Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Гончарова Станіслава Олександровича*

академічної групи *125м-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Нейромережеві методи самотестування для підвищення рівня захищеності АСУ водопостачанням*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В.			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Гончарову С.О.*** **академічної групи** ***125м-17-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1]

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

на тему ***Нейромережеві методи самотестування для підвищення рівня захищеності АСУ водопостачанням***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.2018 № 2025-л_____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***автоматизована система керування процесами водопостачання***

Предмет досліджень ***методи забезпечення інформаційної безпеки автоматизованих систем керування процесами водопостачання***

Мета ***підвищення рівня захищеності автоматизованих систем керування процесами водопостачання***

Вихідні дані для проведення роботи ***результати та матеріали з виробничої та преддипломної практик***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***висновок про можливість використання методів інтелектуального аналізу даних, як засобу підвищення рівня інформаційної безпеки системи***

Практична цінність ***застосування рекомендованих комплексу заходів захисту автоматизованої системи керування процесами водопостачання, аналіз доцільності використання запропонованих засобів захисту інформації***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Закону України «Про інформацію», НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, НД ТЗІ 3.7-001-99

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***підвищення рівня захищеності автоматизованої системи керування процесами водопостачання та економічна доцільність впровадження запропонованих заходів і засобів захисту***

Соціальний ефект ***забезпечення захисту критичної інформації у системах масового споживання та життєзабезпечення суспільства***

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ Флоров С.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Гончаров С.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., 4 додатки, 29 джерел.

Об’єкт дослідження: автоматизована система керування процесами водопостачання.

Мета дипломної роботи: покращення рівня захищеності автоматизованих систем керування процесами водопостачання.

Результати роботи: аналіз стану захищеності систем водопостачання; проектні рішення щодо підвищення захищеності об’єкта досліджень; розглянуті основні підходи щодо реалізації послуг захисту від НСД автоматизованої системи керування процесами водопостачання; запропоноване використання інтелектуального аналізу даних, як складового елемента послуг безпеки.

Практичне значення роботи полягає в застосуванні рекомендованих мір та комплексу заходів захисту автоматизованої системи керування процесами водопостачання, аналізі доцільності використання запропонованих засобів захисту інформації.

Розроблені проектні рішення щодо підвищення рівня захищеності призначені для впровадження та використання у міському водоканалі.

МОДЕЛЬ ЗАГРОЗ, ФУНКЦІОНАЛЬНИЙ ПРОФІЛЬ, АВТОМАТИЗОВАНА СИСТЕМА КЕРУВАННЯ, ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ, ВОДОПОСТАЧАННЯ.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., 4 приложений, 29 источников.

Объект исследования: автоматизированная система управления процессами водоснабжения.

Цель дипломной работы: повышение уровня защищенности автоматизированных систем управления процессами водоснабжения.

Результаты работы: анализ защищенности систем водоснабжения; проектные решения по повышению уровня защищенности объекта исследований; рассмотрены основные подходы к реализации услуги защиты от НСД автоматизированной системы управления процессами водоснабжения; предложено использование интеллектуального анализа данных, как составного элемента услуг безопасности.

Практическое значение работы заключается в применении комплекса рекомендованных мер защиты автоматизированной системы управления процессами водоснабжения, анализе целесообразности использования предложенных средств защиты информации.

Разработаны проектные решения по повышению уровня защищенности предназначены для внедрения и использования в городском водоканале.

МОДЕЛЬ УГРОЗ, ФУНКЦИОНАЛЬНЫЙ ПРОФИЛЬ, АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ, ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ, ВОДОСНАБЖЕНИЕ.

ABSTRACT

Explanatory note: ___ p., __ fig., __ tab., 4 application, 29 sources.

The research object is an automated process control system of water supply.

The purpose of work consists in an increasing protection level of automated process control system of water supply.

Got results: a security analysis of water supply systems; designed solutions to improve the protection of the research object; the basic approaches to implementing security services against unauthorized access to an automated process control system of water supply; proposed the use of data mining, as an integral part of security services.

In the occupational health and safety section hazards when working with PC users were analyzed, engineering occupational health and safety activities for computer users were developed.

Design solutions designed to improve the level of protection designed for introduction and use in municipal company.

MODEL OF THREATS, FUNCTIONALITY PROFILE, AUTOMATED PROCESS CONTROL SYSTEM, DATA MINING, WATER SUPPLY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	–	автоматизована система;
АСУ	–	автоматизована система керування;
АСУ ТП	–	автоматизована система керування технологічним процесом;
ДСК	–	для службового користування;
ІБ	–	інформаційна безпека;
ІзОД	–	інформація з обмеженим доступом;
ІТ	–	інформаційні технології;
ІТС	–	інформаційно-телекомунікаційна система;
КЗЗ	–	комплекс засобів захисту;
ККД	–	коефіцієнт корисної дії;
ЗІ	–	захист інформації;
КСЗІ	–	комплексна система захисту інформації;
НСД	–	несанкціонований доступ;
НД ТЗІ	–	нормативний документ технічного захисту інформації;
ОС	–	обчислювальна система;
ПБ	–	політика безпеки;
ПЕОМ	–	персональна електронно-обчислювальна машина;
ПЗ	–	програмне забезпечення;
ПОВ	–	підйом і обробка води;
ПРВ	–	подача і розподіл води;
ТЗІ	–	технічний захист інформації.

ЗМІСТ

с.

ВСТУП

Водопровідні мережі й водоводи є спорудами у складі систем подачі й розподілу води сучасних населених пунктів і вміщають елементи з різним конструктивним устроєм, технічним ресурсом та мають складну топологію. Такі трубопровідні системи повинні задовольняти вимогам надійного забезпечення всіх споживачів розрахунковими витратами води з необхідним напором при найменших витратах на будівництво й експлуатацію не тільки самих трубопроводів, що входять до їх складу, але й гідравлічно пов’язаних із ними водопровідних споруд. Проблеми забезпечення надійної й ефективної роботи системи водопостачання пов`язані з тим, що вони працюють у надзвичайно складних умовах експлуатації, під впливом дії на них різноманітних факторів конструктивного, об`єктивного і суб`єктивного характеру. При цьому суттєво змінюються характеристики надійності й економічності всієї системи водопостачання.

Під системою водопостачання мається на увазі комплекс взаємопов'язаних споруд, призначених для водозабезпечення будь-якого об'єкта або групи об'єктів. Система водопостачання, що забезпечує водою окремі райони або групи населених пунктів, або групи промислових об'єктів, називається районної чи груповою системою водопостачання.

Централізована система водопостачання населеного пункту або промислового підприємства повинна забезпечувати прийом води з джерела, її кондиціонування (якщо це необхідно), транспортування і подачу до всіх споживачів під необхідним тиском. З цією метою в систему водопостачання повинні бути включені: водоприймальні споруди, призначені для отримання води з природних джерел; насосні станції що створюють напір для передачі води на очисні споруди, в акумулюючи ємкості або споживачам; споруди для обробки води резервуари і водонапірні башти, які є запасними і регулюючими ємкостями; водоводи і водорозподільні мережі призначені для передачі води до місць її розподілу і споживання. Послідовність розташування окремих споруд

системи водопостачання та їх складу можуть бути різними залежно від призначення, місцевих природних умов, вимог водоспоживачів або виходячи з економічних міркувань. Якщо очисні споруди та резервуари чистої води розташовані на досить високих відмітках місцевості, очищена вода може передаватися споживачеві по водоводах самопливом, тобто потреба в насосній станції другого підйому відпадає. При використанні підземних артезіанських вод, що не потребують кондиціонування, система водопостачання об'єкта спрощується за рахунок виключення очисних споруд.

Для правильного вибору системи та джерела водопостачання необхідно мати дані про водоспоживання, знати вимоги що пред'являються до якості води, мати відомості про тиск, під яким вона повинна подаватися споживачеві, знати характеристику наявних природних джерел в районі проектування. Значною мірою система водопостачання залежить від обраного джерела: його характеру (поверхневий або підземний), потужності, якості води, відстані, на яку він віддалений від споживачів [1].

Все різноманіття систем водопостачання можна класифікувати за такими основними ознаками:

– по виду використання природних джерел – водопроводи, які отримують воду з поверхневих джерел, з підземних джерел, і водопроводи змішаного живлення (при використанні різних видів вододжерел);

– за призначенням – водопроводи комунальні (міст, селищ), залізничні, сільськогосподарські, виробничі, які в свою чергу поділяються за галузями промисловості (водопроводи хімічних комбінатів теплових електростанцій, металургійних заводів тощо);

– за ознакою – локальні (одного об'єкта) та групові (чи районні) водопроводи, обслуговуючі групу об'єктів.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність проблеми

Україна має досить розвинені системи водопостачання й водовідведення. Побудовані в радянський час інфраструктурні об’єкти відрізнялися високою капіталомісткістю, досить високою надійністю, але при цьому при їх проектуванні закладалися надмірно високі нормативи витрати води (ощадливе водоспоживання не стимулювалося) і резерв потужності на перспективу росту водоспоживання. Це приводило до надмірних капітальних витрат, а побудовані системи були надлишково енерговитратними.

