вибору хмарного рішення

Рішення VMware володіють найбільш досконалими функціями гібридних хмар, вони сумісні з різними типами навантажень і підтримують міграцію між приватними і публічними хмарами разом із синхронізацією каталогів і шаблонів цих хмар. Крім того, рішення VMware забезпечують побудову скоординованих фреймворків високої доступності та безпеки для приватної і публічної хмари.

Віртуалізація дата-центру

У VMware найпотужніші функції віртуалізації і досвід їх використання в корпоративному секторі з початку минулого десятиліття. Хоча Microsoft в останні роки розширює можливості своєї платформи віртуалізації, Hyper-V як і раніше сильно поступається vSphere за популярністю в корпоративному секторі і застосування бізнес-критичних систем. В середині 2014 року Hyper-V підтримував близько 35 гостьових ОС, в той час як у vSphere це значення

становить майже сотню. В останні релізи Windows Server 2012 було додано кілька важливих нових функцій Hyper-V (наприклад, Extensible Virtual Switch і Replica), але головним недоліком архітектури Hyper-V як і раніше залишається використання батьківської ОС, що знижує безпеку і доступність гипервизора при установці патчів і обслуговуванні материнської Windows Server. Крім того, залежність від Windows Server означає, що реалізація в Hyper-V нових функцій віртуалізації відбувається тільки при виході нових версій цієї ОС.

RHEV використовує гіпервізор KVM, на якому працює переважна більшість хмар OpenStack. Зараз RHEV дуже популярний у сервіс-провайдерів і розробників додатків для вбудованих систем. Як і Hyper-V, RHEL є ОС-центричним гіпервізором (його материнської ОС є Red Hat Enterprise Linux (RHEL)), що погіршує безпеку і знижує доступність через необхідність установки патчів RHEL. Він підтримує тільки 15 гостьових ОС, значно поступаючись за цим показником vSphere і Hyper-V. У Red Hat останніх релізів додали ряд нових функцій, але в ньому як і раніше немає віртуального розподіленого комутатора, пулів ресурсів зберігання, балансування навантаження і засобів контролю введення / виводу зберігання і мережі. Корпоративні замовники рідко використовують хмари OpenStack на базі RHEV.

vSphere здатний масштабуватися на кілька кластерів хостів і розширюватися на нові кластери і віртуальні машини в міру зростання потреб. Як показали тести Taneja Group, архітектура vSphere підтримує більше число віртуальних машин на хост, причому ці ВМ обробляли різні комбінації бізнес-критичних додатків. Засоби управління vcenter Server і vcenter Operations Manager можуть масштабуватися до декількох тисяч і навіть десятків тисяч ВМ.

Через обмеження архітектури Hyper-V не може масштабуватися так само ефективно, як vSphere - наприклад, цей гипервизор не вміє керувати логічними пулами ресурсів (процесорів, пам'яті, мережевих ресурсів і

ресурсів зберігання), тому для гарантії стабільної продуктивності віртуальних машин потрібно використовувати виділений кластер хостів. RHEV також не підтримує пули ресурсів процесорів і пам'яті, які масштабуються на кілька хостів кластера і не забезпечує ізоляцію ресурсів або їх спільне використання пулами.

Пакет VMware vCloud Suite Enterprise забезпечує функції високої доступності, відмовостійкості і відновлення після аварій за допомогою функцій vSphere HA, vMotion, Storage vMotion, Fault Tolerance і vCenter Site Recovery Manager. Для зменшення планових зупинок для обслуговування серверів або СГД функції vMotion і Storage vMotion переносять в онлайновому режимі віртуальні машини і їх диски без зупинки роботи додатків і користувачів. Функція vSphere Replication підтримує різні варіанти реплікації для vCenter Site Recovery Manager (SRM) для захисту від великих аварій. SRM забезпечує централізоване планування післяаварійного відновлення, автоматичні failover і failback з резервного сайту або з хмари vCloud, а також тестування післяаварійного відновлення без переривання роботи додатків.

У Microsoft Windows Server 2012 R2 з Hyper-V досить потужні функції HA, реалізовані за допомогою Failover clustering, в тому числі виявлення збоїв і онлайнова міграція ВМ і віртуальних машин. Однак Failover clustering не оптимізовані для захисту ВМ.

Red Hat RHEV здатний виявляти збої ОС хоста або гостьової ОС і підтримує онлайнову міграцію ВМ і віртуальних машин, але в ньому немає вбудованих функцій резервного копіювання та реплікації для швидкого відновлення після аварій.

Дослідження Taneja Group вийшло в середині 2014 року. За минулий рік на ринок вийшли спочатку vSphere 5.5, потім шоста версія vSphere, і рішення для віртуалізації дата-центрів інших вендорів, але значний технологічний відрив VMware від конкурентів зберігається.

Компанія SAFEDATA використовує VMware vSphere і інші продукти VMware як платформу віртуалізації в своєму рішенні « Віртуальний дата-центр»(Virtual Data Center, VDC), на базі якого замовник може самостійно створювати IT-інфраструктуру будь-якої складності, повністю аналогічну рішенням на фізичному обладнанні. В якості апаратної платформи рішення використовуються леза HP BladeSystem c-Class, а також системи зберігання NetApp FAS6220 і FAS8060.

Замовник VDC отримує обчислювальні ресурси для побудови віртуальної інфраструктури з хмари SFCLOUD, розміщеного в двох територіально-распредёленних дата-центрах. Стійкість до відмов вузлів vSphere в SFCLOUD реалізована на основі технології vSphere High Availability (HA). Замовник крім безпосереднього управління цієї віртуальної інфраструктурою за допомогою VMware vCloud Director може гнучко розподіляти виділені йому ресурси хмари між своїми додатками в залежності від зміни навантаження, наприклад, якщо в якийсь момент число запитів до одного з додатків істотно зросте, то можна тимчасово передати йому частину процесорів, виділених іншим додаткам. Крім того, в процесі використання хмарної послуги VDC замовник може збільшувати або зменшувати обсяг виділених йому ресурсів, а також застосовувати різні моделі тарифікації.

Всі дії, пов'язані з управлінням послугою, зміною її параметрів, моніторингом продуктивності, а також фінансовими документами, здійснюються через веб-інтерфейс «Особистого кабінету» замовника VDC.

4.3 Обґрунтування вибору хмарних сервісів та їх налаштування

У новій версії середовища віртуалізації VMware vSphere з'явилася можливість переносити віртуальні машини з приватної хмари в публічну, між публічними хмарами Google, Amazon і Microsoft і, при бажанні, назад в приватну.

VMware вже давно працює з командою Amazon. Ще в vSphere 5.1 можна було розширити локальну інфраструктуру за рахунок публічної хмари AWS, переносити віртуальні машини в EC2 і управляти ними.

Технології VMware Cloud on AWS дозволяють використовувати всі ті ж надійні, перевірені часом рішення, які вже багато років працюють в ЦОДах наших замовників, але вже с можливістю безшовного розширення в публічне хмара Amazon. Причому це стосується не тільки базової технології віртуалізації обчислювальних ресурсів, але також і віртуалізації мережі (VMware NSX) і системи зберігання даних (VMware vSAN).

Таким чином, з одного боку, замовник може використовувати вже відомі йому технології VMware, а з іншого - розширювати за необхідності ємність свого Цода за рахунок публічного хмари Amazon. Перевага в тому, що можна використовувати ті ж інструменти і поняття, до яких звикли адміністратори, без необхідності переучуватися і занурюватися в ідеологію «Амазону». Крім іншого, це дозволяє забезпечити необхідний рівень SLA і сумісність додатків замовника як з приватною, так і з публічної інфраструктурою.

Якщо спуститися на рівень нижче, то для такого спільного проекту в рамках інфраструктури Amazon використовується виділене обладнання, яке допомагає запускати оптимізовані продукти віртуалізації VMware поверх технологій Amazon: VMware vSphere і Amazon EC2 (обчислювальні ресурси), VMware NSX і Amazon VPC (мережеві ресурси), VMware vSAN і Amazon EBS (ресурси для зберігання). З боку технологій VMware все управляється через єдине вікно - vCenter, з боку Amazon можна використовувати всі можливості AWS. Ці технології дають найкраще з двох світів приватних і публічних хмар: можливість перенесення додатків, готову інфраструктуру безпеки, необхідну продуктивність, еластичність сервісів, можливості використання DR, мікросегментацію, запуск контейнерів,ефективне управління вартістю ресурсів і багато іншого - і все це за моделлю «як

сервіс». Причому всі сервіси надаються, керуються, підтримуються і продаються через єдиного постачальника - VMware.

Нове в vSphere 6.5

У жовтні на конференції VMworld 2016 компанія VMware оголосила про прийдешнє оновлення платформи віртуалізації vSphere до версії 6.5. Заявлено, що в ньому з'являться нові засоби автоматизації і менеджменту. Ось кілька ключових новинок в vSphere 6.5:

vCenter - засіб, який спрощує доставку патчів, апгрейд, бекапи і відновлення, стане ключовим елементом vSphere;

vSphere Client - нове клієнтське засіб адміністрування засновано на HTML5 і спрощує адміністрування;

VM Encryption - засіб шифрування рівня віртуальних машин, покликане захистити від несанкціонованого доступу до даних і віртуальним машинам, які проходять міграцію за допомогою vMotion;

Secure Boot - нововведення, яке забезпечить захист від втручання в образи і від завантаження неавторизованих компонентів;

інтегровані контейнери (Integrated Containers) - інтерфейс, сумісний з Docker, який дозволить клієнтам завантажувати контейнери, не порушуючи інфраструктуру.

Окремо варто відзначити появу RESTful API, які спрощують автоматизацію і полегшують життя програмістам і адміністраторам. Ну і звичайно, нова версія зазнала ряд оптимізацій, які повинні помітно збільшити продуктивність. Міграція між приватною і публічною хмарою

1. Вибираємо місце розташування (рис. 4.2.)

Рисунок 4.2. Орієнтування

При використанні даної технології є можливість вибрати один з регіонів для розміщення ресурсів замовника, зокрема один з регіонів, доступних в AWS. Для розміщення ресурсів використовується виділена апаратна інфраструктура Amazon нового покоління, на якій забезпечується робота справжнього гипервизора VMware ESX.

2. Вибираємо розмір (Рис. 4.3)

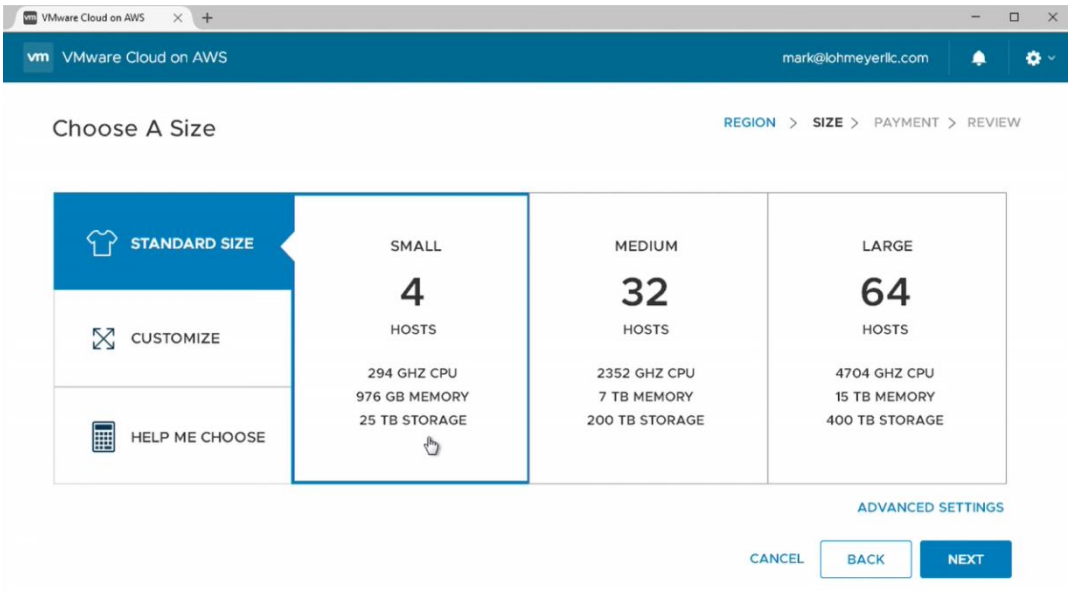


Рисунок 4.3. Розмір

Для оренди публічних обчислювальних ресурсів Amazon можна вибрати кілька варіантів: від декількох хостів до потужного кластера в 64 Ноди. Все залежить від потреб замовника. Оренда ресурсів в Amazon відбувається з єдиного аккаунта VMware через стандартний особистий кабінет, звідки можна управляти всіма ліцензіями VMware. Якщо необхідно, можливо використовувати REST API для виділення ресурсів, розширення публічного Цода, білінгу та іншого.

3. Оплата (Рис. 4.4)

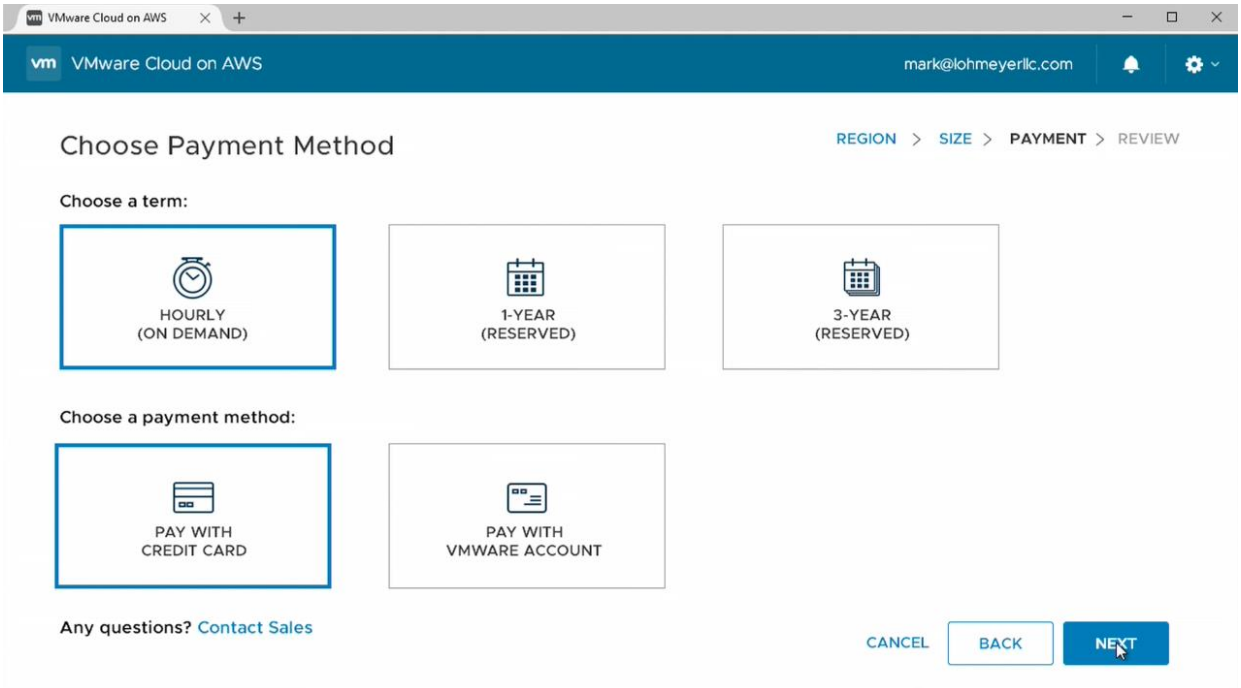


Рисунок 4.4. Оплата

Вибір моделі резервування та обліку ресурсів: погодинна оплата (Pay-As-You-Go) або резерв ресурсів на один або три роки. Оплатити можна кредиткою або з балансу особистого кабінету VMware.

4. Оточення VMware SDDC (Рис. 4.5)

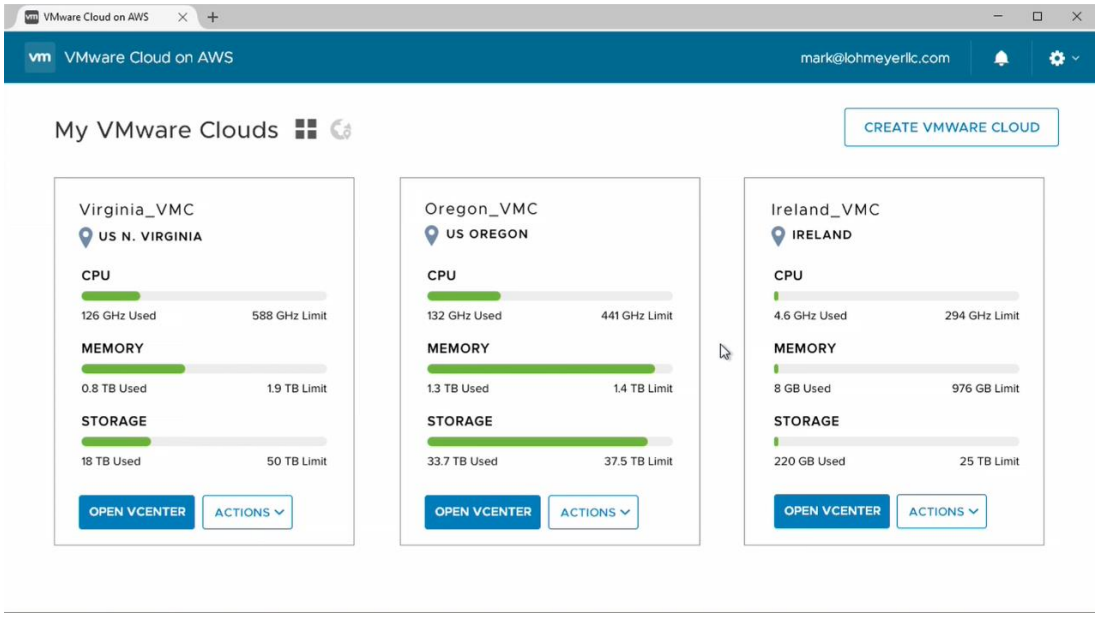


Рисунок 4.5. Оточення

Панель моніторингу та управління публічними ресурсами: ресурси в публічному хмарі Amazon орендуються в декількох регіонах, відображається їх завантаження.

5. vCenter, full environment (Рис. 4.6)

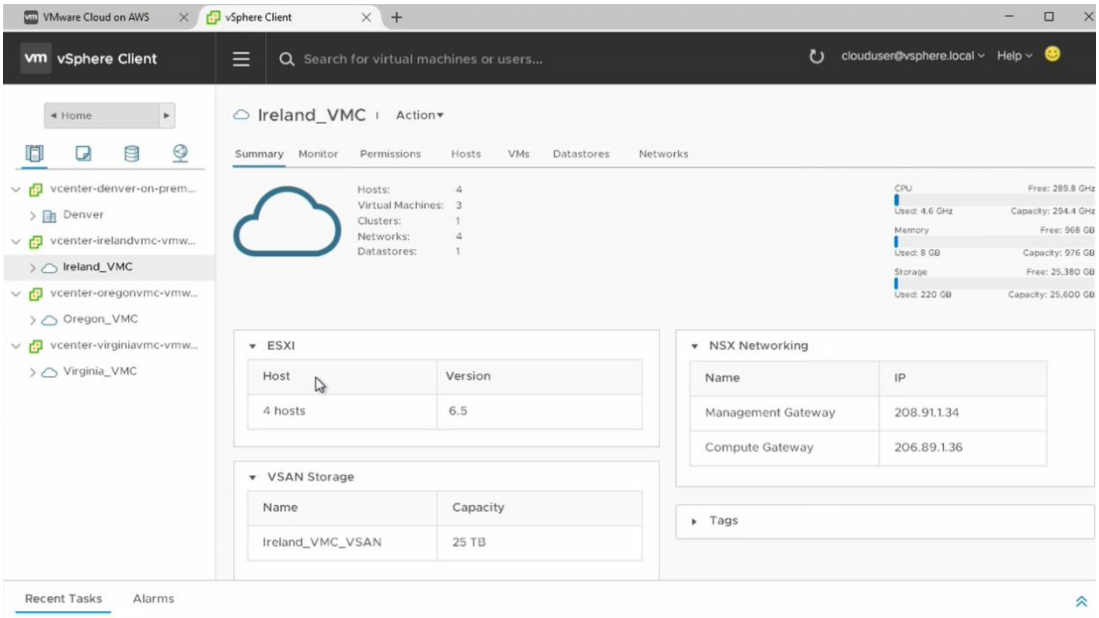


Рисунок 4.6. vCenter, full environment

Можливість мати єдиний засіб управління прямо з консолі vCenter. Не треба переключатися між різними інтерфейсами, використовувати різні

консолі і так далі. У адміністратора всього одне вікно для управління як внутрішніми ресурсами, так і публічними Amazon, включаючи управління різними регіонами.

6. Перемещаем сервіс з одного хмари в інше (Рис. 4.7)

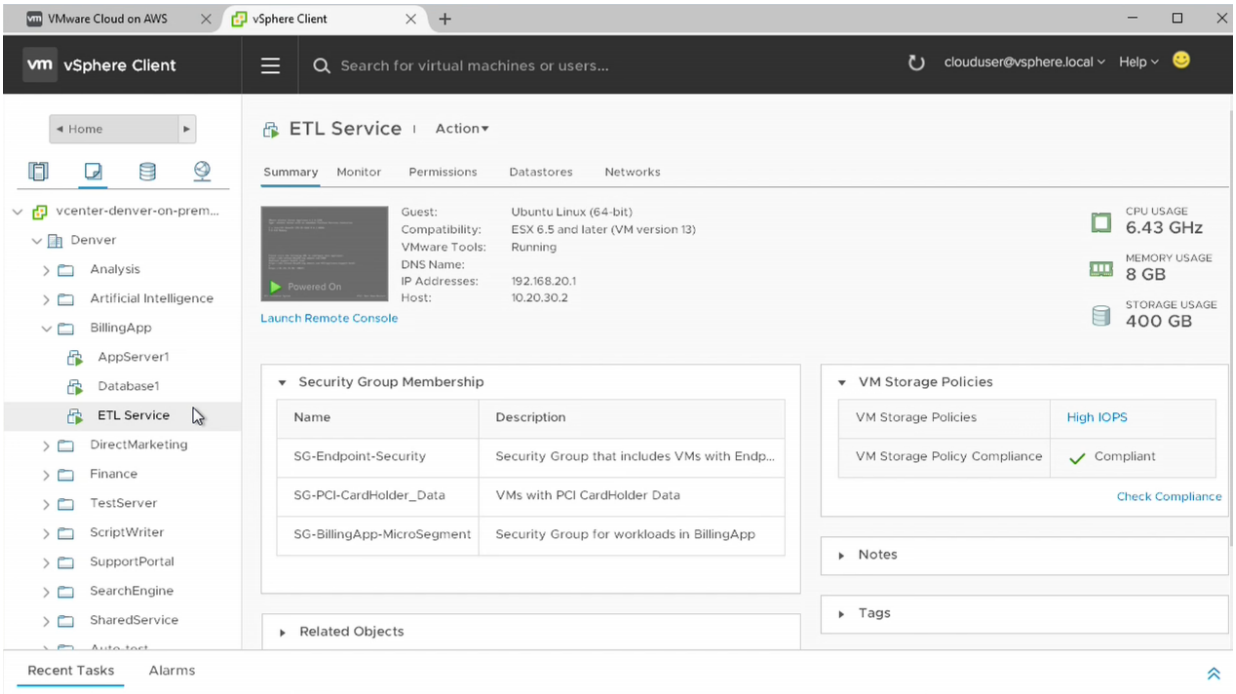


Рисунок 4.7. Перемещаем сервіс з одного хмари

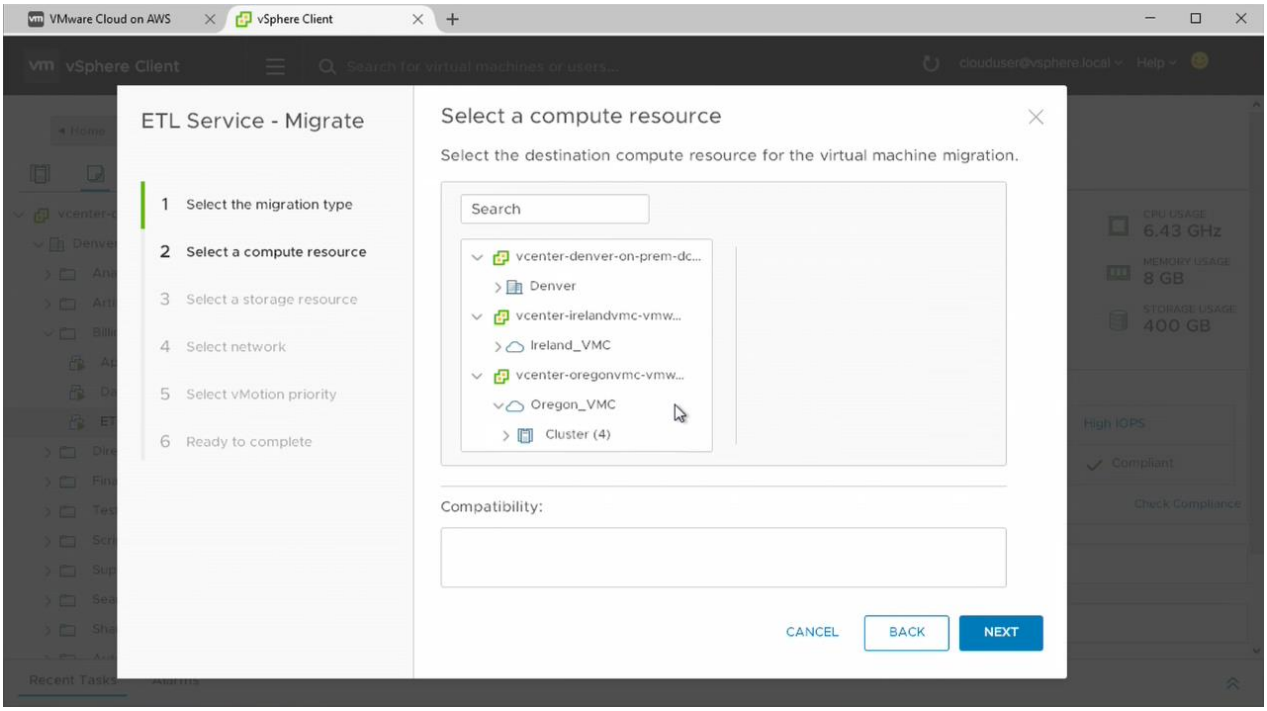


Рисунок 4.8. Перемещаем сервіс з однієї хмари

Можливість міграції віртуальної машини (Рис. 4.8) існує вже дуже давно. Зараз же ми виходимо на новий рівень - можна переміщати ВМ як з локального Цода в публічний (з внутрішнього хмари VMware в хмару Amazon), так і між різними регіонами публічної хмари Amazon.