Але таке положення не позначалося на платежах населення, оскільки всі капіталовкладення здійснювалися з бюджетних коштів, а поточні витрати в значній мірі покривалися за рахунок підвищених тарифів для промислових споживачів. Завдання із забезпечення соціально–економічної й політичної стабільності в дев’яності роки минулого століття були ключовими проблемами цих країн. Сектор водопостачання й водовідведення відіграв практично у всіх країнах у цей час роль інституту соціальної допомоги держави населенню. Це виражалося в тому, що платежі населення в більшості країн не покривали навіть операційних витрат на функціонування систем водопостачання й водовідведення. Але й у силу важкого економічного становища бюджетних коштів на підтримку систем водопровідно–каналізаційного господарства (не говорячи вже про його розвиток) практично не виділялося. Такий стан справ привів до різкого падіння якості послуг водопостачання й водовідведення. Основні фонди практично не обновлялися, підвищилася аварійність. У багатьох містах вода стала поставлятися з перервами, перестали функціонувати спорудження по очищенню стічних вод. Спостерігається погіршення якості водопостачання й зниження надійності роботи технічних систем. Тому сьогодні необхідним є докорінне технічне відновлення об’єктів водопостачання й водовідведення, впровадження нових технологій, забезпечення природоохоронних заходів.

Надійність і безпека систем водопостачання та водовідведення є невід'ємним елементом національної безпеки країни. Майже 100% населення в містах користується системами централізованого водопостачання. Хвороби інфекційної або неінфекційної природи з легкістю проникнуть в будь-яке житло у разі ненадійності мереж та відсутності систем аналізу стану води. З іншого боку порушення водопостачання також є реальною загрозою. Разом с тим існуючий стан систем водопостачання на даний момент характеризується, як кризовий. Довжина мереж водопостачання в цілому по Україні з 1990 року зросла на 37 – 39%, а довжина аварійних мереж — в 6 разів. В 2013 році загальна довжина водогінних мереж становила 182 626,3 км, з них 36,4% або 66 462,5 км потребують негайної заміни. Зношення устаткування в системах централізованого водопостачання й водовідведення становить 63%. У середньому по Україні рівень втрат води в мережах централізованого водопостачання становить – 40,4%, з великим розкидом по регіонах – від 16% до 82%. Незадовільний технічний стан «побутових» мереж призводить до значних втрат питної води в мережах – до 16 млн. куб. м на добу.

Відсоток охоплення послугами водовідведення в цілому по Україні становить 66,7%, або менше ніж 50% для середніх міст і понад 75% для великих. У містах, де чисельність населення перевищує 100 тисяч людей, приблизно 80% зібраних стічних вод зазнають механіко-біологічному очищенню. У малих містах очищається близько 45% від загального обсягу зібраних стічних вод. Загальна довжина мереж водовідведення в 2008 році в цілому по країні становила 50 756,5 км, з них вимагало негайної заміни – 17 269,2 км, або 34%. У ЖКГ експлуатується 25% основних фондів України, зайнято 5% працездатного населення. При цьому в аварійному стані перебуває 30% водопровідних і 27% каналізаційних мереж. На ліквідацію аварій витрачається в 2–3 рази більше засобів, ніж на профілактику або заміну труб у мережах [2].

1.2 Технологічний процес водопостачання міста

Прямоточна система застосовується для господарсько-питного та протипожежного водопостачання у містах. У деяких випадках застосовується і для виробничо-технічного водопостачання.

На рисунку 1.1 наведена схема взаємозв'язку основних елементів у прямоточною системі водопостачання:

1 – водозабір;

2.1 – насосна станція 1-го підйому;

2.2 – насосна станція 2-го підйому;

2.3 – насосна станція 3-го підйому;

3.1 – очисні споруди природної води;

3.2 – очисні пристрої для забруднених стоків;

4.1 – резервуар чистої води;

5 – водоводи;

6 – водонапірна вежа (резервуар);

7.1 –7.6 – споживачі води;

8 – водопровідна мережа;

9 – мережа трубопроводів для збору відпрацьованої води;

10 – водоохолоджувальний пристрій [3, 4].

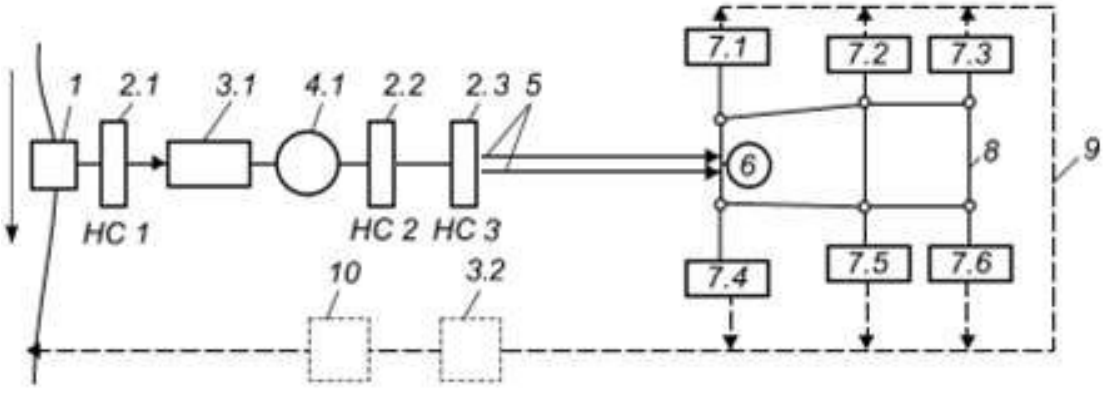

Рисунок 1.1 – Схема прямоточної системи водопостачання

При роботі цієї системи вода забирається з джерела за допомогою водозабірного пристрою 1 і подається насосами насосної станції 1 –го підйому (НС 1) на очисні споруди 3.1. Тут зазвичай вода йде самопливом. Очищена до необхідної якості вона збирається в резервуарі очищеної води 4.1. Звідси насосами насосної станції 2–го підйому (НС 2) та 3–го підйому (НС 3) вода по водоводах 5 подається до споживачів. З водоводів вода потрапляє у водопровідну мережу 8 і подається споживачам 7.1–7.6. Приєднана до мережі регулююча ємність 6 дозволяє згладжувати вплив піків водоспоживання на роботу насосів НС 3. Вона може бути встановлена в будь –якій точці водопровідної мережі. Вся відпрацювала вода скидається в джерело нижче (за течією) місця забору води. При необхідності ця вода очищається і охолоджується перед скиданням. У цьому випадку в системі передбачаються пристрої 3.2 і 10 [5].

АСУ ТП являють собою вищий етап автоматизації водопровідних споруд і покликані забезпечувати оптимальне ведення технологічних процесів водопостачання. У технологічному процесі водопостачання можна виділити два підпроцеса – підйом і обробку води, подачу і розподіл води. Відповідно до цього під АСУ ТП водопостачання слід розуміти комплекс систем, що складається з:

– АСУ ТП підйому і обробки води (АСУ ТП ПОВ), що здійснює управління насосними станціями 1–го підйому і водоочисними спорудами;

– АСУ ТП подачі і розподілу води (АСУ ТП ПРВ), що охоплює резервуари чистої води, насосні станції 2–го і наступних підйомів, водопровідні мережі.

Основними функціями АСУ ТП є:

1 Централізований контроль та облік стану технічного об’єкту та діагностика технологічного процесу.

2 Визначення раціонального режиму роботи.

3 Визначення режиму роботи у разі надзвичайних ситуацій у системах водопостачання (аварія, відхилення показників технологічного процесу від норми тощо).

Функції АСУ технічного об’єкту підсистемі ПОВ забезпечуються наступним комплексом завдань:

1) контроль значень технологічних параметрів (якості вихідної води, якості води на очисних спорудах, витрати води через очисні споруди, витрати води на власні потреби, витрати електроенергії станцій 1-го підйому, стану насосних агрегатів станції 1-го підйому);

2) вимірювання, відображення та реєстрація технічних параметрів та показників стану обладнання;

3) виявлення, оперативне відображення і сигналізація відхилень значень технологічних параметрів від встановлених меж;

4) виявлення, оперативне відображення і сигналізація про аварійні стани (при виникненні аварії).

У підсистемі ПРВ ця функція реалізується тим же комплексом завдань, але для інших значень технологічних параметрів:

– подачі води по водоводах;
– подачі води по станціях;
– напору на виході станції;
– рівня води в резервуарах;
– витрати електроенергії станції;
– стану насосних агрегатів станції;
– тиску в контрольних точках мережі.

Автоматичне управління кожної з насосних станцій та установок, які входять в систему подачі і розподілу води, слід передбачати з урахуванням її взаємодії з іншими насосними станціями системи (в тому числі загальносистемними і локальними станціями підкачки), а також з регулюючими ємкостями та регулюючими пристроями на водоводах і мережі. При цьому слід контролювати зміну подачі води нерегулюючими насосами (в результаті їх

саморегулювання) з тим, щоб вони не виходили за межі допустимого діапазону кожного з насосів. В необхідних випадках слід обмежити неприпустиме збільшення подачі води дроселюванням, а неприпустиме її зниження – рециркуляцією. Автоматичне управління роботою систем, як єдиного цілого, має забезпечити подачу необхідної добової витрати води при мінімальних сумарних витратах потужності всіма спільно працюючими насосами, забезпечення вільних напорів в мережі не нижче необхідних і зниження до можливого мінімуму надлишкових вільних напорів, що викликає збільшення витрат води внаслідок витоків та нераціонального витрачання.