7. Що буде, якщо перевищити обсяг кластера? (Рис. 4.9)

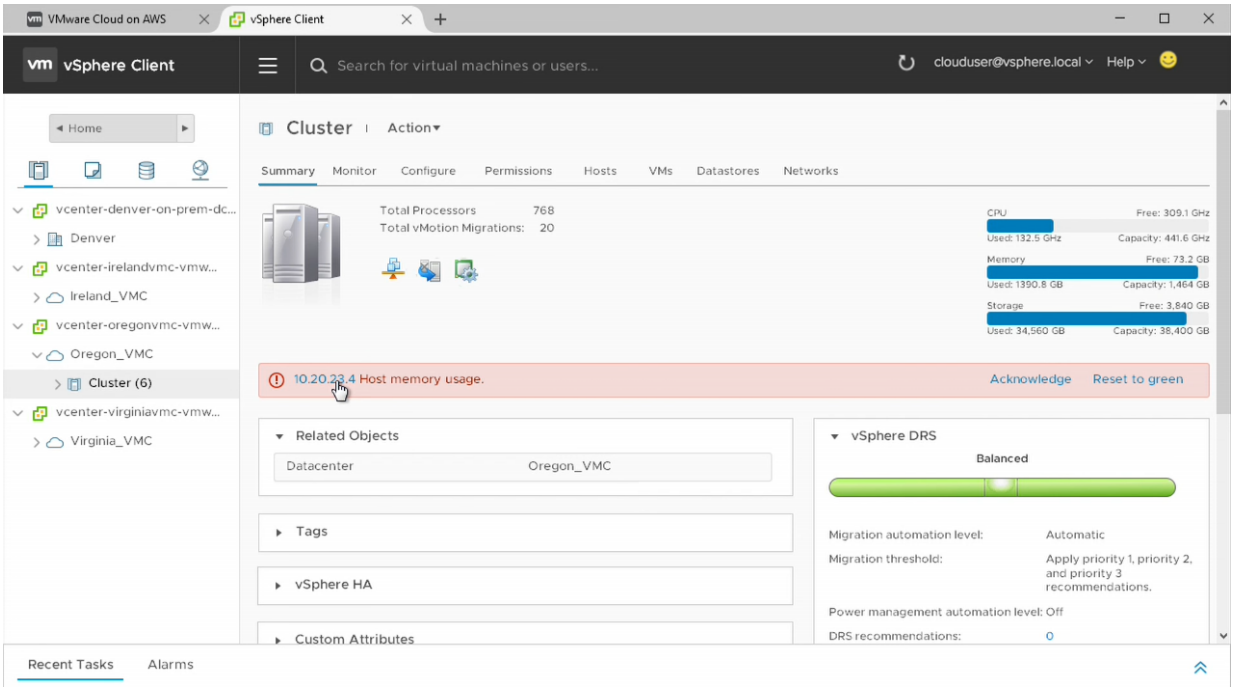


Рисунок 4.9. Обсяг кластеру

Адміністратор організації має можливість активувати автоматичне масштабування обчислювальних ресурсів. Тобто в разі нестачі публічних ресурсів в автоматичному режимі будуть запитані і виділені нові. З одного боку, технологія побудована поверх AWS EC2 API, яка і забезпечує можливість виділення нових ресурсів, а з іншого - використовується ресурсна модель і аналіз використання ресурсів від VMware. Причому поряд з простим перерозподілом ресурсів реалізовані і технології обходу відмов, коли в разі падіння апаратного сервера для замовника тут же виділяється новий абсолютно безкоштовно. Ця технологія була б неможлива без спільного використання всіх накопичених ноу-хау VMware і Amazon.

Технологія мережевого доступу на основі моделі Zero Trust Network Access (ZTNA): VMware Secure Access - це сервіс ZTNA, який об'єднує продукти VMware Workspace ONE і VMware SD-WAN в єдине хмарне рішення, яке забезпечує більш безпечний, оптимізований і зручний доступ для розподілених користувачів .

Інструменти хмарної і веб-безпеки: VMware співпрацює з провідними гравцями на ринку, щоб надати замовникам більш широкий вибір рішень відповідно до їх вимог до хмарних обчислень і веб-безпеки. Новий сервіс VMware Cloud Web Security дозволить інтегрувати Menlo Security - компонент Service Broker для доступу до хмарним сховищ і віддаленій ізоляції браузера - безпосередньо в рішення VMware SASE.

Інтегрований міжмережевий екран наступного покоління: VMware NSX Firewall - це міжмережевий екран сьомого рівня з контролем стану, який буде надаватися за моделлю SaaS і інтегруватися в платформу VMware SASE як при розрахованому на одного користувача, так і при многопользовательском використанні. Це доповнює можливості брандмауера існуючого рішення VMware SD-WAN. У своєму звіті Now Tech: Enterprise Firewalls, Q1 2020 аналітики з Forrester Research назвали VMware одним з п'яти провідних виробників міжмережевих екранів в світі.

Рішення VMware Workspace Security об'єднує провідну в галузі систему уніфікованого управління кінцевими точками і платформу забезпечення їх безпеки. Це дозволяє замовникам використовувати всі переваги роботи з великими даними для досягнення повної прозорості кінцевих точок, а також отримувати потенційно корисні дані і використовувати технологію предиктивної аналітики на єдиної панелі управління. Сьогодні VMware оголошує про додаткові пропозиції для VMware Workspace ONE і Workspace Security, які застосовуються для організації ефективної і надійної захисту пристроїв.

VMware Workspace Security Remote - комбінація ведучої в галузі системи для уніфікованого управління кінцевими пристроями (UEM) і

технології забезпечення безпеки кінцевих пристроїв і віддаленій IT-підтримки. Сьогодні, в той час як команда фахівців з інформаційної безпеки зосереджена на запобіганні, виявленні та реагуванні на загрози, IT-фахівці контролюють суворе відповідність нормативним вимогам і допомагають замовникам з розгортанням систем безпеки. Workspace Security Remote об'єднує ці два напрямки, щоб підвищити працездатність пристроїв, забезпечити доступ на основі моделі Zero Trust і автоматизувати процеси реагування на загрози.

VMware Workspace Security VDI інтегрує технології VMware Horizon і VMware Carbon Black Cloud в єдине уніфіковане рішення, що дозволяє IT-спеціалістам і фахівцям з інформаційної безпеки створювати віртуальні робочі столи і додатки з високим ступенем захисту. Workspace Security VDI відрізняється від звичних рішень, оскільки інтегрує технологію Carbon Black особливим чином - безпосередньо в рішення VMware vSphere Hypervisor і VMtools. Це підвищує загальну захищеність системи від злому і відкриває можливості по виявленню програм-вимагачів і безфайлові програмного забезпечення.

4.4 Аналіз захищеності інформації та методів і способів (протоколів) для її кіберзахисту

В даний час не існує, будь-яких стандартизованих методик аналізу захищеності АС, тому в конкретних ситуаціях алгоритми дій аудиторів можуть істотно відрізнятися. Однак методику аналізу захищеності корпоративної мережі запропонувати все-таки можливо.

І хоча даний підхід не претендує на загальність, його ефективність багаторазово перевірена на практиці. Типова методика включає використання таких методів:

• вивчення вихідних даних по АС;

• оцінка ризиків, пов'язаних з наявністю загроз безпеки щодо ресурсів АС;

• аналіз механізмів організаційного рівня, політики;

• безпеки організації і організаційно-розпорядчої;

• документації та оцінка їх відповідності вимогам існуючих нормативних документів, а також їх адекватності існуючим ризикам;

• ручний аналіз конфігураційних файлів маршрутизаторів, між мережевих екранів (МЕ) і проксі-серверів, які здійснюють управління між мережевими взаємодіями, поштових і DNS-серверів, а також інших критичних елементів мережевої інфраструктури;

• сканування зовнішніх мережевих адрес локальної обчислювальної системи (ЛОС) з мережі Інтернет;

• сканування ресурсів ЛВС зсередини;

• аналіз конфігурації серверів і робочих станцій ЛВС за допомогою спеціалізованих програмних засобів.

Методи тестування системи захисту. Перераховані методи дослідження припускають використання як активного, так і пасивного тестування системи захисту. Активне тестування системи захисту полягає в емуляції дій потенційного зловмисника по подоланню механізмів захисту. пасивне тестування передбачає аналіз конфігурації ОС і додатків за шаблонами з використанням списків перевірки. Тестування може проводитися вручну або з використанням спеціалізованих програмних засобів.

Таким чином, аналіз системи захисту АС проводиться з метою перевірки ефективності використовуваних в ній механізмів захисту, їх стійкості в щодо можливих атак, а також з метою пошуку вразливостей в захисті.

Традиційно використовуються два основні методи тестування:

• тестування за методом «чорної скрині»;

• тестування за методом «білої скрині».

Перший варіант передбачає відсутність у тестирующей боку будь-яких спеціальних знань про конфігурацію і внутрішню структуру об'єкта випробувань.

При цьому проти об'єкта випробувань реалізуються всі відомі типи атак, і перевіряється стійкість системи захисту щодо цих атак. використовувані методи тестування емулюють дії потенційних зловмисників, які намагаються зламати систему захисту. Основним засобом тестування в даному випадку є мережеві сканери, що володіють базами даних відомих вразливостей. Всі дослідження можуть проходити як з попередженням обслуговуючого персоналу про плановані роботах, так і без нього. У другому випадку існує можливість оцінити, за який час після початку дослідження персонал зафіксує інцидент, а також яка адекватність зроблених дій зі мінімізації його впливу або запобігання.

Метод «білого ящика» передбачає складання програми тестування на підставі знань про структуру і конфігурації об'єкта випробувань. В ході тестування перевіряються наявність і працездатність механізмів безпеки, відповідність складу і конфігурації системи захисту вимогам безпеки і існуючим ризиками. Висновки про наявність вразливостей робляться на підставі аналізу конфігурації використовуваних засобів захисту і системного ПО, а потім перевіряються на практиці. Це найбільш продуктивний метод проведення аналізу захищеності, що дозволяє виявити найбільше число вразливостей. Однак варто зауважити, що даний метод позбавлений можливості поглянути на додаток з позицій атакуючого.

Засоби аналізу захищеності. Арсенал програмних засобів, які використовуються для аналізу захищеності АС досить широкий. Причому в багатьох випадках вільно поширювані програмні продукти нічим не поступаються комерційним версіями.

Системи аналізу захищеності (security assessment systems), також відомі як сканери безпеки (security scanners) або системи пошуку вразливостей, проводять всебічні дослідження систем з метою виявлення вразливостей, які можуть привести до порушень політики безпеки. Результати, отримані від коштів аналізу захищеності, представляють звіт стану захисту системи в даний момент часу. Незважаючи на те, що ці системи не можуть виявляти

атаку в процесі її розвитку, вони можуть визначити потенційну можливість реалізації атак, що дозволяє знизити витрати на експлуатацію засобів захисту. застосування засобів аналізу захищеності дозволяє швидко визначити всі вузли корпоративної мережі, доступні в момент проведення тестування, виявити використовувані в мережі сервіси та протоколи, їх налаштування і можливості для несанкціонованого впливу (як зсередини корпоративної мережі, так і зовні). За результатами сканування ці кошти виробляють рекомендації і покрокові заходи, що дозволяють усунути виявлені недоліки. за з уществует, дії системи аналізу захищеності аналогічні діям охоронця, періодично обходить всі поверхи будівлі, що охороняється в пошуках відкритих дверей, незакритих вікон і інших проблем. Тільки в якості будівлі виступає корпоративна мережа, а в якості незакритих вікон і дверей - уразливості.

Класифікація засобів аналізу захищеності по типу виявляються вразливостей. Нагадаємо, уразливості інформації - це властиві об'єкту причини, призводять до порушення безпеки інформації та обумовлені недоліками процесу функціонування об'єкта, властивостями архітектури АС, протоколами обміну і інтерфейсами, застосовуваним ПЗ, апаратною платформою, а також умовами експлуатації.

Засоби пошуку вразливостей проектування. При пошуку вразливостей даного типу використовуються два підходи:

1. аналіз алгоритму програмно-апаратного забезпечення;

2. аналіз проекту системи.

Прикладом першого підходу може служити система Prototype Verification System (PVS), розроблена в Computers Science Laboratory інституту SRJ, відомого своїми системами виявлення атак NIDES і EMERALD. У систему PVS вбудований мова опису формальних специфікацій програмного продукту, а також підсистема, докази теорем. Другий підхід реалізований, наприклад, в системі CRAMM (CCTA Risk Analysis and Management Technology). Крім неї існують інші системи для

аналізу ризиків, в тому числі і для аналізу вразливостей проектування. Такі як: RANK-IT, @RISK, ALRAM, ARES, LAVA, ГРИФ і інші.

Система CRAMM була розроблена в 1985 році BIS Applied Systems Limited по замовленням уряду Великобританії. Продукт, заснований на методології Центральної Агентства по Комп'ютерам і телекомунікацій Великобританії (ССТА), за час свого існування зазнав кілька модифікацій в

Залежно від того, які системи інформаційної безпеки аналізувалися з його допомогою. На сьогоднішній день існують версії для військових відомств, державних структур, приватних організацій та фінансових інститутів.

Система ГРИФ передбачає, що для проведення повного аналізу інформаційних ризиків перш за все необхідно побудувати повну модель АС з точки зору інформаційної безпеки (ІБ). Для вирішення цього завдання ГРИФ, на відміну від представлених на ринку західних систем аналізу ризиків, досить громіздких і часто не припускають самостійного використання IT-менеджерами і системними адміністраторами, відповідальними за забезпечення безпеки інформаційних систем компаній, володіє простим і інтуїтивно зрозумілим для користувача інтерфейсом. Однак за зовнішньою простотою ховається складний алгоритм аналізу ризиків, враховує більш ста параметрів, який дозволяє на виході дати точну оцінку існуючих в інформаційній системі ризиків, засновану на аналізі особливостей практичної реалізації АС. Основне завдання системи ГРИФ - дати можливість IT-менеджеру самостійно (без залучення сторонніх експертів) оцінити рівень ризиків в АС і ефективність існуючої практики по забезпеченню ІБ компанії, а також надати можливість доказово (в кількісних показниках) переконати керівництво підприємства в необхідності інвестицій в сферу її інформаційної безпеки.

Гідність системи - автоматизація важко формалізується завдання, недоліками є залежність якості роботи від закладених в неї знань експертів і висока вартість.

Засоби пошуку вразливостей реалізації. Уразливості реалізації - це по суті помилки, допущені на етапі написання коду. Системи, пошуку таких вразливостей, можуть бути використані навіть не стільки розробниками ПЗ, що відносяться з розумінням до питань ІБ, скільки різними організаціями, які проводять сертифікацію програмно-апаратних засобів.

Тут можна виділити два підходи:

• аналіз на основі вихідного тексту;

• аналіз на основі виконуваного файлу;

У першому випадку для вирішення завдання реалізацій програмно-апаратного забезпечення, вільного від помилок, можна, по-перше, правильно організувати процеси розробки даного забезпечення, що має місце далеко не завжди через бажання скоріше випустити продукт на ринок або в термін виконати взяті з договору зобов'язання. В даному варіанті використовуються різні формальні методи опису алгоритму роботи продукту, відповідно до яких перевіряється протягом всього процесу розробки. По-друге, можна провести тестування вже готового виробу на предмет відсутності вразливостей в його початковому тексті.

Система SLINT є аналізатором захищеності вихідного коду програм (Source Code Security Analyzer), написаних на мовах C і C ++. даний аналізатор створений відомою групою експертів в області безпеки LOpht і призначений для виявлення наступних найбільш відомих помилок при програмуванні, призводять до виникнення вразливостей і можливості реалізації атак:

- переповнення буфера;
- вихід за межі масиву при індексації;
- відсутність перевірки аргументів;
- некоректний доступ до пам'яті;
- невідповідні аргументи виклику критичних процедур.

Процес верифікації ПЗ розбивається на наступні кроки:

1. Запис алгоритму аналізованого ПЗ в канонізований вигляді (опис, складене на основі математичного поняття «відповідність»).

2. Переклад канонізованого опису в тензорне рівняння за допомогою транслятора СОТМ (Словесний Опис - Тензорно- Множинний Апарат).

3. Відтворення початкового тексту аналізованого ПЗ на мові асемблера або С. При цьому початковий вихідний текст виходить на мові асемблера,

який потім переводиться в синтаксис С. Обробка вихідного тексту програми на мові асемблера або С за допомогою детранслятора АСТМА (Асемблер - ТензорноМно-жественний Апарат) і отримання тензорного рівняння.

4. Порівняння тензорних рівнянь програми і алгоритму і висновок про їх відповідність.

Аналіз виконуваного коду. У більшості випадків ПЗ поставляється без вихідних текстів. Крім того, аналіз вихідних текстів вимагає високої кваліфікації від обслуговуючого персоналу. Та й відсутність відповідних ефективних систем аналізу не дозволяє проводити дослідження на якісному рівні. Саме тому великий інтерес викликають системи пошуку вразливостей в виконуваному коді. Ці системи аналізу по функціональності можуть бути розділені на кілька класів: аналіз розміру, дати файлів і інших ознак; перевірка під час виконання коду; генерація тестів; дизасемблювання; імітація атак.

Метод аналізу атрибутів файлу заснований на простому порівнянні розміру, дати або будь-яких інших ознак файлу з наявними в базі даних вразливостей. На підставі результатів порівняння робиться висновок про наявність чи відсутність уразливості. Наприклад, перевірки такого роду виконує System Scanner.

Системи, що реалізують аналіз процесу виконання файлу, виявляють різні помилки (в тому числі і уразливості), які важко «відловити» в процесі аналізу вихідних текстів. Вони перевіряють:

• коректність виконання операцій з пам'яттю;

• коректність роботи з покажчиками;

• виклик функцій.

Система BoundsChecker Pro призначена для виявлення помилок, пов'язаних з правил зберігання до пам'яті. При її використанні препроцесор, наявний в BoundsChecker Pro, вбудовує в певні ділянки перевіряється програми свої фрагменти коду, які і відповідають за контроль операцій з пам'яттю, виклик функцій, роботу з покажчиками і масивами і т.д. необхідно відзначити, що за всіма своїми достоїнствами BoundsChecker Pro приховує і ряд недоліків. Це, по-перше, уповільнення роботи аналізованої програми за рахунок «Зайвого» коду, який здійснює перевірку. По-друге, помилки, не пов'язані з неправильним використанням пам'яті, не виявляються цією системою.

Система HeapAgent не змінює аналізований код, як це робить BoundsChecker Pro. Однак вона підставляє на місце будь-якого пулу пам'яті, що виділяється аналізованого додатком, свій власний, який і дозволяє відстежувати всі невірні операції з даними пулом пам'яті. До недоліків системи HeapAgent можна віднести те, що вона не дозволяє виявляти ніяких інших помилок (виклики функцій, переповнення стека і т. д.), крім безпосередньо помилок пулу пам'яті.

Система Purify NT так само, як і BoundsChecker Pro, вставляє в аналізований код свої фрагменти, що відповідають за перевірку роботи з пулом пам'яті і стеком.

Крім уповільнення роботи діагностується ПЗ, властивого і BoundsChecker Pro, обмежуючим її поширення фактором є те, що система Purify NT функціонує тільки під управлінням лінійки ОС Windows і дуже чутлива до типу процесора.

Системи генерації тестів проводять ряд зовнішніх впливів на аналізоване програмне забезпечення і вивчають відповідні дії системи на ці тести. дуже часто ці кошти аналізують реакцію системи на різні граничні значення вхідних даних, до яких можна віднести:

- переповнення буфера;
- вихід за межі масиву при індексації;
- відсутність перевірки аргументів;
- некоректний доступ до пам'яті;
- невідповідні аргументи виклику критичних процедур;

Потреба в такого роду тестах закономірна, оскільки за статистикою більшість вразливостей реалізації пов'язано саме з зазначеними помилками, наприклад, переповненням буфера. Більшість відомих систем генерацій-тестів розроблено для ОС Unix.

Сам процес дизассемблирования мало чим може допомогти при виявленні вразливостей, так як в цьому випадку обсяги аналізованого коду будуть набагато перевершувати розмір початкового тексту на мові програмування високого рівня для тієї ж програми. Однак дизасемблювати код може служити джерелом інформації для аналізаторів більш високого рівня, наприклад, для системи ACTMA.

Імітатори атак призначені для моделювання різних несанкціонованих впливів на компоненти АС. Саме ці системи отримали широку популярність зважаючи на свою відносну простоту і дешевизну.

За допомогою таких імітаторів уразливості виявляються ще до того, як вони будуть використані порушниками для реалізації атак. До числа систем даного класу можна віднести SATAN, Internet Scanner, Cisco Secure Scanner, NetRecon і т. д. з вітчизняних товарів можна виділити систему НКВД. Засоби імітації атак з однаковим успіхом виявляють не тільки уразливості реалізації, а й уразливості експлуатації. Саме ці розробки, поряд з системами пошуку вразливостей експлуатації, набули найбільшого поширення серед користувачів.

Засоби пошуку вразливостей експлуатації найбільш поширені, оскільки користувачі корпоративної мережі найчастіше мають справу саме з етапом експлуатації.

Такі засоби виявляють слабкості системної політики (наприклад, слабкі паролі), помилки настройки програмно-апаратного забезпечення і т.п.

В основі сучасних методик, які використовуються для аналізу захищеності АС, лежать критерії оцінки безпеки інформаційних технологій, що встановлюють класи і рівні захищеності. методики і концепції оцінки безпеки, а також набір критеріїв в достатньому обсязі містяться в міжнародних стандартах ISO, керівних документах, відомчих нормативних документах.

Незважаючи на відсутність будь-яких стандартизованих методик аналізу захищеності АС, типову методику запропонувати все-таки можна. Вона містить в собі

- вивчення вихідних даних;
- аналіз ризиків і оцінку політики безпеки організації;
- аналіз конфігураційних файлів маршрутизаторів, МЕ і проксі-серверів, поштових та DNS-серверів, а також інших критичних елементів мережевої інфраструктури;
- сканування ЛОМ зовні і зсередини; аналіз конфігурації серверів і робочих станцій ЛОМ за допомогою спеціалізованих програмних засобів.

Підводячи підсумок всьому вищесказаному, відзначимо, що в даний час питання аналізу захищеності корпоративних АС є добре опрацьованими. Є багатий арсенал засобів і методів для проведення подібних робіт. відпрацьовані методики проведення обстеження (аудиту) безпеки АС відповідно до перевіреними критеріями, затвердженими в якості міжнародних стандартів, уможливлюють отримання вичерпної інформації про властивості АС, що мають ставлення до безпеки.

На практиці аналіз захищеності АС проводиться при допомоги потужного програмного інструментарію, в достатньому обсязі представленого на ринку засобів захисту інформації.

4.5 Прогнозування економічного ефекту впровадження системи розумного агрострахування

Головною метою впровадження сучасної системи розумного агрострахування є підвищення якості обслуговування клієнтів і поліпшення процесу управління. Основними показниками якості для служби агрострахування є час обслуговування і максимальне, безпомилкове виконання побажань клієнта. Розрахунок середніх витрат часу на обслуговування клієнтів наведено в таблиці 4.2.

Таблиця 4.2 – **Час обробки в даний час і в проектному варіанті**

	Параметри у поточний час	**Параметри у проектному варіанті**
1	**2**	**3**
Кількість клієнтів, що обслуговуються за рік	6500	6500
Час на збір інформації з датчиків, хв..	5	5
Час оформлення первинної документації, хв..	10	3
Уточнення параметів, хв.	5	1
Внесення даних про основні показники в базу, хв..	5	0
Передача інформації в інші відділи, хв..	5	0
Час на формування повного пакету, з урахуванням усіх використаних послуг та показників датчиків, хв.	6	1

При автоматизованій системі управління річні витрати часу на обробку інформації складаються з витрат часу на обробку первинної інформації (перший етап) та витрат часу на збір і обробку інформації по кожному

аграрному комплексу (другий етап). У підсумку загальна трудомісткість робіт при такому способі обробки:

$$(5 * 6500) + ((10 + 5 + 5 + 5) * 6500) = 19000/60 = 3500 \text{ год / рік.} \quad (4.1)$$

У проектному варіанті роботи зі збору та аналізу інформації виконуються швидше, так як програма працює он-лайн, вносячи зміни в режимі реального часу відразу в базу даних без проміжних вікон підтвердження.

Загальна трудомісткість робіт при впровадженні сучасної системи агрострахування складе:

$$(5 * 6500) + ((3 + 1) * 6500) == 54000/60 = 950 \text{ год / рік} \quad (4.2)$$

Розрахунки показують, що при запровадженні нової сучасної системи агрострахуавння загальна трудомісткість роботи знизиться, користувач витратить на 2100 годин на рік менше, ніж в даний час. З цього можна зробити висновок, що якість обслуговування, підвищиться за рахунок економії часу.

Загальний час, який йде на обробку та формування звітної документації по всіх агровідділеннях з діючої системи становить:

$$6 * 6500 = 36000/60 = 650 \text{год / рік.} \quad (4.3)$$

З використанням сучасної АСУ агрострахування час, необхідний на виставлення остаточного страхового рішення дорівнює:

$$1 * 6000 = 6000/60 = 100 \text{ год / рік,} \quad (4.4)$$

що на 500 годин менше.

Це пов'язано з тим, що в сучасній системі агрострахування модулі «Рахунки» і «Показники» вже інтегровані в систему, досить при проведенні моніторингу просто роздрукувати вже проаналізовану інформацію по агрокомплексу з урахуванням усіх відділів, а не працювати з кожним модулем окремо. Це дозволяє відзначити збільшення швидкості обслуговування в даному напрямку.

Агропромислове підприємство, що розглядається у рамках даної дипломної роботи вже має 1 сервер на Linux, комп'ютерне оснащення робочих місць, змонтовані електричні слабкострумові мережі, організована локальна мережа. На підставі цього був складений перелік обладнання і витрат на реалізацію проекту впровадження сучасної системи агрострахування в таблиці 4.3.

Таблиця 4.3 – **Капітальні вкладення за проектом впровадження сучасної системи агрострахування**

Найменування	**Ціна за од. тис. грн..**	**Кількість, шт..**	**Вартість, тис. грн.**
1	**2**	**3**	**4**
Програмне забезпечення	600	1	600
2 робочих місця	1,2	4	4,8
Робоча станція (ПК Celeron G540 (2.5GHz)/2GB /Intel HD/320GB/DVDRW/Cam/WiFi/KB+M/DOS/Black)	14,7	2	2,94
Сенсорні монітори ZTE 11.6	6,4	46	243
Універсальне кріплення Holder DRS-3103	0,24	46	10,8
Кабель UTP кат.5е бухта 305м Telecom Ultra	0,99	1	0,99
Установка додаткових модулів	10,6	1	10,6
Послуги фахівців з впровадження	3	10	60
Навчання персоналу	-	-	80
Інфрачервоний датчик руху Ajax MotionProtect Outdoor	0,3	12	3,6
Всього			893,69

Реалізація проекту буде здійснюватися поетапно протягом тижня.

Паралельно з впровадженням ПЗ буде проводитися установка сенсорних моніторів з «блоковим» інтерфейсом Metro, спеціально розробленим для агропідприємства.

В процесі впровадження і установки необхідно проводити навчання персоналу, на організацію семінарів виділено 80 тис. грн., консультанти компанії-підрядника проведуть 2 семінари та консультуватимуть користувачів з виникаючих питань в процесі навчання роботи на новій системі. Етапи впровадження представлені в таблиці 4.4.

Таблиця 4.4 – **Реалізація проекту та терміни виконання**

Найменування етапу	**Строки виконання**
1	**2**
Аналіз існуючої системи агрострахування	Одна доба
Впровадження розумної системи	Упродовж тижня
Навчання персоналу і гарантійний супровід програми	Упродовж тижня
Установка сенсорних моніторів	Упродовж тижня

Для оцінки рівня ризику в агро бізнесі найкращим чином підійде метод експертних оцінок, який дозволяє визначати рівні фінансових ризиків в тому випадку, якщо на підприємстві відсутня необхідна інформація для здійснення розрахунків або порівнянь. Даний метод базується на опитуванні експертів (кваліфікованих фахівців страхових, податкових, фінансових органів, інвестиційних менеджерів, працівників відповідних спеціалізованих фірм) з подальшою статистичною обробкою результатів опитування. Комерційні ризики пов'язані з реалізацією послуг (зменшення розмірів і місткості ринку, зниження платоспроможного попиту, появу нових конкурентів).

Заходами щодо зниження ризиків будуть:

- систематичне вивчення кон'юнктури ринку послуг;
- відповідна цінова політика;

– створення системи комплексного обслуговування і додаткових послуг.

Фінансові ризики можуть бути викликані інформаційними процесами, загальними неплатежами, коливаннями валютних курсів і пересичення ринку пропозицій.

Підприємство враховує і ризики, пов'язані з форс-мажорними обставинами, - це ризики, обумовлені непередбаченими обставинами (від зміни політичного курсу країни до страйків і землетрусів). Для зниження загального впливу ризиків на ефективність роботи підприємство передбачає комерційне страхування по системах менеджменту страхування.

Ризик появи альтернативної послуги на ринку послуг страхування досить великий. Для зниження рівня даного ризику можна застосувати систему знижок, що знизить ціни в порівнянні з конкурентами і приверне нових клієнтів. Щоб знизити ризик нестійкості попиту відсутності резервів, агропідприємству можна запропонувати акцентувати увагу на унікальних пропозиціях – тих продуктах, які ніколи раніше не пропонувалися.

Велику увагу варто приділяти ризику зниження цін конкурентами, так як більшість споживачів вибирають там де дешевше. Для зниження даного ризику організації можна запропонувати стежити за діяльністю конкурентів і своєчасно реагувати на зміни.

Таким чином, підбиваючи підсумки проведеного дослідження, можна зробити висновок, що впровадження сучасної системи агрострахування дозволить:

1) підвищити відповідальність кожної категорії службовців, шляхом автоматизації їх діяльності;

2) скоротити час обслуговування, використовуючи сучасну систему управління;

3) знизити змінні витрати на електроенергію, шляхом підключення модуля енергозбереження з датчиками руху;

4) збільшити дохід агропідприємства, завдяки автоматизації бізнес-процесів, пов'язаних з плануванням і проведенням заходів, а також за рахунок використання розумного планування та моніторингу.