Система повинна забезпечувати подачу води з мінімально можливими енергетичними витратами на одиницю поданого об’єму води, не допускаючи перевантаження окремих агрегатів, роботи їх в зоні низьких ККД, в зонах помпажу і кавітації [6].

1.3 Характеристика об’єкту інформаційної діяльності

Підприємство з водопосточання являється крупним виробничим підприємством з рядом технологічних процесів, пов’язаних з виробництвом та транспортуванням питної води споживачам.

Діяльність підприємства в першу чергу спрямована на цілодобове забезпечення питною водою споживачів міста з прилеглими територіями для господарчо–побутових потреб та пожежогасіння, транспортування стічних вод та їх очистку, експлуатацію водопровідних і каналізаційних мереж і споруд.

Найбільш крупними і важливими об’єктами підприємства залишаються Кайдакська та Ломовська насосно–фільтрувальні станції, водопровідні насосні станції перекачки (10 станцій), станції підкачки холодної води (47 станцій), Центральна, Лівобережна та Південна станції аерації, також каналізаційні насосні станції (52 станції).

Забезпечення міста питною водою здійснюється з трьох джерел водопостачання. На теперішній час підприємство має на своєму балансі більш 2,0 тис.км. водопровідних магістральних мереж та приблизно 1,5 тис.км. каналізаційних мереж [7].

Вхід на територію підприємства в робочі дні та часи вільний, в’їзд машин на територію обмежений (лише для співробітників та за домовленістю), периметр закладу огороджений та охороняється у неробочий час.

В якості об’єкту інформаційної діяльності розглядається АСУ керування технологічним процесом водопостачання міста. Автоматизована система систем водопостачання відноситься до АС 3-го класу – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності [8], через наявність виходу у незахищену мережу Інтернет.

Функціонально АС являє собою обчислювальний комплекс, який створений на базі розподіленої мережі ЕОМ призначеної для обробки інформацій.

1.4 Загальна характеристика об’єкту

В АС передбачений багатокористувачевий режим роботи. При цьому користувачі наділені різними правами доступу до інформації, що оброблюється в АС.

Інформація зберігається на сервері. Користувачі отримують доступ до інформації шляхом використання клієнт–серверного програмного забезпечення.

Організаційна структура підприємства представлена на рисунку 1.2.

Рисунок 1.2 – Організаційна структура підприємства

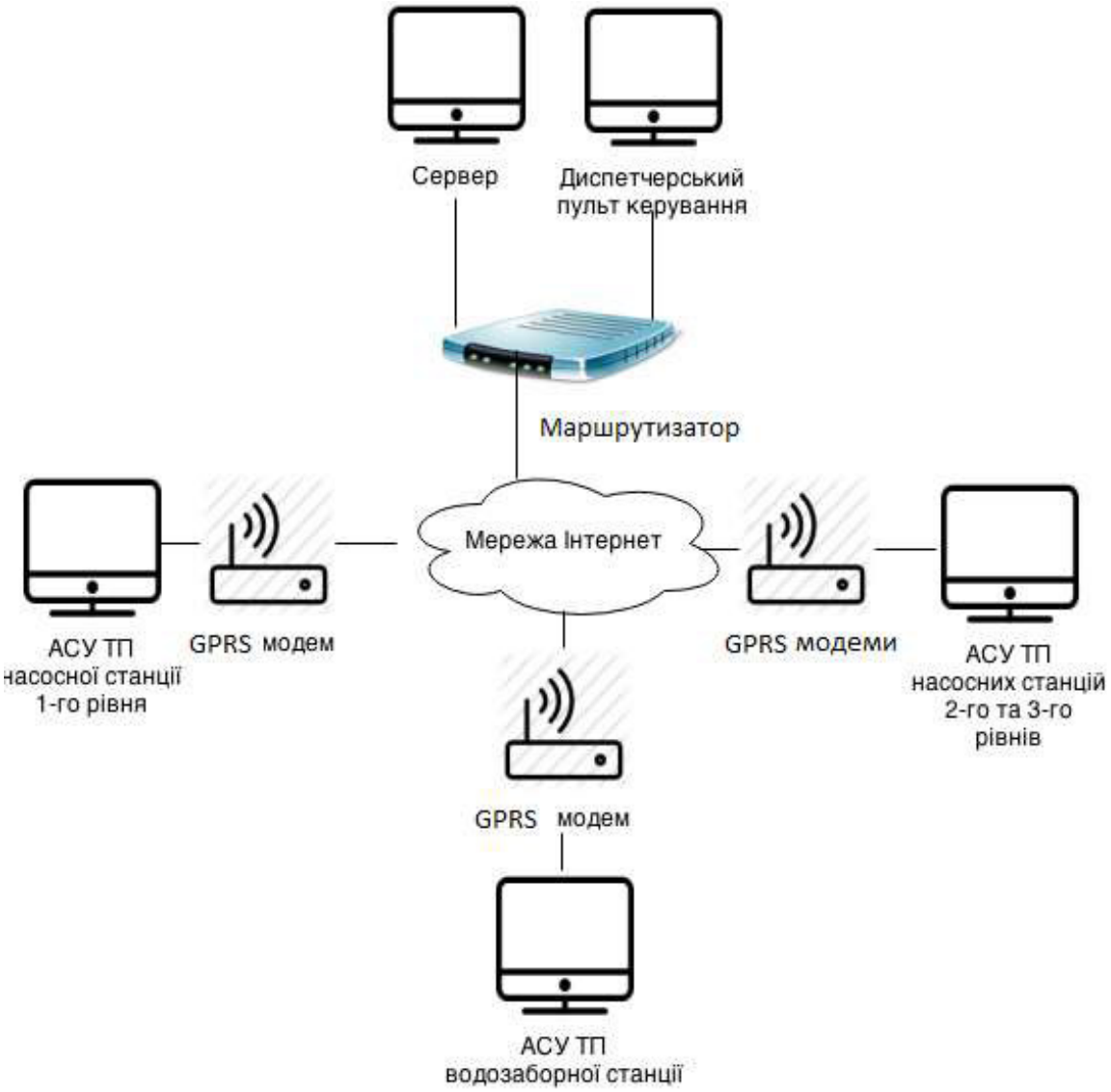

Рисунок 1.3 – Логічна схема АС

Комп’ютери АС об’єднані в єдину віртуальну мережу, через мережу Інтернет. Схема АС зображена на рисунку 1.3.

Система складається с АСУ ТП насосних та водозабірних станцій з клієнтським програмним забезпеченням, АРМ диспетчера та серверу. По відношенню до вказаних об’єктів реалізований набор організаційних та режимних мір захисту.

До складу технічних засобів АСУ входять:

– серверне обладнання;
– робоча станція диспетчера;
– ЕОМ керування технологічним процесом
– мережеве обладнання.

Фізично мережа має архітектуру «зірка». З’єднання організоване за допомогою кабельної системи «Вита пара». Протокол передачі даних в АС – TCP/IP. За логічною структурою АС має структури мережі з виділеним сервером.

Використовувана операційна система серверу – Windows Server 2008 R2 Enterprise.

Операційна система робочих місць операторів – Windows XP SP2.

Прикладне ПЗ – Автоматизована система «MasterEnergy».

1.5 Характеристики інформації та технологія її оброблення

У АС циркулює наступна інформація:

– інформація стану технічного об’єкту системи підйому і обробки води (стану насосних агрегатів станції 1-го підйому, роботи фільтрів водозбірної системи, витрати води через очисні споруди, інформація про аварійний стан);

– діагностична інформація технологічного процесу системи підйому і обробки води (характеристики якості вихідної води, якості води на очисних спорудах, витрати води через очисні споруди);

– керувальні команди системи підйому і обробки води;

– інформація стану технічного об’єкту системи подачі і розподілу води (стану насосних агрегатів станції 2-го і 3-го підйомів, витрати електроенергії станції, стану насосних агрегатів станції, тиску в контрольних точках мережі, інформація про аварійний стан);

– діагностична інформація технологічного процесу системи подачі і розподілу води (подачі води по водоводах, подачі води по станціях, напору на виході станції, рівня води в резервуарах);

– керувальні команди системи подачі і розподілу води;

– автентифікаційна інформація (логін та пароль).

Найвищий гриф секретності інформації, циркулюючої на об’єкті – для службового користування. Об'єм інформації з найвищим грифом секретності – незначний. Причина категорювання: первинне. Встановлена категорія: IV [9].

Технологія обробки інформації в АС дозволяє виконувати над інформацією в електронному вигляді наступні дії: створення, перегляд, редагування, друк, зберігання та видалення. Виконуються ці операції програмними та апаратними засобами АС.

Редагування інформації на відбувається авторизованим користувачем програмними засобами робочої станції через мережу Інтернет (не залежно від того чи виконується доступ з локальної мережі чи з глобальної мережі Інтернет), відповідно до його повноважень за протоколом HTTPS по незахищеному каналу мережі Інтернет.

Усі інформаційні ресурси зберігаються на сервері на території підприємства. Видалення інформації може бути виконано авторизованим вповноваженим користувачем (користувачем який створив інформацію чи має схожі права, адміністратором).