Сформована практика впровадження даної автоматизованої системи агрострахування в агробізнесі за кордоном, а також і на території України показує, що при впровадженні проекту більш ефективним стане зв'язок між функціональними підрозділами. Істотно скоротиться час на обробку інформації і прийняття рішень, підвищиться якість управлінської праці.

Використання сучасних технологій дозволяє досягти підвищення продажів, прихильності клієнтів і ефективності роботи працівників. Агропромисловий комплекс перетворюється в кероване підприємство, здатне гнучко реагувати на зміни в ринковій ситуації, що робить вкладення коштів в технології повністю такими, що окупаються.

Для успішної реалізації проекту необхідний обсяг капітальних вкладень становить 893590000 грн. Джерелом фінансування проекту виступають власні кошти агропромислового підприємства в необхідному розмірі.

Звіт про фінансові результати підготовлений з урахуванням минулорічних фінансових звітів організації, поточної ринкової вартості на основні статті витрат. У таблиці 4.5 представлений прогноз виручки після реалізації проекту впровадження автоматизованої системи агрострахування. У перший рік реалізації проекту відбудеться зростання виручки від експлуатації на 4%, у другий – на 3%, третій рік – 2,5%, 4 рік – 2%. (табл..4.5)

Вихідні дані для аналізу ефективності інвестиційних вкладень при розробці та реалізації заходів в таблиці 4.6.

Таблиця 4.5 – **Прогноз виручки після впровадження системи агрострахування, грн.**

Показники	**Роки**				
	2021	**2022**	**2023**	**2024**	**2025**
1	**2**	**3**	**4**	**5**	**6**
Дохід від експлуатації системи	82882760	85368220	87502420	89252470	92037520
Прибуток (збиток) до оподаткування	22800320	23284330	23523940	23784220	24059900
Чистий прибуток (збиток)	8399040	8652022	8867286	9044632	9225525
Збільшення прибутку за рахунок впровадження АСУ агрострахування	323040	757022	792286	968632	2249525

У перший рік реалізації проекту виручка організації збільшиться на 3 187760 грн. і складе 82 881760 грн., у другий рік – на 5 674210 грн. з паралельним збільшенням чистого прибутку за рахунок скорочення постійних і змінних витрат, шляхом використання енергозберігаючої системи з датчиками автоматичного включення освітлення в коридорах, а також знизяться витрати на семінари, конференції та комерційні витрати на рекламу і оплату комісійних служби супроводу.

Автоматизація робочих місць всіх категорій співробітників підвищує їх залученість в управлінський процес. Аналітична база нової системи агрострахування дозволить створювати резерви для зниження податкового навантаження.

Запропоновані заходи передбачають вдосконалення процесу агрострахування на агропромисловому підприємстві на підставі впровадження сучасної автоматизованої системи агрострахування.

В результаті впровадження автоматизованої системи агрострахування в пропонованому проектному варіанті значно зменшилися витрати часу і кількість помилок. Це дозволило підвищити якість обслуговування на агропромисловому підприємстві. Зростання частки постійних клієнтів призведе до зростання виручки агропідприємства.

Таблиця 4.6 – **Розрахунок економічної ефективності проекту впровадження системи агрострахування, грн.**

Показники	**Роки**				
	2021	**2022**	**2023**	**2024**	**2025**
1	**2**	**3**	**4**	**5**	**6**
Програмне забезпечення	500000	-	-	-	-
Додаткове обладнання	233890	-	-	-	-
Послуги спеціалістів по впровадженню	80000	-	-	-	-
Навчання персоналу	60000	-	-	-	-
Усього витрат	893590	-	-	-	-
Збільшення рівня прибутку за рахунок впровадження автоматизованої системи агрострахування	-	323040	575022	792286	968632
Економічний ефект	- 893590	323040	575022	792286	968632

В результаті агропромисловий комплекс оснащений сучасною системою агрострахування та одночасно механізмом розумного управління, де на високому рівні реалізовані функції контролю і статистики, управління заходами обліку, що покращує процес управління та документообігу.

4.6 Висновки

У четвертому розділі здійснено реалізацію архітектури інформаційно-аналітичної моделі, наведено алгоритм системи агрострахування на основі даних з IoT,здійснено обґрунтування вибору хмарних сервісів та їх налаштування, проаналізовано рівень захищеності інформації та методів і способів (протоколів) для її кіберзахисту.

Запропоновані заходи передбачають вдосконалення процесу агрострахування на агропромисловому підприємстві на підставі впровадження сучасної автоматизованої системи агрострахування.

В результаті впровадження автоматизованої системи агрострахування в пропонованому проектному варіанті значно зменшилися витрати часу і кількість помилок. Це дозволило підвищити якість обслуговування на агропромисловому підприємстві. Зростання частки постійних клієнтів призведе до зростання виручки агропідприємства.

В результаті агропромисловий комплекс оснащений сучасною системою агрострахування та одночасно механізмом розумного управління, де на високому рівні реалізовані функції контролю і статистики, управління заходами обліку, що покращує процес управління та документообігу.

ВИСНОВКИ

В дипломній роботі проведено дослідження системи розумного агро страхування на основі даних з IoT. При вивченні концепції інтелектуальної системи управління будівлею були сформульовані основні вимоги і характеристики її реалізації. Серед існуючих в світі на сьогоднішній день реалізацій ті, які найбільш повно задовольняють вимогам концепції інтелектуального комплексного моніторингу приміщень інтегровані до системи управління будівлею. В рамках своїх стандартів вони забезпечують виконання всіх вимог системи, володіючи при цьому безсумнівними перевагами:

- тривале і глибоке опрацювання таких систем безліччю розробників;
- наявність відкритих стандартів, підтримуваних широким колом розробників;
- економічні вигоди як для творців систем, так і для їх користувачів;

Тому, дана реалізація була обрана в якості об'єкта для створення макета. Таким чином, у межах дипломного проекту було створено модель системи комплексного моніторингу приміщень за допомогою технології Інтернет речей. Модель зроблена щоб максимально знизити витрати на монтаж системи. Щодо моделі сучасної інтелектуальної системи комплексного моніторингу приміщень за допомогою технології Інтернет речей, то вона зроблена так, щоб за потребою у неї можна було вносити необхідні зміни не перериваючи її роботу та не припиняючи її.

Переваги створеної системи системи розумного агро страхування на основі даних з IoT:

– дозволяє здійснити моніторинг всієї системи розумного агрострахування з урахуванням розташування датчиків інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– відкрита гетерогенна архітектура управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– об'єднана розподілена база даних управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– інтерфейси між процесами управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

– масштабовані рішення управління інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT;

Недоліки створеної системи:

– висока вартість;

– обов’язкове навчання персоналу призначеного для роботи з системою розумного агро страхування на основі даних з IoT.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Луценко О. А., Поливана Л. А. Сучасний стан та перспективи розвитку ринку аграрного страхування. Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. 2018. Вип. 191. С. 273-284.

2. Прокопчук О. Т. Зарубіжний досвід страхування аграрних ризиків та доцільність його застосування в Україні / О. Т. Прокопчук, Ю. В. Уланич, К. Ф. Уланич // Збірник наукових праць Уманського національного університету садівництва. 2013. Вип. 83. С. 227-234.

3. Якубович В. Система страхования аграрных рисков в Испании: выводы для Украины [Электронный ресурс] / В. Якубович. – Режим доступа: http://forinsurer.com/public/06/11/30/2719– Название с экрана. Дата звернення: 20.05.2021.

4. Сравнение программ страхования урожая в США [Электронный ресурс] / Режим доступа: http://www.agroinsurance.com/files//publications/CropInsPlanCompar%20-20rus_1.doc Название с экрана. Дата звернення: 20.05.2021.

5. Шолойко А. Світовий досвід державної підтримки сільського господарства через програми страхування. Економіка АПК. 2013. № 135. С. 41-43.

6. «Интернет вещей» в промышленности: обзор ключевых технологий и трендов // Ли Да Сюй (Li Da Xu), Ву Хе (Wu He) - whe@odu.edu, Сянчан Ли (Shancang Li) - shanchang.li@bristol.ac.uk, перевод Алексей Осотов. – http://www.controlengrussia.com/internet-veshhej/klyuchevy-h-tehnologij/(Дата обращения: 20.05.2021)

7. Семенченко П.И. Обзор и анализ функциональных возможностей платформ для устройств интернета вещей. Российский экономический университет им. Г.В. Плеханова, 2017. № 5. С. 156-168.

8. Шварц Марко Интернет вещей с ESP8266: Пер. с англ. СПб.: БХВ-Петербург, 2018. 192 с.

9. Li S., Xu L., Wang X. Compressed sensing signal and data acquisition in wireless sensor networks and internet of things // IEEE Trans. Ind. Informat. 2013. Vol. 9. No. 4.

10. He W., Xu L. Integration of distributed enterprise applications: A survey // IEEE Trans. Ind. Informat. 2014. Vol. 10. No. 1.

11. Uckelmann D., Harrison M., Michahelles F. An architectural approach towards the future internet of things // Uckelmann D., Harrison M., Michahelles F. Architecting the Internet of Things. USA, NY: Springer, 2011.

12. Wang L., Xu L., Bi Z., Xu Y. Data filtering for RFID and WSN integration // IEEE Trans. Ind. Informat. 2014. Vol. 10. No. 1.

13. Internet of Things Global Standards Initiative [Электронный ресурс]. – Режим доступа : http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (дата обращения: 20.05.2021).

14. Алгулиев, Р. Ш. Интернет вещей / Р. Ш. Алгулиев, Р. Ш. Махмудов // Информационное общество. 2013. № 3. С. 42–48.

15. L. A. Grieco, M. B. Alaya, T. Monteil, K. K. Drira, Architecting information centric ETSI-M2M systems, in: IEEE PerCom, 2014.

16. R. H. Weber, Internet of things - new security and privacy challenges, Comput. Law Secur. Rev, Jan. 2010, Vol. 26, № 1, pp. 23–30.

17. H. Feng, W. Fu, Study of recent development about privacy and security of the internet of things, in: 2010 : International Conference on Web Information Systems and Mining (WISM), Sanya, 2010, pp. 91–95

18. R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Networks, 2013, Vol. 57, № 10, pp. 2266–2279.

19. S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 : 2nd International Conference on Wireless Communication, Vehicular Technology, Information

Theory and Aerospace and Electronic Systems Technology (VITAE), Chennai, India, 2011, pp. 1–5.

20. Y. Zhao, Research on data security technology in internet of things, in: 2013 : 2nd International Conference on Mechatronics and Control Engineering (ICMCE), Dalian, China, 2013, pp. 1752– 1755.

21. T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authentication for the internet of things, Ad Hoc Networks, 2013, Vol. 11. № 8, pp. 2710–2723.

22. M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutorials, 2013, Vol. 15, № 3, pp. 1389–1406.

23. R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Comput. Electrical Eng., 2011, Vol. 37, № 2, pp. 147–159.

24. W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Trans. Inf. Syst. Secur. (TISSEC), 2005, Vol. 8, № 2, pp. 228–258.

25. Z.-Q. Wu, Y.-W. Zhou, J.-F. Ma, A security transmission model for internet of things, Jisuanji Xuebao/Chin. J. Comput., 2011, Vol. 34, № 8, pp. 1351–1364.

26. Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini, Security, Privacy & Trust in Internet of Things: the road ahead, Computer Networks (Elsevier), 2015, Vol. 76, pp. 146–164.

27. J.-Y. Lee, W.-C. Lin, Y.-H.Huang, A lightweight authentication protocol for internet of things, in: 2014 : International Symposium on Next-Generation Electronics (ISNE), Kwei-Shan, 2014, pp. 1–2.

28. M. Turkanovi, B. Brumen, M. Holbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion, Ad Hoc Networks, 2014, Vol. 20, pp. 96–112.

29. N. Ye, Y. Zhu, R.-C. b. Wang, R. Malekian, Q.-M. Lin, An efficient authentication and access control scheme for perception layer of internet of things, Appl. Math. Inf. Sci., 2014, Vol. 8, № 4, pp. 1617–1624.

30. A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot targetdriven applications, Comput. Secur., 2013, Vol. 37, pp. 111–123.

31. J. Ma, Y. Guo, J. Ma, J. Xiong, T. Zhang, A hierarchical access control scheme for perceptual layer of iot, Jisuanji Yanjiu yu Fazhan, Comput. Res. Dev., 2013, Vol. 50, № 6, pp. 1267– 1275.

32. M. Ali, M. ElTabakh, C. Nita-Rotaru, FT-RC4: A Robust Security Mechanism for Data Stream Systems, Tech. Rep. TR-05- 024, Purdue University, Nov. 2005, pp. 1–10.

33. M. A. Hammad, M. J. Franklin, W. Aref, A. K. Elmagarmid, Scheduling for shared window joins over data streams, in : Proceedings of the 29th International Conference on Very Large Data Bases (VLDB), Berlin, Germany, 2003, pp. 297–308.

34. S. Papadopoulos, Y. Yang, D. Papadias, Continuous authentication on relational data streams, VLDB Journal, 2010, Vol. 19, № 1, pp. 161–180.

35. S. Papadopoulos, G. Cormode, A. Deligiannakis, M. Garofalakis, Lightweight authentication of linear algebraic queries on data streams, in : Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data (SIGMOD), New York, USA, 2013, pp. 881–892.