Класифікація інформації за рівнем доступу та місця її обробки та зберігання подані у таблиці 1.1.

Користувачі відповідно до своїх прав та службових обов’язків повинні мати відповідні навички та знати про наслідки порушення технічних правил та правил безпеки щодо використання АС.

Таблиця 1.1 – Класифікація інформації за рівнем доступу

Інформація	Вид	Місце обробки	Місце зберігання
Інформація стану технічного об’єкту системи ПОВ	Відкрита	АСУ ТП ПОВ, Диспетчерський пульт	Сервер
Діагностична інформація технологічного процесу системи ПОВ	Відкрита	АСУ ТП ПОВ Диспетчерський пульт	Сервер

Продовження таблиці 1.1

Інформація	Вид	Місце обробки	Місце зберігання
Керувальні команди системи ПОВ	ІЗоД	АСУ ТП ПОВ, Диспетчерський пульт	Сервер
Інформація стану технічного об’єкту системи ПРВ	Відкрита	АСУ ТП ПРВ, Диспетчерський пульт	Сервер
Діагностична інформація технологічного процесу системи ПРВ	Відкрита	АСУ ТП ПРВ, Диспетчерський пульт	Сервер
Керувальні команди системи ПРВ	ІЗоД	АСУ ТП ПРВ, Диспетчерський пульт	Сервер
Автентифікаційна інформація	ІЗоД	Диспетчерський пульт	Сервер

Порядок доступу до програмних засобів та компонентів АС користувачам різних категорій розробляється та надається адміністратором, і затверджується керівником підприємства.

Встановлені правила повинні відповідати нормативним та розпорядчим документам з питань захисту інформації в АС.

Видача персональних ідентифікаторів до облікових записів персоналу та паролів до них на редагування відповідної інформації на сайті виконується адміністратором системи. Для кожного користувача АС створені персональні облікові записи, захищені паролем, що дозволяє однозначно його ідентифікувати та відстежити їх дії.

1.6 Схема інформаційних потоків

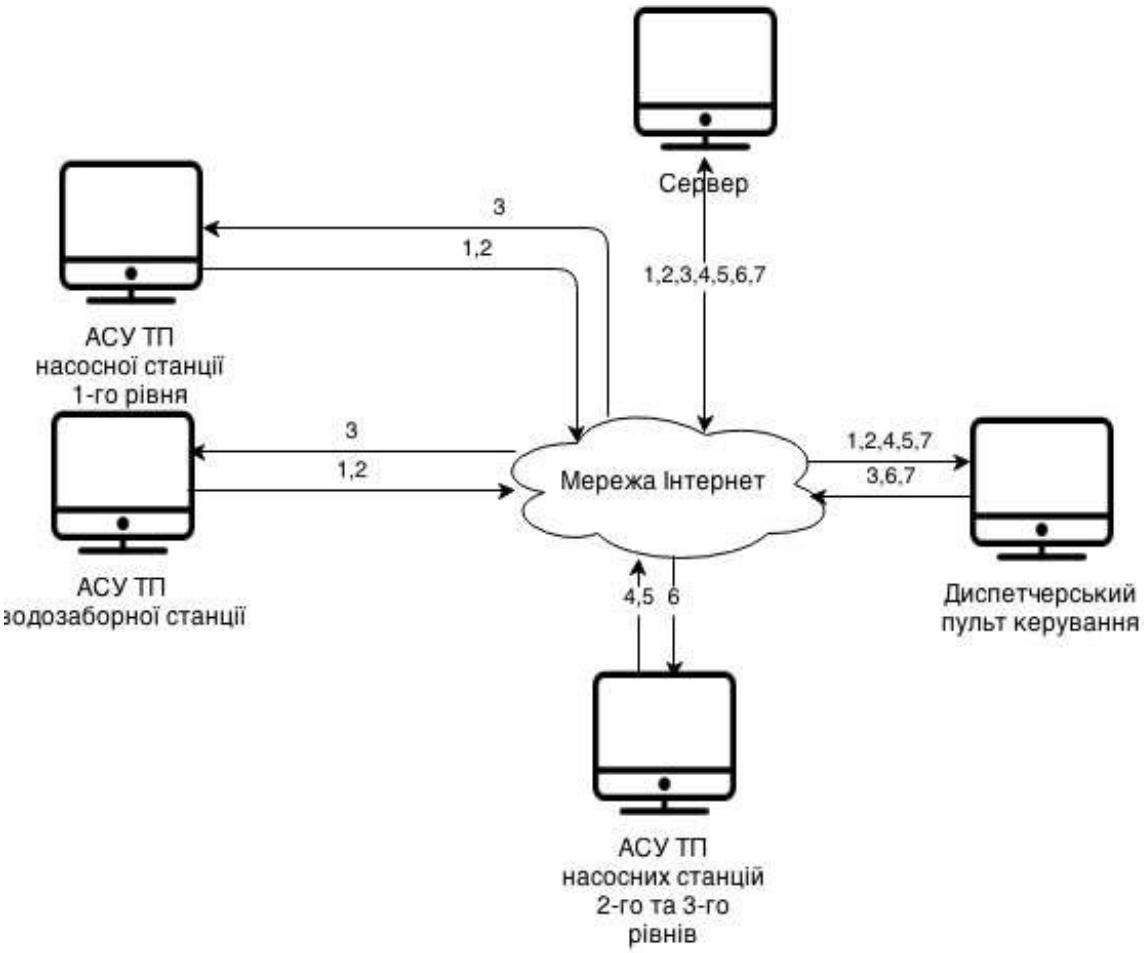

Рисунок 1.4 – Схема інформаційних потоків системи водопостачання

Схема інформаційних потоків зображена на рисунку 1.4. Види інформації, що циркулює згідно схеми:

1) інформація стану технічного об’єкту системи ПОВ;
2) діагностична інформація технологічного процесу системи ПОВ;
3) керувальні команди системи ПОВ;
4) інформація стану технічного об’єкту системи ПРВ;
5) діагностична інформація технологічного процесу системи ПРВ;
6) керувальні команди системи ПРВ;
7) автентифікаційна інформація.

1.7 Класифікація інформації за її властивостями

За доступністю:

Д4 – без неї робота суб'єкта зупиняється;

Д3 – без неї можна працювати, але дуже короткий час;

Д2 – без неї можна працювати якийсь час, але рано чи пізно вона знадобиться;

Д1 – без неї можна працювати, але її використання економить ресурси.

За цілісністю:

Ц4 – її несанкціонована зміна призведе до неправильної роботи всього суб'єкта або значної його частини; наслідки модифікації незворотні;

Ц3 – її несанкціонована зміна призведе до неправильної роботи суб'єкта через деякий час, якщо не будуть зроблені деякі дії; наслідки модифікації незворотні;

Ц2 – її несанкціонована зміна призведе до неправильної роботи частини суб'єкта через деякий час, якщо не будуть зроблені деякі дії; наслідки модифікації оборотні;

Ц1 – її несанкціонована зміна позначиться через деякий час, але не призведе до збою в роботі суб'єкта; наслідки модифікації оборотні.

За конфіденційністю:

К4 – розголошення інформації призведе до краху роботи суб'єкта або до дуже значних матеріальних втрат;

К3 – розголошення призведе до значних матеріальних втрат, якщо не будуть зроблені деякі дії;

К2 – розголошення призведе до деяких матеріальним (може бути, непрямим) або моральних втрат, якщо не будуть зроблені деякі дії;

К1 – приносить скоріше моральний збиток, може бути використана тільки в певних ситуаціях;

Інформація, класифікована за її властивостями подана у таблиці 1.2

Таблиця 1.2 – Класифікація інформації за властивостями

Інформація	Властивості інформації		
	конфіденційність	цілісність	доступність
Інформація стану технічного об'єкту системи ПОВ	К1	Ц2	Д2
Діагностична інформація технологічного процесу системи ПОВ	К1	Ц3	Д2
Керувальні команди системи ПОВ	К1	Ц2	Д3
Інформація стану технічного об'єкту системи ПРВ	К1	Ц2	Д2
Діагностична інформація технологічного процесу системи ПРВ	К1	Ц3	Д2
Керувальні команди системи ПРВ	К1	Ц2	Д3
Автентифікаційна інформація	К2	Ц2	Д2

1.8 Користувачі автоматизованої системи

Суб'єкти, що мають доступ до технічних засобів, поділяються на такі категорії користувачів (права доступу користувачів подано в таблиці 1.3):

– адміністратор безпеки;

– диспетчер, та інші співробітники, що мають безпосереднє відношення до процесів водопідготовки та водопостачання;

– співробітники підприємства, що не мають безпосереднього відношення до процесу водопостачання;

– директор.

Таблиця 1.3 – Матриця доступу користувачів до інформації

Інформація	Користувачі та їх права доступу			
	адміністратор безпеки	диспетчер	співробітники	директор
Інформація стану об’єкту системи ПОВ	R	R	R	R
Діагностична інформація техпроцесу системи ПОВ	R	R	R	R
Керувальні команди системи ПОВ	R	CRW	–	R
Інформація стану технічного об’єкту системи ПРВ	R	R	R	R
Діагностична інформація технологічного процесу системи ПРВ	R	R	R	R
Керувальні команди системи ПРВ	R	CRW	–	R
Автентифікаційна інформація	CRD	W	–	–

Можливість суміщення однією особою декількох з наведених ролей не виключається. Перелік та кількість користувачів, що допускаються до роботи в АС, визначаються внутрішніми наказами та/або розпорядженнями підприємства.

1.9 Модель порушника

Модель порушника – абстрактний формалізований, або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і так далі. По відношенню до АС порушники можуть бути внутрішніми (з числа

співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Таблиця 1.4 – Модель порушника

Порушник	Тип	Мета порушника	Рівень кваліфікації	Характер дій	Місце дії
Зловмисник (без ІТ підготовки)	Зовнішній	М2, М3	К1	Д1	МД3, МД4
Зловмисник (з ІТ підготовкою)	Зовнішній	М1, М2, М3	К3	Д2, Д3, Д4	МД4, МД5, МД1
Співробітник підприємства (що не відноситься до технологічного процесу ПОВ чи ПРВ)	Внутрішній	М1	К1	Д1	МД2, МД3
Адміністратор безпеки	Внутрішній	М2, М3	К4	Д4	МД5

Метою порушника можуть бути:

М1 – отримання необхідної інформації у потрібному обсязі та асортименті;

М2 – мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

М3 – нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Класифікація порушників за рівнем можливостей, що надаються їм засобами АС. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

К1 – перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

К2 – другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

К3 – третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

К4 – четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

Класифікація порушників за використовуваними методами і способами можна класифікувати як таких, що:

Д1 – використовують виключно агентурні методи одержання відомостей;

Д2 – використовують пасивні технічні засоби перехоплення інформаційних сигналів;

Д3 – використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

Д4 – використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

МД1 – без одержання доступу на контрольовану територію організації (АС);

МД2 – з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

МД3 – з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;

МД4 – з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

МД5 – з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ [10].

Модель порушника подано в таблиці 1.4

1.10 Модель загроз

Загрози для інформації, яка обробляється, залежать від характеристик обчислювальної системи, фізичного середовища, персоналу, технологій обробки і оброблюваної інформації АС.

Загрози можуть мати об'єктивну або суб'єктивну природу. Загрози, які мають суб'єктивну природу, можуть бути випадковими (ненавмисними) або навмисними.

Загрози можуть бути направлені на порушення цілісності, доступності, конфіденційності інформації, а також на спостережливість КС.

Вірогідність реалізації загрози залежить від існуючих засобів і механізмів захисту в обстежуваній системі.

Оскільки вимоги із захисту інформації від витоку технічними каналами на об’єктах 4 категорії, де обробляється службова інформація в нормативних документах системи технічного захисту інформації не визначені, опис загроз, що можуть реалізовуватися такими каналами не проводиться.

Побудована модель загроз подана в таблиці 1.5.

Таблиця 1.5 – Модель загроз

Загроза	Що порушує	Вірогідність	Джерело загрози	Механізм реалізації
Розвідка, аналіз трафіка	К, Д, Ц	Низька	Зовнішні порушники	Перехоплення інформації, що пересилається у незашифрованому виді в широкомовному середовищі передачі даних, відсутність виділеного каналу зв’язку між об’єктами АС

Продовження таблиці 1.5

Випадковий запуск хибних команд керування АСУ ТП	Д	Низька	Внутрішні порушники	Виконання автоматизованою системою команд систем керування водопостачанням заданих оператором(диспетчером) або порушником
Несанкціонований запуск команд керування АСУ ТП	Д	Середня	Внутрішні та зовнішні порушники	
Модифікація програмного забезпечення	К, Д, Ц	Низька	Внутрішні та зовнішні	Підміна прикладного програмного забезпечення, що забезпечує керування технологічним процесом
Блокування сервісу чи перевантаження запитами системи управління доступом (відмова в обслуговуванні)	Д	Середня	Зовнішні порушники	Використання атак типу “спрямований шторм” (Syn Flood), передачі на об’єкт, що атакується, не коректних, спеціально підібраних запитів. Використання анонімних (чи із модифікованими адресами) запитів на обслуговування типу електронної пошти (spam) чи вірусних атак спеціального типу

1.11 Профіль захищеності

Згідно з НД ТЗІ 2.5-005-99 основними загрозами для інформації оброблюваної в АС керування технологічними процесами є загрози порушення доступності АС і технології обробки інформації. В зв’язку з цим до КЗЗ ОС, що входять до складу таких АС, в першу чергу пред’являються вимоги до забезпечення доступності і адміністративного керування доступом щодо інформації з боку об’єктів-процесів. Для даної АС було обрано наступний профіль захищеності 3.ЦД: { ЦД-1, ЦА-1, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1, НВ-1 }

ЦД – довірча цілісність;

ЦО – відкат;

ЦВ – цілісність при обміні;

ДР – використання ресурсів;

ДВ – стійкість до відмов;

НР – реєстрація;

НИ – ідентифікація і автентифікація;

НК – достовірний канал;

НО – розподіл обов'язків;

НЦ – цілісність КЗЗ;

НТ – самотестування;

НВ – автентифікація при обміні.

1.11.1 Опис критеріїв що входять до складу профілю захищеності

ЦД-1. Мінімальна довірча цілісність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту [11].

У складі об’єкта експертизи наявні засоби, що реалізують керування доступом на підставі атрибутів доступу користувачів та об’єктів, тож

реалізованою є послуга ЦД-1. Керування потоками до об`єктів що належать домену користувача здійснюється засобами операційної системи.

ЦА-1. Адміністративна цілісність. Ця послуга дозволяє адміністратору чи спеціально авторизованому користувачу керувати потоками інформації від користувачів і процесів до захищених об'єктів. Згідно з політикою адміністративної цілісності (в повній аналогії з адміністративною конфіденційністю) об'єкту привласнюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі чи процеси, які намагаються модифікувати об’єкт. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування аналогічно рівням послуги довірча цілісність з тією відмінністю, що тільки адміністратор або авторизований адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

У складі об’єкта експертизи наявні засоби, що реалізують керування доступом на підставі атрибутів доступу користувачів та об’єктів, тож реалізованою є послуга ЦА-1. Керування потоками інформації від захищених об’єктів до користувачів сайту виконується засобами системи управління технологічним процесом «MasterEnergy» та засобами операційної системи.

ЦО-1. Обмежений відкат. Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Засоби системи управління ТП «MasterEnergy» дозволяють відмінити певну кількість операцій підчас роботи додатком, тож реалізовано лише рівень послуги ЦО-1. Програмними засобами операційної системи згідно до календарного плану адміністратором виконується резервне копіювання

інформації, що дозволить повернути програмну частину та інформацію на сервері до первинного стану.

ЦВ-2. Цілісність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від модифікації інформації у разі підключенні несанкціонованих користувачів. Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє забезпечити виявлення випадкових або навмисних порушень цілісності не тільки окремих повідомлень, але і потоків, повідомлень в цілому. Дана послуга не реалізується, оскільки у складі об’єкта експертизи відсутні механізми виявлення фактів несанкціонованої модифікації інформації переданої інформації чи фактів несанкціонованого видалення або дублювання переданих пасивних об’єктів.

ДР-1. Квоти. Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Квоти використовуються таким чином, щоб гарантувати, що жоден користувач не зможе захопити решту певного ресурсу, дозволяючи виділяти менші обсяги ресурсів, ніж максимальна квота користувача, гарантуючи таким чином іншому користувачеві доступ до розділюваного ресурсу.

Послуга реалізована оскільки в операційних системах Windows існує можливість керування обсягом виділених ресурсів (дисковий простір), що надаються окремому користувачу. Проте, політика використання ресурсів поширюється не всі інформаційні ресурси АС.

ДВ-1. Ручне відновлення. Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення

яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування. Відновлення можливе на рівні послуги ДВ-1 у випадку відмови чи переривання обслуговування за допомогою відміни певної послідовності операцій.

НР-2. Захищений журнал. Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КЗЗ має бути здатним негайно; інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій.

Засобами операційної системи, програмним продуктами «MasterEnergy», є можливість реєструвати наступні події: надання доступу, відмова в доступі, створення, модифікація, видалення об’єкта. Журнали дозволяють реєструвати інформацію про час, дату, тип та успішність кожної зареєстрованої події. Створювані журнали є захищеними від сторонньої модифікації, проте відсутня можливість аналізу подій та повідомлення адміністратора про події, які свідчать про перевищення порогів безпеки, тож послуга реалізована на рівні НР-2.

НИ-2. Одиночна ідентифікація і автентифікація. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Для програмного продукту «MasterEnergy» що виконує шифрування даних за протоколом SSL реалізується захищена передача автентифікованого ідентифікатора користувача від деякого зовнішнього джерела. Механізм аутентифікації функціонує з використанням одного захищеного механізму (знання паролю), що дозволяє гарантувати реалізацію послуги на рівні НИ-2.

НК-1. Однонаправлений достовірний канал. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

Засобами програмного продукту «MasterEnergy» можливе створення захищеного шляху передачі інформації між користувачем та об’єктом обстеження, що ініціюється лише користувачем, не може бути імітованим і інформація, що передається по ньому не може бути отримана чи модифікована сторонніми користувачами чи процесами. Послуга реалізована на рівні НК-1, оскільки можливість ініціювання з’єднання зі сторони КЗЗ відсутня.