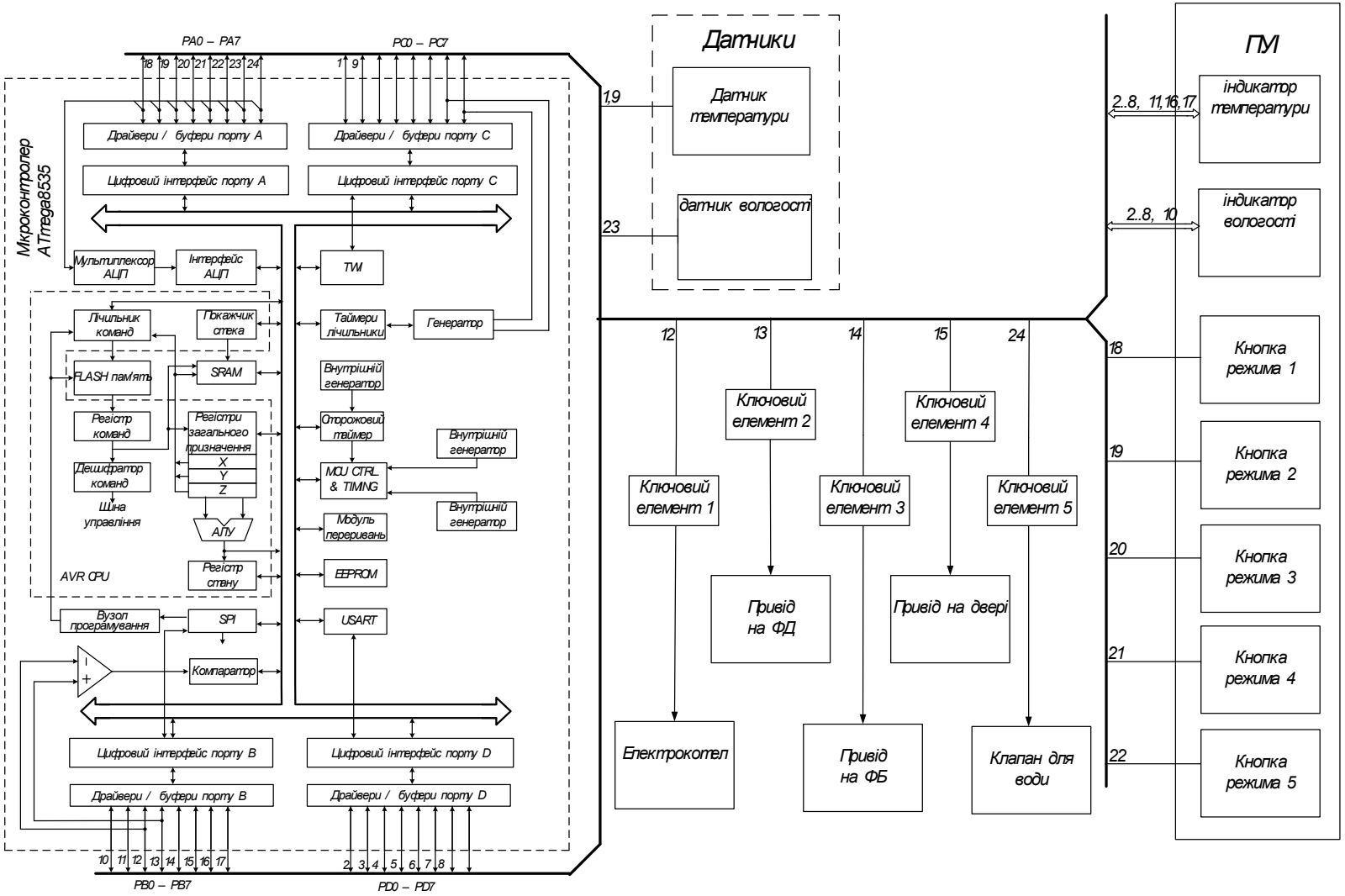
36. A. Cherkaoui, L. Bossuet, L. Seitz, G. Selander, R. Borgaonkar, New paradigms for access control in constrained environments, in: 2014 : 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), Montpellier, 2014, pp. 1–4.

37. L. Veltri, S. Cirani, S. Busanelli, G. Ferrari, A novel batchbased group key management protocol applied to the internet of things, Ad Hoc Networks, 2013, Vol. 11, № 8, pp. 2724–2737.

Додатки

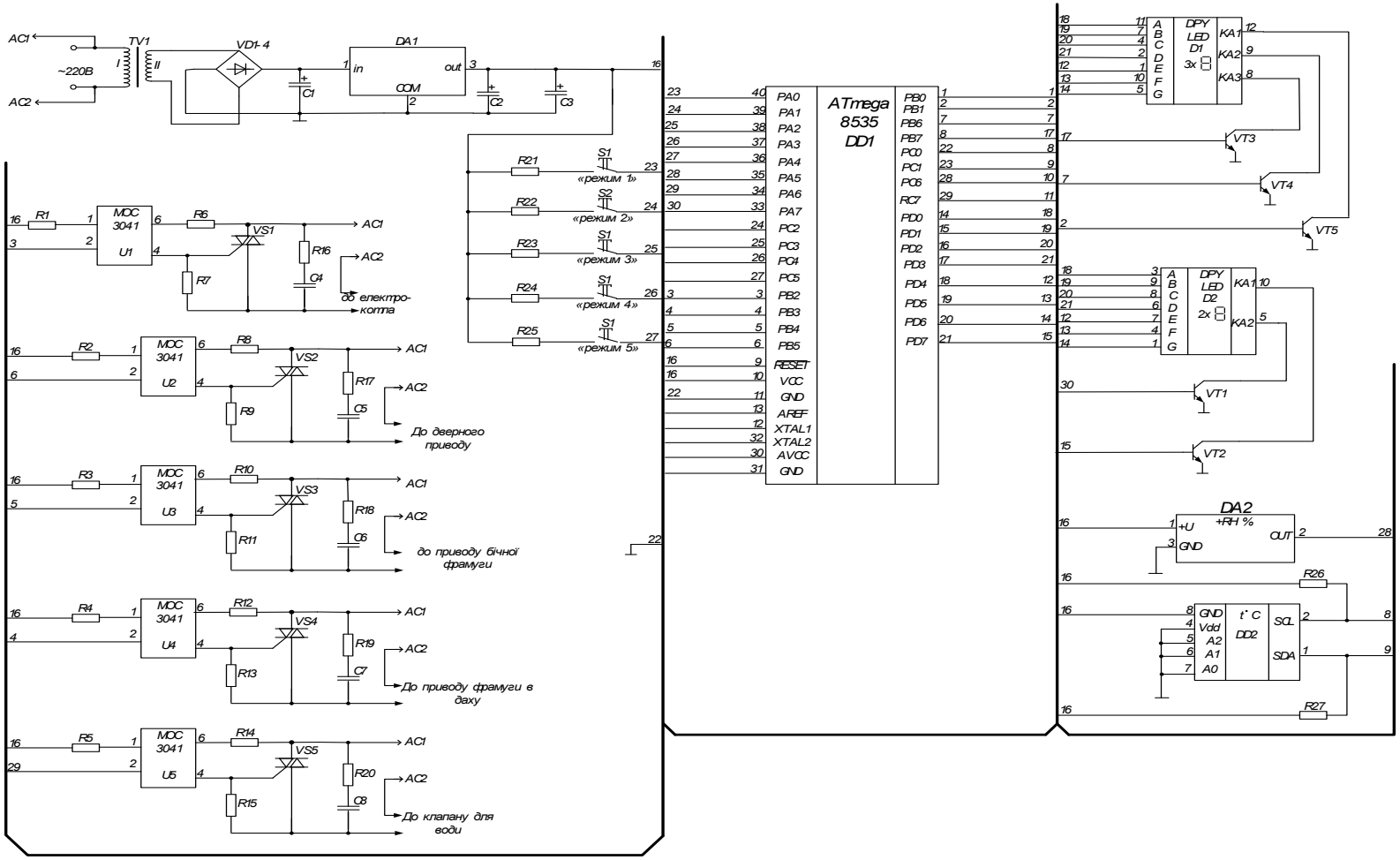
Додаток А

Функціональна схема IoT-рішення



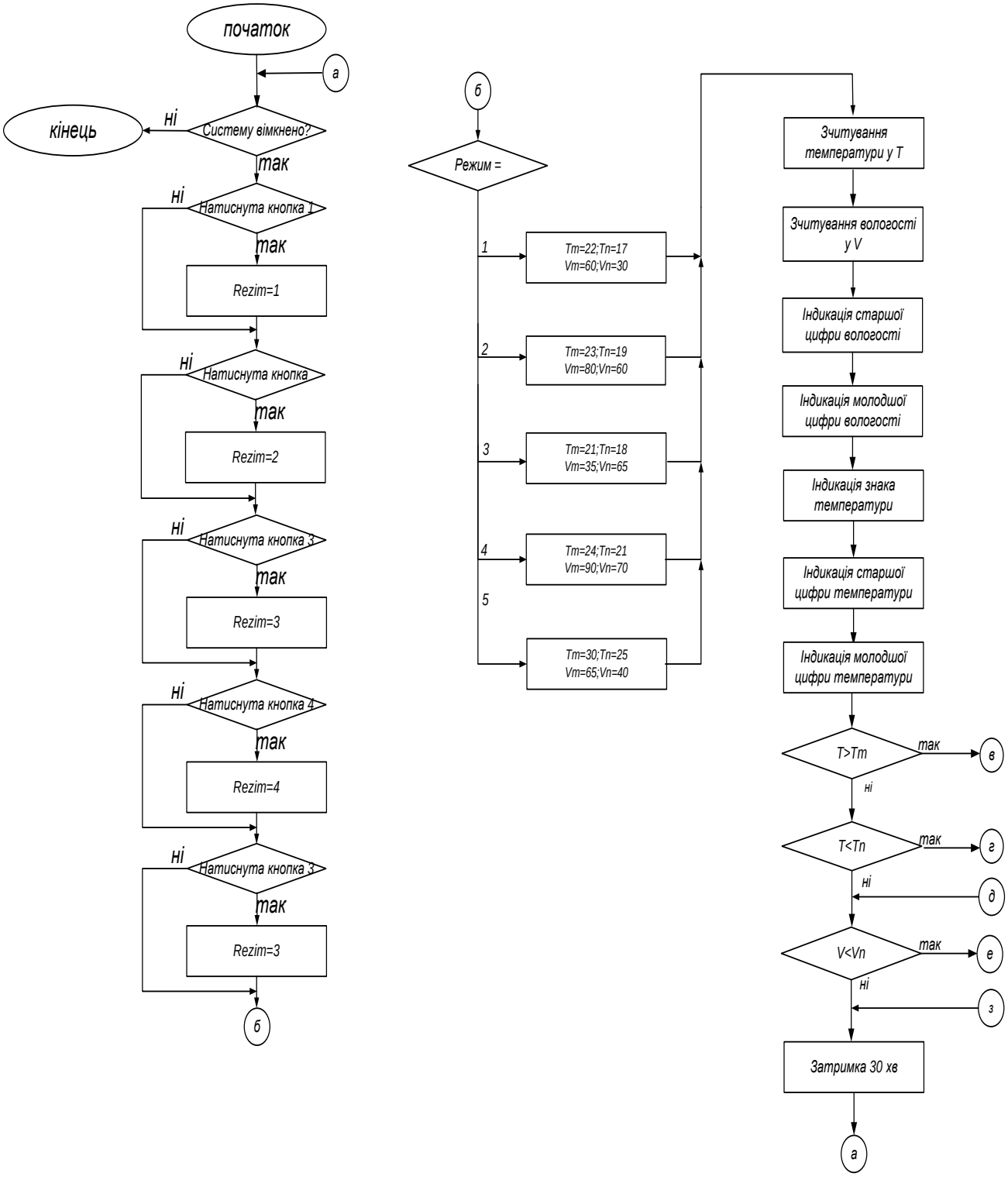
Додаток Б

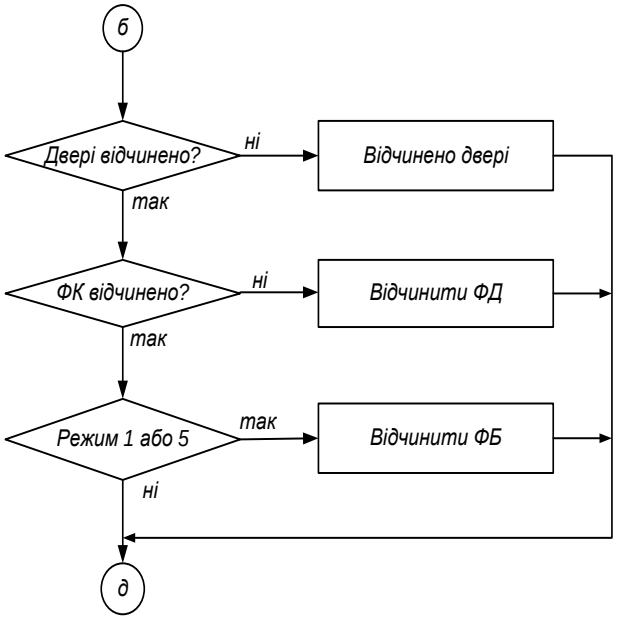
Електрична принципова схема IoT-рішення

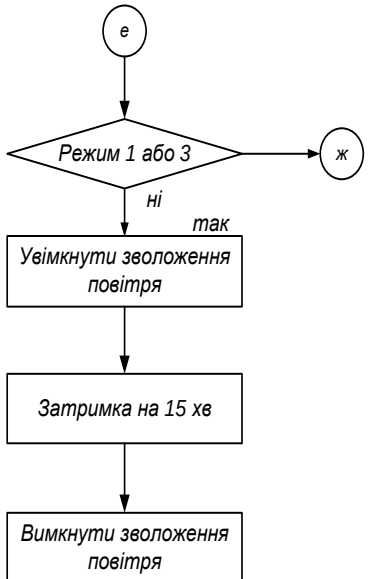


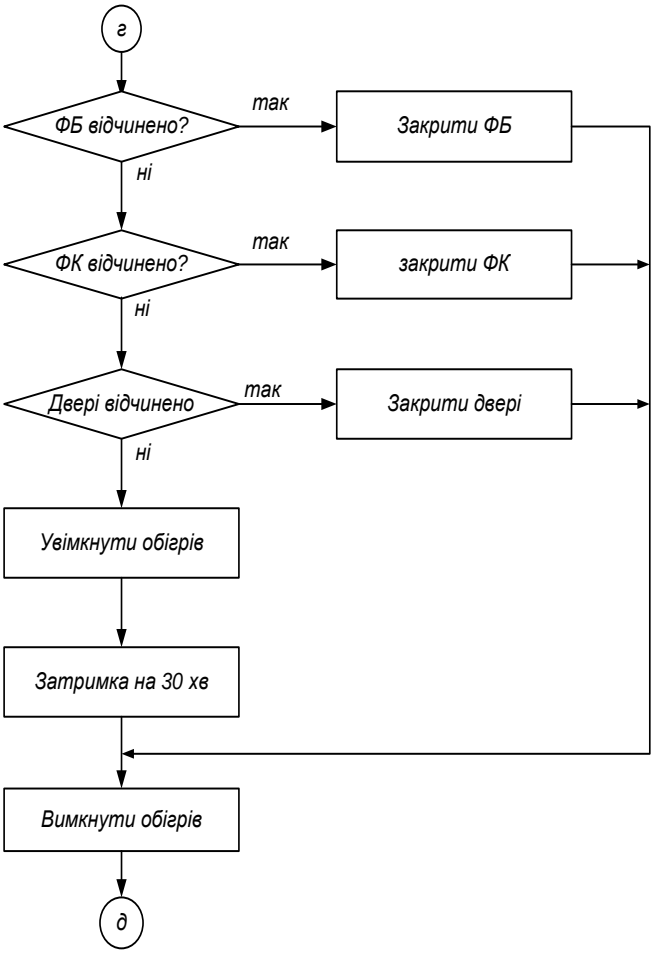
Додаток В

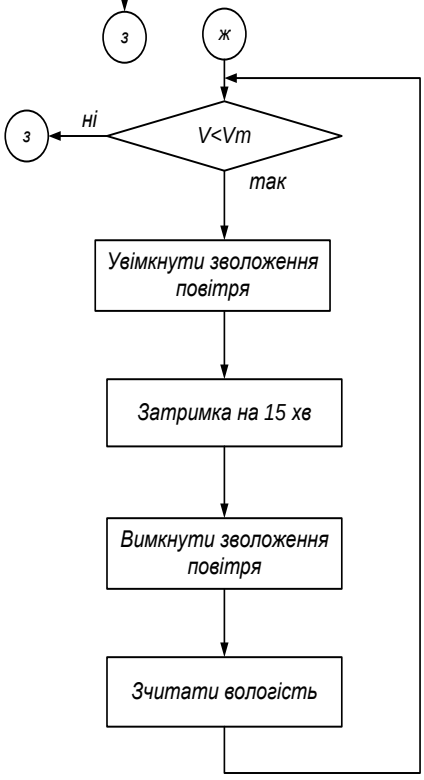
Блок-схема алгоритму системи агрострахування на основі даних з IoT