НО-1. Виділення адміністратора. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Політика розподілу обов'язків, що реалізується КЗЗ,

повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Послуга реалізована, оскільки серед переліку ролей існує декілька ролей (зокрема адміністратор, диспетчер і т.д.), та немає розподілу обов`язків адміністратора на декілька ролей.

НЦ-2. КЗЗ з гарантованою цілісністю. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Послуга не реалізована, оскільки для реалізації рівня НЦ-2 потрібно описати обмеження які дозволяють гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити до доступу до захищених об’єктів контролюються КЗЗ.

НТ-3. Самотестування у реальному часі. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися в процесі штатної роботи.

Послуга не реалізована оскільки відсутня політика самотестування, яка описувала б властивості ОС та реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

НВ-1. Автентифікація вузла. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

Послуга не реалізована, скільки відсутні механізми, що виконували б процес ідентифікації одним КЗЗ іншого.

Обраний профіль захищеності інформації в АС від НСД відображено у таблиці 1.6. Послуги ЦВ-2, НЦ-2, НТ-2, НВ-1є не реалізованими.

Таблиця 1.6 – Функціональний профіль захищеності інформації від НСД

Критерій	Послуга безпеки	Рівень послуги безпеки
Цілісність	Цілісність адміністративна	ЦА-1
	Цілісність довірча	ЦД-1
	Відкат	ЦО-1
	Цілісність при обміні	ЦВ-2
Доступність	Використання ресурсів	ДР-1
	Відновлення після збоїв	ДВ-1
Спостережність	Реєстрація	НР-2
	Ідентифікація та автентифікація	НИ-2
	Достовірний канал	НК-1
	Розподіл обов’язків	НО-1
	Цілісність КЗЗ	НЦ-2
	Самотестування	НТ-2
	Автентифікація при обміні	НВ-1

1.12 Постановка задачі

Було поставлено наступні задачі:

– запропонувати проектні рішення щодо підвищення рівня захищеності автоматизованої системи керування процесами водопостачання;

– дослідити можливість використання інтелектуальних засобів аналізу даних для реалізації послуги самотестування.

1.13 Висновок

У цьому розділі отримані наступні основні результати:

1 Виконано аналіз поточного стану захищеності автоматизованої системи керування процесом водопостачання міста, виконано обстеження ОІД та установи де він знаходиться, описано умови функціонування АС, її структуру та оброблювану інформацію.

2 Проведено синтез та аналіз загроз інформації, що циркулює на ОІД.

3 Було обрано профіль захищеності, та проведено аналіз реалізації послуг в АС.

4 Поставлено основні задачі, що стають перед службою захисту інформації та потреби яким повинна задовольняти КСЗІ.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Методи підвищення рівня захисту у системі водопостачання

На основі аналізу стану захищеності було виділено наступні послуги, реалізація яких необхідна для повноти захисту відповідно до профіля захищеності: ЦВ-2 (цілісність при обміні), НЦ-2 (цілісність КЗЗ), НТ-2 (самотестування), НВ-1 (автентифікація отримувача).

2.2 Цілісність при обміні

Послуга «цілісність при обміні» дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти крипостійкість використовуваних алгоритмів шифрування.

Рівень ЦВ-1 даної послуги забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від модифікації інформації у разі підключенні несанкціонованих користувачів.

Відповідно до термінології, приведеної в нормативних документах в галузі захисту інформації під цілісністю інформації розуміється її властивість, яка полягає у тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Іншими словами, під цілісністю

інформації розуміється відсутність в ній будь-яких викривлень (модифікацій), які не були санкціоновані її власником, не залежно від причин або джерел виникнення таких викривлень. Під доступністю інформації розуміється властивість інформації, що полягає у тому, що вона знаходиться у вигляді, необхідному користувачу (процесу), в місці, необхідному користувачу (процесу), і в той час, коли вона йому необхідна. Звідси можна зробити висновок про те, що порушення цілісності інформації неминуче приводить і до порушення її доступності.

Виділяють наступні способи забезпечення цілісності інформаційних об'єктів (програмних засобів, інформації при її обробці і передачі), включаючи відновлення зруйнованої інформації, шляхом:

– застосування різного роду завадостійких кодів з виявленням помилок в прийнятій (зчитаній) інформації, які дозволяють реалізувати програмні, апаратні або програмно-апаратні засоби виявлення викривлень;

– застосування різного роду завадостійких коригуючих кодів, які дозволяють реалізувати програмні, апаратні або програмно-апаратні засоби виявлення і усунення викривлень.

Для забезпечення контролю цілісності інформаційних об'єктів, включаючи і відновлення зруйнованої інформації, до складу інформації, яка захищається, включають надмірну інформацію – ознаку цілісності або контрольну ознаку (залежно від прийнятої в задачах контролю цілісності або завадостійкого кодування термінології), своєрідний образ, відображення цієї інформації, процедура формування якого відома, і який з дуже високою ймовірністю відповідає інформації, що захищається.

При цьому між інформацією, що захищається, і ознаками цілісності або контрольними ознаками встановлюється регулярний (функціональний) односторонній зв'язок (процедури розрахунку контрольної ознаки за початковою інформацією, що захищається, відомі, а процедури розрахунку початкової інформації по контрольних ознаках найчастіше не існує). Контроль цілісності зводиться при цьому до тих або інших процедур перевірки наявності

вказаного регулярного одностороннього зв'язку між ознаками цілісності і прийнятої з каналу зв'язку інформацією.

Боротьба з виникаючими помилками ведеться на різних рівнях семирівневої моделі взаємодії відкритих систем (в основному на перших чотирьох). Для боротьби з виникаючими помилками відомо багато різних способів. Всіх їх можна підрозділити на дві групи: такі, що не використовують зворотний зв'язок і такі, що використовують його.

У першому випадку на передаючій стороні передані дані кодуються одним з відомих кодів з виправленням помилок. На приймальній стороні, відповідно, здійснюється декодування інформації, що приймається, і виправлення знайдених помилок. Виправляюча можливість вживаного коду залежить від числа надмірних бітів, що генеруються кодером. Якщо надмірність, що вноситься, невелика, то існує небезпека того, що дані, що приймаються, міститимуть незнайдені помилки, які можуть привести до помилок в роботі прикладного процесу. Якщо ж використовувати код з високою виправляючою здатністю (великою надмірністю), то це приводить до необґрунтовано низької реальної швидкості передачі даних.

У системах із зворотним зв'язком застосовуються процедури виявлення помилок і перезапиту так звані процедури з вирішальним зворотним зв'язком або виявлення помилок з автоматичним запитом повторення. В цьому випадку код застосовується тільки в режимі виявлення помилок, що дозволяє досягти дуже низької вірогідності незнайденої помилки при незначному рівні надмірності, що вводиться.

Характерною особливістю випадкових викривлень є те, що вони, через відсутність навмисності, порушують регулярний односторонній зв'язок між прийнятою інформацією і ознаками цілісності, сформованими перед передачею. Тому при виявленні порушення вказаного зв'язку встановлюється факт наявності таких викривлень, а за певних умов, і їх місця і величини (характеру). За відсутності порушення цього зв'язку встановлюється факт відсутності викривлень.

Характерною ж особливістю навмисних викривлень є те, що зловмисник прагне забезпечити, зімітувати наявність регулярного зв'язку між модифікованою їм початковою інформацією, прийнятою, і ознаками цілісності. З цією метою порушник, використовуючи знання процедур формування контрольних ознак, після необхідної для його цілей модифікації початкової інформації перед передачею одержувачу забезпечує формування відповідних ознак. При успішному формуванні вказаних ознак, розкрити наявність модифікації неможливо. Для боротьби з цим власнику (або авторизованому користувачу) необхідно використовувати або секретні (невідомі потенційним порушникам) процедури формування контрольних ознак (що дуже складно забезпечити), або вводити в загальновідомі процедури формування контрольних ознак секретні параметри (ключі перетворення). Не знаючи цих секретних параметрів (ключів перетворення), порушник не зуміє забезпечити, зімітувати наявність регулярного зв'язку між модифікованою їм початковою інформацією, прийнятою, і ознаками цілісності.

2.2.1 Методи контролю цілісності даних

2.2.1.1 Метод контрольних сум

Найбільш простий спосіб перевірки цілісності даних, переданих в цифровому представленні, – це метод контрольних сум. Під контрольної сумою розуміється деяке значення, розраховане шляхом додавання всіх чисел із вхідних даних. Якщо сума всіх чисел перевищує максимально допустиме значення, наперед заданий для цієї величини, то величина контрольної суми дорівнює коефіцієнту отриманої суми чисел – тобто це залишок від ділення підсумкової суми на максимально можливе значення контрольної суми, збільшене на одиницю. Якщо сказане записати у вигляді формули, то для розрахунку контрольної суми буде використовуватися такий вираз:

$$C = T \bmod (Max + 1), \tag{2.1}$$

де T – підсумкова сума, розрахована за вхідними даними;

Max – максимально допустиме значення контрольної суми, задане заздалегідь;

C – розрахункове значення контрольної суми.

Метод контрольних сум – це найбільш проста форма цифрової ідентифікації; тобто величина, отримана в результаті підрахунку вмісту деяких інших даних, змінюється при корекції даних, на основі яких він отриманий.

Недолік методу контрольних сум полягає в тому, що хоча розбіжність значень цих сум служить вірним доказом, що даний документ зазнав зміни, рівність порівнюваних значень ще не дай гарантії, що інформація залишилася незмінною.

Можна довільним чином змінити порядок проходження чисел у документі, а контрольна сума при цьому збереже колишнє значення. До того ж можна змінити окремі числа в документі і підігнати решта таким чином, щоб забезпечити колишнє значення контрольної суми.

При використанні для контрольних сум 8-розрядної змінної ймовірність того, що контрольні суми двох зовсім випадково вибраних послідовностей даних будуть однакові, дорівнює 1/256. При збільшенні довжини змінної під контрольну суму до 16 або 32 розрядів, ймовірність збігів зменшується, проте цей механізм все одно дуже чутливий до можливих помилок, щоб забезпечити високу ступінь довіри до представлених даних [12].

2.2.1.2 Контроль CRC

Більш досконалий спосіб цифрової ідентифікації деякої послідовності даних – це обчислення контрольного значення її циклічного надмірного коду. Алгоритм контролю CRC вже протягом тривалого часу широко використовується в системах мережевих адаптерів, контролерів жорсткого диска та інших пристроїв для перевірки ідентичності вхідний і вихідний інформації.

Механізм CRC заснований на поліноміальному розподілі, де кожен розряд деякої порції даних відповідає одному коефіцієнту великого поліноміального вираження. Ключовим принципом обчислень для механізму

CRC є те, що операції множення і ділення цих поліномів виконуються точно так само, як із звичайними числами. Якщо певний поліном (коефіцієнти якого отримані відповідно до використовуваним алгоритмом CRC) розділити на поліном, який представляє будь-то послідовність даних, то в результаті виходить поліном-приватне і поліном-залишок. Друге з цих значень служить основою для створення контрольного параметра CRC. Так само, як і для контрольних сум, параметром CRC не потрібно багато місця (зазвичай їх довжина становить 16 або 32 розряди); однак у порівнянні з ними, надійність виявлення невеликих змін вхідної інформації тепер значно вище. Якщо в деякому величезному блоці даних лише один розряд став іншим, то і контрольний параметр CRC зі 100-відсотковою ймовірністю також буде мати інше значення. Якщо ж зміняться два розряди, то ймовірність виявлення помилки при довжині параметра CRC в 16-розрядів, становить понад 99,99%.

2.2.1.3 Алгоритми хешування

Хешування – перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. Такі перетворення також називаються функцією хешування, або хеш-функцією [14].

Хешування застосовується для порівняння даних: якщо у двох масивах хеш-коди різні, масиви гарантовано розрізняються; якщо однакові - масиви, швидше за все, однакові. У загальному випадку однозначної відповідності між вихідними даними і хеш-кодом немає в силу того, що кількість значень хеш-функцій менше, ніж варіантів вхідного масиву; існує безліч масивів, які дають однакові хеш-коди - так звані колізії. Ймовірність виникнення колізій відіграє важливу роль в оцінці якості хеш-функцій.

Існує безліч алгоритмів хешування з різними характеристиками (розрядність, обчислювальна складність, крипостійкість і т. п.). Вибір тієї чи іншої хеш-функції визначається специфікою розв'язуваної задачі. Найпростішими прикладами хеш-функцій може служити контрольна сума або CRC.

Серед безлічі існуючих хеш-функцій прийнято виділяти криптографічно стійкі, які застосовуються в криптографії. Для того, щоб хеш-функція H вважалася криптографічно стійкою, вона повинна задовольняти трьом основним вимогам, на яких засновано більшість застосувань хеш-функцій в криптографії:

1 Незворотність: для заданого значення хеш-функції m повинно бути обчислювально нездійсненно знайти блок даних X, для якого H (X) = m.

2 Стійкість до колізій першого роду: для заданого повідомлення M повинно бути обчислювально нездійсненно підібрати інше повідомлення N, для якого H (N) = H (M).

3 Стійкість до колізій другого роду: має бути обчислювально нездійсненно підібрати пару повідомлень (M, M'), що мають однаковий хеш.

Дані вимоги не є незалежними:

1 Оборотна функція нестійка до колізій першого і другого роду.

2 Функція, нестійка до колізій першого роду, нестійка до колізій другого роду; зворотне невірно.

Варто зазначити, що не доведено існування необоротних хеш-функцій, для яких обчислення будь-якого прообразу заданого значення хеш-функції теоретично неможливо. Зазвичай знаходження зворотного значення є лише обчислювально складним завданням.

HMAC - механізм перевірки цілісності інформації, що передається або зберігається в ненадійному середовищі. Механізми, які надають такі перевірки цілісності на основі секретного ключа, зазвичай називають кодом автентичності повідомлення (MAC). Як правило, MAC використовується між двома сторонами, які поділяють секретний ключ для перевірки автентичності інформації, переданої між цими сторонами. Механізм, який використовує криптографічні хеш-функції в поєднанні з секретним ключем називається HMAC.

2.2.1.4 Електронний цифровий підпис

Електронний підпис - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних; електронний цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [14]. Електронний цифровий підпис використовується фізичними та юридичними особами – суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Безпека використання ЕЦП забезпечується тим, що засоби, які використовуються для роботи з ЕЦП, проходять експертизу та сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, що гарантує неможливість злому і підробки ЕЦП.

Цифровий підпис призначений для автентифікації особи, яка підписала електронний документ. Крім цього, використання цифрового підпису дозволяє здійснити:

– контроль цілісності переданого документа: при будь-якому випадковому або навмисному зміну документа підпис стане недійсним, тому що обчислена вона на підставі вихідного стану документа і відповідає лише йому;

– захист від змін (підроблення) документа: гарантія виявлення підробки при контролі цілісності робить підроблюють недоцільним у більшості випадків;

– неможливість відмови від авторства. Так як створити коректну підпис можна, лише знаючи закритий ключ, а він повинен бути відомим тільки власнику, то власник не може відмовитися від свого підпису під документом;

– доказове підтвердження авторства документа: так як створити коректну підпис можна, лише знаючи закритий ключ, а він повинен бути

відомим тільки власнику, то власник пари ключів може довести своє авторство підпису під документом. Залежно від деталей визначення документа можуть бути підписані такі поля, як «автор», «внесені зміни», «мітка часу».

Автентифікація захищає двох учасників, які обмінюються повідомленнями, від впливу деякої третьої сторони. Однак проста автентифікація не захищає учасників один від одного, тоді як і між ними теж можуть виникати певні форми суперечок.

У ситуації, коли обидві сторони не довіряють один одному, необхідно щось більше, ніж автентифікація на основі загального секрету. Можливим рішенням подібної проблеми є використання цифрового підпису. Цифровий підпис повинний володіти наступними властивостями:

1 Повинна бути можливість перевірити автора, дату і час створення підпису.

2 Повинна бути можливість автентифікувати вміст під час створення підпису.

3 Підпис повинен бути перевірений третьою стороною для вирішення спорів. Таким чином, функція цифрового підпису включає функцію автентифікації.

На підставі цих властивостей можна сформулювати наступні вимоги до цифрового підпису:

– підпис повинен бути двійковим зразком, який залежить від повідомлення, що підписується;

– підпис повинен використовувати деяку унікальну інформацію відправника для запобігання підробки або відмови;

– створювати цифровий підпис має бути відносно легко;

– повинно бути обчислювально неможливо підробити цифровий підпис, як створенням нового повідомлення для існуючого цифрового підпису, так і створенням помилкової цифрового підпису для деякого повідомлення;

– цифровий підпис має бути досить компактним і не займати багато пам'яті.

При використанні прямого цифрового підпису взаємодіють тільки самі учасники, тобто відправник та одержувач. Передбачається, що одержувач знає відкритий ключ відправника. Цифровий підпис може бути створений шифруванням усього повідомлення або його хеш-коду (перетворення вхідного масиву даних довільної довжини в вихідний бітовий рядок фіксованої довжини) закритим ключем відправника.

Конфіденційність може бути забезпечена подальшим шифруванням усього повідомлення разом з підписом відкритим ключем одержувача (асиметричне шифрування) або розділяються секретним ключем (симетричне шифрування). Зазвичай функція підпису виконується першою, і тільки після цього виконується функція конфіденційності. У разі виникнення спору якась третя сторона повинна переглянути повідомлення і його підпис. Якщо функція підпису виконується над зашифрованим повідомленням, то для вирішення спорів доведеться зберігати повідомлення як в незашифрованому вигляді (для практичного використання), так і в зашифрованому (для перевірки підпису). Або в цьому випадку необхідно зберігати ключ симетричного шифрування, для того щоб можна було перевірити підпис початкового повідомлення. Якщо цифровий підпис виконується над незашифрованим повідомленням, одержувач може зберігати тільки повідомлення в незашифрованому вигляді і відповідний підпис до нього.

Всі прямі схеми мають спільне слабке місце. Дієвість схеми залежить від безпеки закритого ключа відправника. Якщо відправник згодом не захоче визнати факт відправлення повідомлення, він може стверджувати, що закритий ключ був втрачений або вкрадений, і в результаті хтось підробив його підпис. Можна застосувати адміністративне управління, що забезпечує безпеку закритих ключів, для того щоб, принаймні, хоч у якійсь мірі послабив ці загрози. Один з можливих способів полягає у вимогах до кожного підпису повідомлення включати позначку часу (дату і час) і повідомляти про скомпрометовані ключі в спеціальний центр.