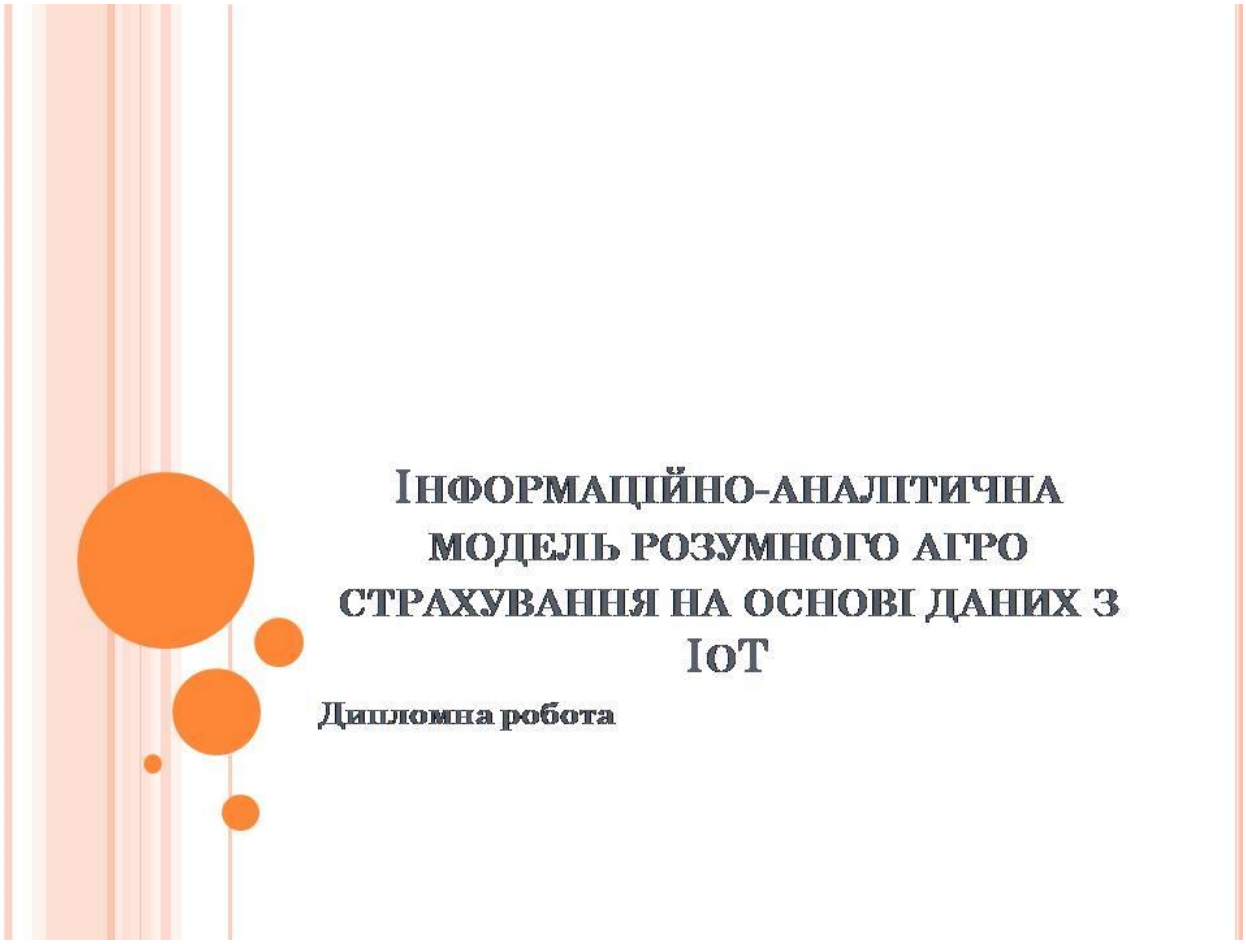

б
Двері відчинено?
ні
Відчинено двері
так
ФК відчинено?
ні
Відчинити ФД
так
Режим 1 або 5
так
Відчинити ФБ
ні
д


е
Режим 1 або 3
ж
ні
так
Увімкнути зволоження повітря
Затримка на 15 хв
Вимкнути зволоження повітря
з


г
ФБ відчинено?
так
Закрити ФБ
ні
ФК відчинено?
так
закрити ФК
ні
Двері відчинено
так
Закрити двері
ні
Увімкнути обігрів
Затримка на 30 хв
Вимкнути обігрів
д


ж
з
ні
V<Vm
так
Увімкнути зволоження повітря
Затримка на 15 хв
Вимкнути зволоження повітря
Зчитати вологість

Додаток Г


ІНФОРМАЦІЙНО-АНАЛІТИЧНА МОДЕЛЬ РОЗУМНОГО АГРО СТРАХУВАННЯ НА ОСНОВІ ДАНИХ З IoT
Дипломна робота

Актуальність теми.

- Інтернет речей (IoT - Internet of Things) є сучасною концепцією, що має на меті об'єднання об'єктів, «речей», в єдину всесвітню мережу, яка дозволяє речам бути розумними для взаємодії як з один з одним, так і з людиною в будь-який час і в будь-якому місці. На сьогоднішній день число пристроїв, підключених до мережі, перевищує число всіх жителів планети і продовжує стрімко збільшуватися, що піднімає питання про присвоєння кожному об'єкту унікальної адреси, забезпечення конфіденційності і безпеки при передачі даних. Незважаючи на це, до цих пір немає загальноприйнятого методу ідентифікації речей, який би задовольняв всім вимогам як для існуючих пристроїв і додатків Інтернету речей, так і для знову створюваних.

Мета і завдання дослідження.

- Метою роботи є дослідження методів та засобів побудови інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.
- Для досягнення поставленої мети вирішуються наступні задачі:
- описати призначення і область застосування;
- навести технічні характеристики інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.;
- провести огляд існуючих рішень і обґрунтування вибору структури інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.;
- розробити та описати структурну та функціональну схеми проектованої інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.;
- здійснити вибір і обґрунтування окремих вузлів інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.;
- розробити і описати принципову схему та алгоритм керуючої програми;
- дослідити інформаційно-аналітичну модель розумного агро страхування на основі даних з IoT.

Об'єкт та предмет дослідження

- ***Об'єкт дослідження*** – технологія Інтернет речей.
- ***Предмет дослідження*** – розробка інформаційно-аналітичної моделі розумного агро страхування на основі даних з IoT.

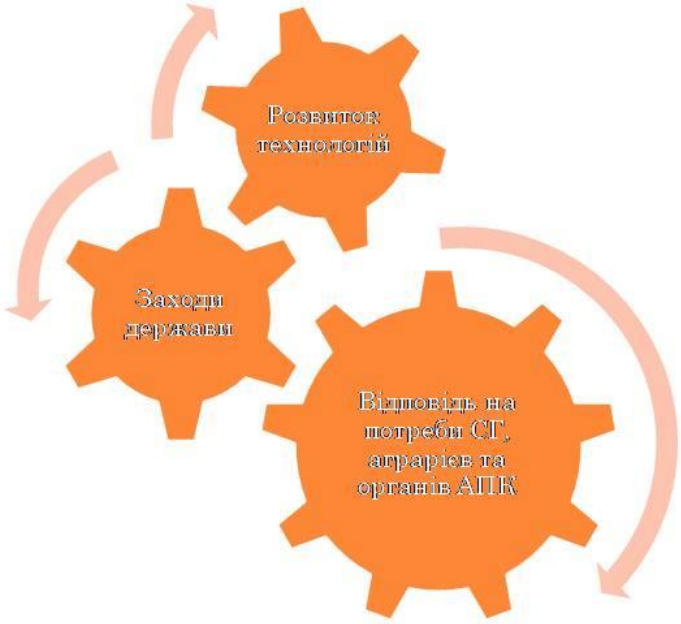
Наукова новизна та практичне отриманих результатів

- ***Наукова новизна отриманих результатів.***
- 1) Запропоновано комплексне рішення для комплексного моніторингу приміщень за допомогою технології Інтернет речей.
- 2) Розроблена інформаційно-аналітична модель розумного агро страхування на основі даних з IoT.
- ***Практичне значення отриманих результатів.*** Результати дослідження можуть бути впроваджені у рамках реального приміщення для комплексного моніторингу приміщень за допомогою технології Інтернет речей.

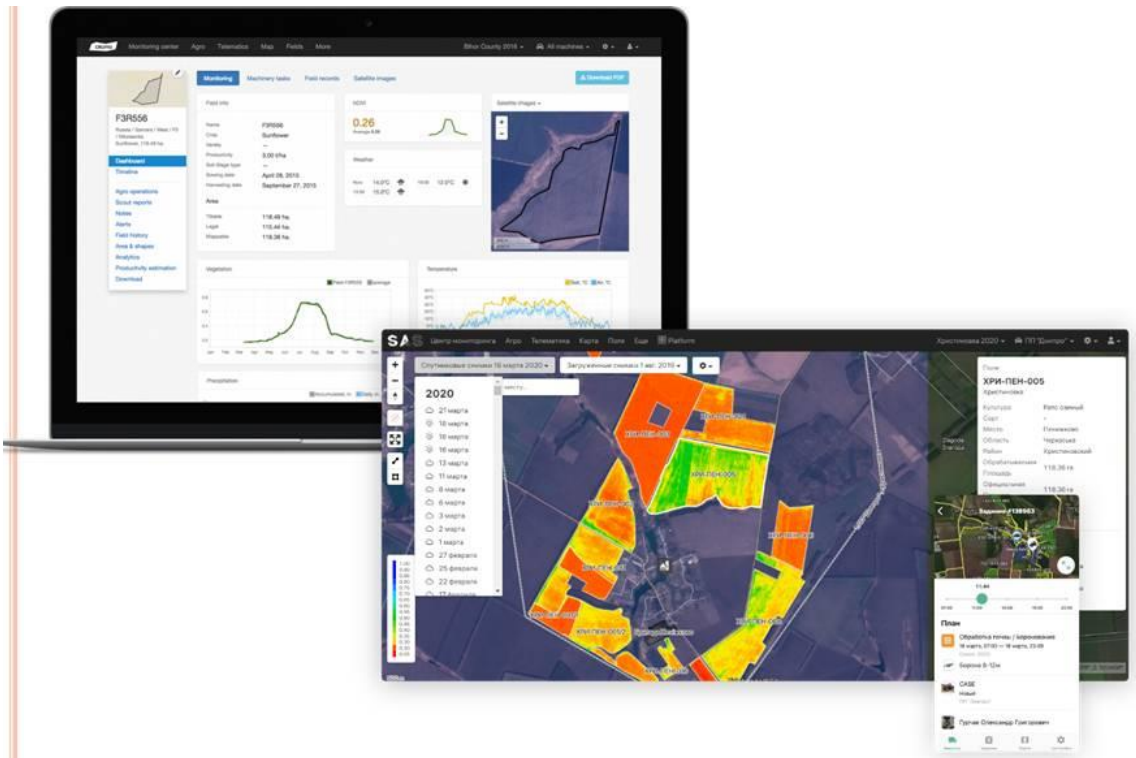
ПОСТАНОВКА ЗАДАЧІ ТА АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

Дистанційний моніторинг	• Методи страхової експертизи • Розробка індексних страхових продуктів
Маркетплейси	• Вбудовування пропозиції зі страхування в платформи, де пропонуються різні послуги для аграріїв • Особистий кабінет аграрія, в т. ч. щодо отримання субсидій та здержання виплат
Big Data	• Інтеграція з системами держорганів • Можливість використання в актуарних розрахунках • Адаптація страхових продуктів
Роботизація	• Можливість використання для фіксування страхових подій • Поява кіберризиків в області АПК (Приклад: неправильне розпорошення гербіциду - втрата врожаю)

- Області цифровізації АПК

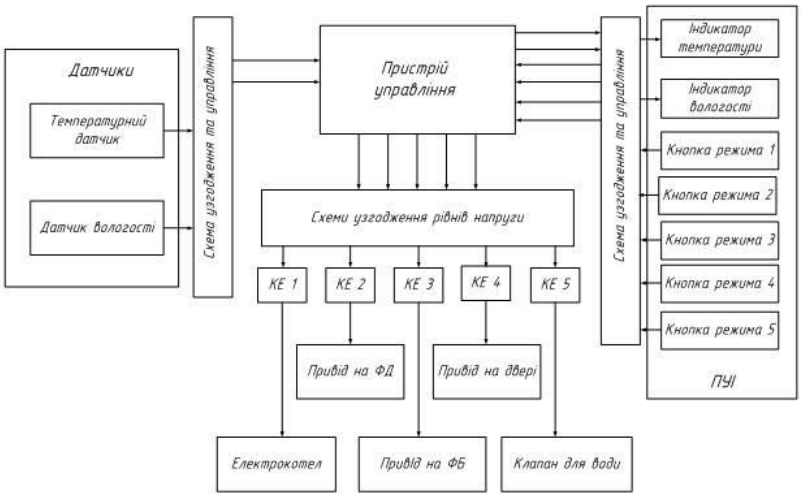


- **Драйвери впливу на розвиток цифровізації у агрострахуванні**



- Огляд систем автоматизації

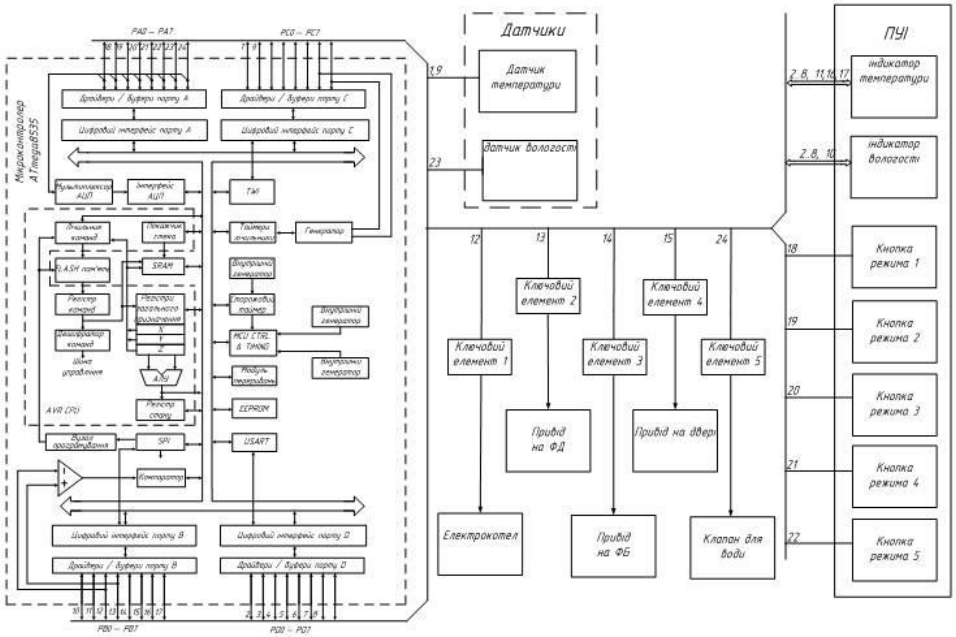
РОЗРОБКА АРХІТЕКТУРИ ПРОЕКТУ ІОТ-РІШЕННЯ



- **КЕ – ключовий елемент; ФБ – фрамуга бокова; ФД – фрамуга в даху; ПУІ – пульт управління та індикації**
- **Рисунок – Структурна схема системи управління приміщення 2–х поверхового котеджу аграрного призначення, що стоїть окремо з урахуванням технології Інтернет речей**

- **Схема взаємодії всіх складових системи управління приміщення 2– х поверхового котеджу аграрного призначення, що стоїть окремо з урахуванням технології Інтернет речей**

РОЗРОБКА ФУНКЦІОНАЛЬНОЇ СХЕМИ

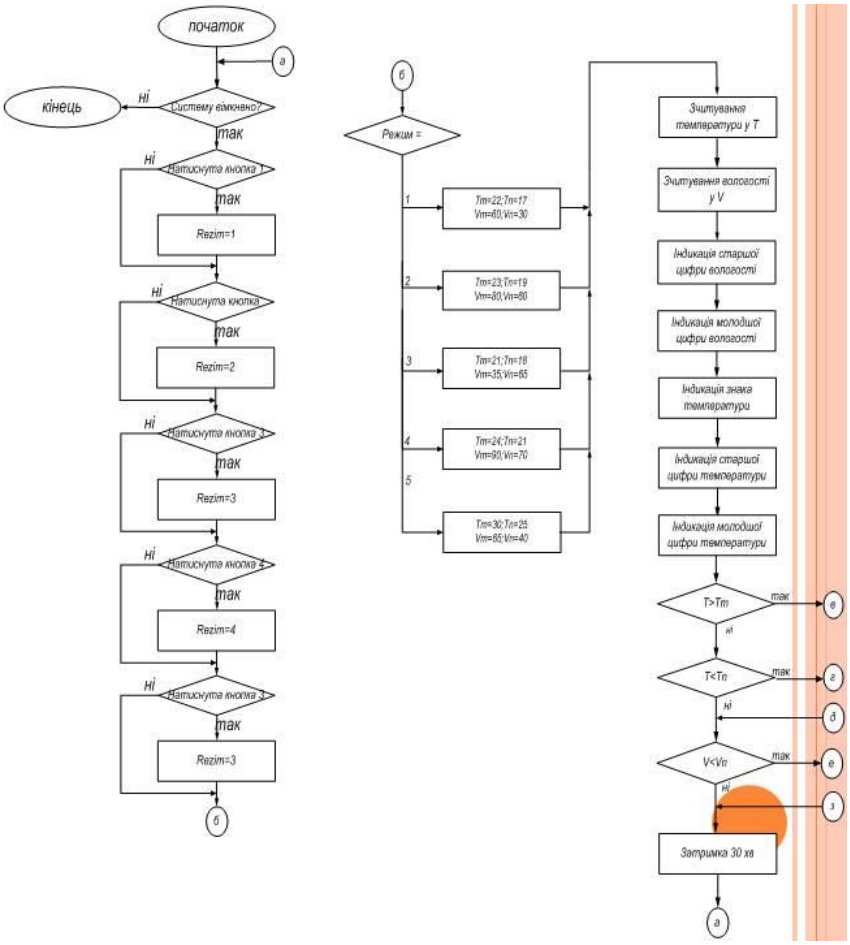


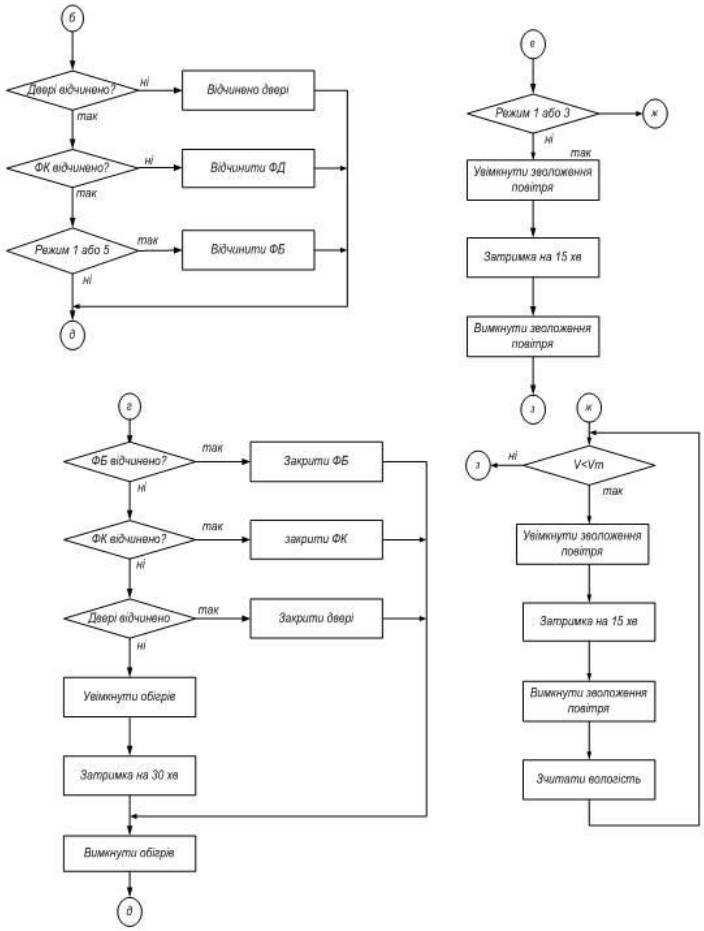
- **Функціональна схема**

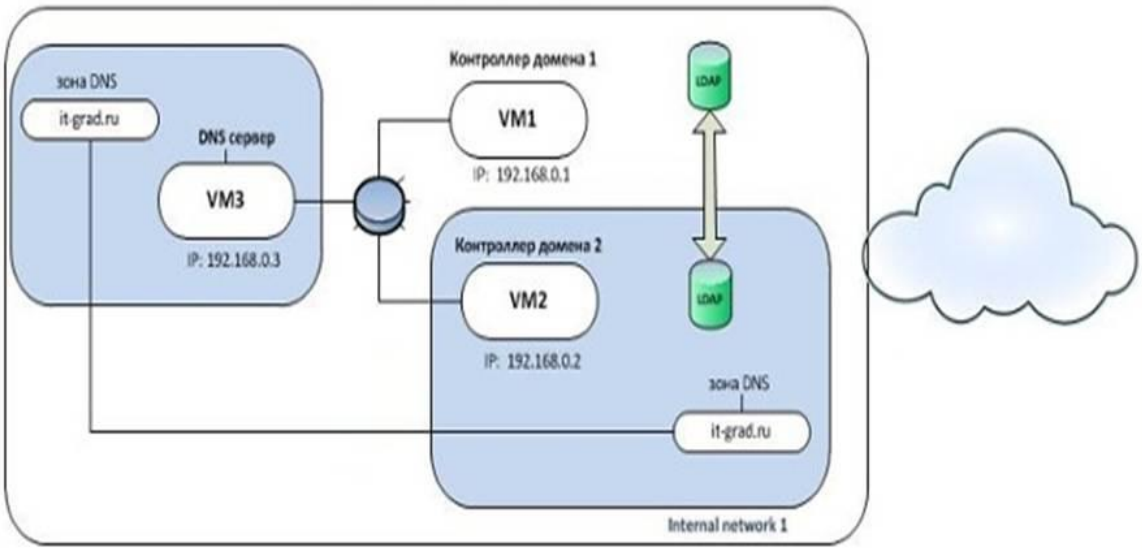
РЕАЛІЗАЦІЯ АРХІТЕКТУРИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ МОДЕЛІ

- **Інформаційно-аналітична модель розумного агро страхування на основі даних з IoT призначена для створення комфортних умов, захисту матеріальних цінностей, людей, що знаходяться у комплексі аграрного призначення, що захищається, забезпечує виконання наступних функцій:**
- **формування сигналів тривог;**
- **забезпечення мікроклімату;**
- **надання сповіщення про наявність і місце виникнення тривожної / аварійних ситуацій на пульт сигналізації і зовнішній світлозвуковий оповіщувач;**
- **закриття кульових кранів подачі гарячої та холодної води;**
- **автоматичний контроль стану елементів системи і її складових частин;**
- **надання сповіщення про тривожну / аварійну ситуацію в охоронні структури через термінал;**
- **надання сповіщення про тривожну / аварійну ситуацію, інших подій дзвоном і за допомогою SMS власнику і / або в охоронні структури**

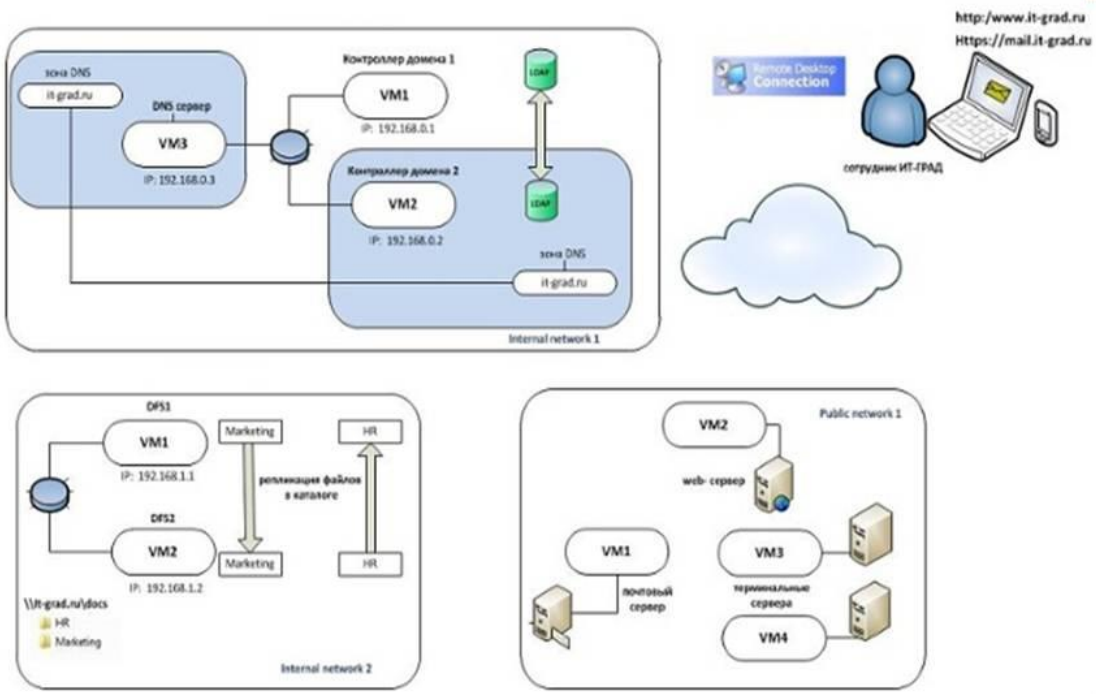
- Алгоритм роботи системи розумного агро страхування на основі даних з IoT







- Фрагмент ізольованої підмережі в хмарі



- Фрагмент хмари з двома ізольованими мережами і мережею публічного доступу

ВИСНОВКИ

- В дипломній роботі проведено дослідження системи розумного агро страхування на основі даних з IoT. При вивченні концепції інтелектуальної системи управління будівлею були сформульовані основні вимоги і характеристики її реалізації. Серед існуючих в світі на сьогоднішній день реалізацій ті, які найбільш повно задовольняють вимогам концепції інтелектуального комплексного моніторингу приміщень інтегровані до системи управління будівлею.
- Згідно до проведеного дослідження варто відзначити, що системи розумного агро страхування на основі даних з IoT за всіма показниками перевершує систему комплексного моніторингу приміщень за допомогою технології Nest, що говорить про високу якість системи комплексного моніторингу приміщень та можливість впровадження її в реальну роботу за потребою.

Дякую за увагу!