Інша загроза полягає в тому, що закритий ключ може бути дійсно вкрадений у X в момент часу T. Порушник може потім послати повідомлення, підписане підписом X і позначений тимчасовою міткою, яка менше або дорівнює T.

Проблеми, пов'язані з прямим цифровим підписом, можуть бути частково вирішені за допомогою арбітра. Існують різні схеми з застосуванням арбітражного підпису. У загальному вигляді арбітражний підпис виконується наступним чином. Кожне підписане повідомлення від відправника до одержувача X Y першою справою надходить до арбітра A, який перевіряє підпис для цього повідомлення. Після цього повідомлення датується і надсилається до Y із зазначенням того, що воно було підтверджено арбітром. Присутність A вирішує проблему схем прямого цифрового підпису, при яких X може відмовитися від повідомлення.

Арбітр грає важливу роль в подібного роду схемах, і всі учасники повинні йому довіряти.

Асиметричні схеми ЕЦП відносяться до криптосистем з відкритим ключем. На відміну від асиметричних алгоритмів шифрування, в яких шифрування проводиться за допомогою відкритого ключа, а розшифрування - за допомогою закритого, у схемах цифрового підпису підписування проводиться із застосуванням закритого ключа, а перевірка - із застосуванням відкритого.

Загальновизнана схема цифрового підпису охоплює три процеси :

1 Генерація ключової пари. За допомогою алгоритму генерації ключа рівно ймовірним чином з набору можливих закритих ключів вибирається закритий ключ, обчислюється відповідний йому відкритий ключ.

2 Формування підпису. Для заданого електронного документа за допомогою закритого ключа обчислюється підпис.

3 Перевірка (верифікація) підпису. Для даних документа та підпису за допомогою відкритого ключа визначається дійсність підпису.

Для того, щоб використання цифрового підпису мало сенс, необхідно виконання двох умов:

Верифікація підпису повинна проводитися відкритим ключем, відповідним саме тому закритому ключу, який використовувався під час підписання. Без володіння закритим ключем має бути обчислювально складно створити легітимний цифровий підпис [15].

У разі додавання лічильника повідомлень разом із цифровим підписом, у КЗЗ з’явиться можливість відстежувати модифікацію, знищення чи дублювання повідомлень, таким чином критерій ЦВ-2 буде реалізовано.

2.3 Цілісність комплексу засобів захисту

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Жодна КС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу. У зв'язку з цим рівень НЦ-1 даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг.

Для рівня НЦ-1 даної послуги необхідно, щоб КЗЗ мав можливість перевіряти свою цілісність і в разі виявлення її порушення переводити систему в стан, з якого її може вивести тільки адміністратор.

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Для реалізації даної послуги необхідно забезпечити виконання серверних та клієнтських додатків системи «MasterEnergy» від імені окремо виділеного користувача, авторизація до якого не можлива засобами операційної системи (наприклад NT AUTHORITY\LocalService). Політикою безпеки необхідно забезпечити надання мінімально необхідних повноважень для нормального функціонування даному користувачу. Таким чином буде забезпечено окремий домен виконання для даного додатку. Для забезпечення саме цілісності КЗЗ та

переведення КЗЗ у режим аварійного стану необхідно реалізувати контроль цілісності додатків та їх модулів із програмного коду у режимі реального часу, та також обмежити атрибути доступу мінімально необхідними правами виконувані додатки та їх модулі.

2.4 Автентифікація вузла

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

Для реалізації даної послуги пропонується ввести наступний протокол ідентифікації КЗЗ подібний до CHAP [15] (КЗЗ1 - КЗЗ, що ініціює запит, КЗЗ2 - КЗЗ до якого ініціюється запит):

1 КЗЗ1 ініціює запит до КЗЗ2 повідомленням з ідентифікатором користувача КЗЗ1.

2 КЗЗ2 надсилає до КЗЗ1 повідомлення з ідентифікатором КЗЗ2, випадковим набором даних обмеженої довжини, ідентифікатором запиту.

3 КЗЗ1 рахує значення хешу отриманого випадкового набору даних, ідентифікатору запиту разом із паролем користувача КЗЗ1 та надсилає повідомлення формату до КЗЗ2, до складу якого входять ідентифікатор запиту та обчислений хеш.

4 У разі відповідності хешу повідомлення та обчисленого самим КЗЗ2 значенням хешу до КЗЗ1 надсилається відповідь про успішно встановлене з’єднання, в іншому випадку надсилається повідомлення про відмову встановлення з’єднання.

2.5 Самотестування КЗЗ

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися в процесі штатної роботи.

Реалізацію даної послуги можна умовно поділити на чотири етапи: формування переліку тестів, обрання алгоритму обробки даних тестів, розробка програмного забезпечення, впровадження системи. Особливостями послуги самотестування в реальному часі при реалізації на об`єкті обстеження є наступні чинники:

1 Процес водопідготовки, як складова процесу водопостачання є тривалим процесом, який не має чітких часових лімітів (у середньому триває від 4 до 24 годин).

2 Під час процесу водопідготовки КС задіяна лише на період введення лабораторних даних та на період переведення об`єму підготовленої води до сховища, під час проведення лабораторних випробувань КС не використовується.

Після проведення аналізу АС було обрано наступні параметри системи для тестування:

- доступність сервера (шляхом виклику моніторингового сервісу);
- цілісність додатку клієнта;
- цілісність компонентів серверу додатків;
- проміжок часу, що минув після останньої маніпуляції з даними;
- потужність використання насосної станції першого рівня;
- потужність використання насосної станції другого рівня.

Множина стану системи з огляду на особливості технологічного процесу складається з трьох значень:

а) нормальний режим роботи;

б) порушення нормального режиму роботи, що не призводить до негативних наслідків у короткостроковій перспектив;

в) порушення нормального режиму, що може призвести до негативних наслідків у короткостроковій перспективі.

Задача оцінки стану системи через обмежену кількість допустимих значень на виході фактично є задача класифікації. В результаті рішення задачі класифікації виявляються ознаки, які характеризують групи об'єктів досліджуваного набору даних - класи; за цими ознаками новий об'єкт можна віднести до того чи іншого класу, на відміну від кластеризації, що може виділяти нові класи у разі відсутності схожих класів. Кластеризація - це автоматичне розбиття елементів деякої множини на групи залежно від їх схожості. Синонімами терміну «кластеризація» є «автоматична класифікація», «навчання без вчителя» і «таксономія». Завдання кластеризації схожа з завданням класифікації, є її логічним продовженням, але її відмінність в тому, що класи досліджуваного набору даних заздалегідь не визначені. Таким чином кластеризація призначена для розбиття сукупності об'єктів на однорідні групи (кластери або класи). Якщо дані вибірки представити як точки в просторі ознак, то завдання кластеризації зводиться до визначення згрупувань точок.

2.5.1 Штучні нейромережі

Штучні нейромережі є моделями нейронної структури мозку, який здатен сприймати, обробляти, зберігати та продукувати інформацію. Особливістю мозку також є навчання та самонавчання на власному досвіді. Адаптивні системи на основі штучних нейронних мереж дозволяють з успіхом вирішувати проблеми розпізнавання образів, виконання прогнозів, оптимізації, асоціативної пам'яті і керування.

Механізм природного мислення базується на збереженні інформації у вигляді образів. Штучні нейронні мережі дозволяють створення паралельних мереж, їх навчання та вирішення інтелектуальних завдань, не використовуючи традиційного програмування. Оригінальність нейромереж, як аналога

біологічного мозку, полягає у здібності до навчання за прикладами, що складають навчальну множину. Процес навчання нейромереж розглядається як налаштування архітектури та вагових коефіцієнтів синаптичних зв'язків відповідно до даних навчальної множини для ефективного вирішення поставленої задачі.

Більшість реалізацій нейромереж використовують контрольоване навчання, де вихід постійно порівнюється з бажаним виходом. Вагові коефіцієнти зв’язків на початку встановлюються випадково (ініціалізація мережі), але під час наступних ітерацій коректуються, щоб досягти близької відповідності між бажаним та біжучим виходами. Такі методи навчання націлені на мінімізації біжучих похибок всіх елементів обробки, що відбувається завдяки неперервної зміни синаптичних ваг до досягнення прийнятної точності мережі.

Перед використанням, нейромережа з контрольованим навчанням повинна бути навченою. Фаза навчання займає певний час. Навчання вважається закінченим при досягненні нейромережею визначеного користувачем рівня ефективності і бажаної статистичної точності. Після навчання вагові коефіцієнти зв’язків фіксуються для подальшого застосування. Деякі типи мереж дозволяють під час використання продовжувати навчання, і це допомагає мережі адаптуватись до змінних умов.

Навчальні множини повинні бути достатньо великими, щоб містити всю необхідну інформацію для виявлення важливих особливостей і зв'язків. Навчальні приклади повинні містити широке різноманіття даних. Якщо мережа навчається лише для одного прикладу, вагові коефіцієнти, що старанно встановлено для цього прикладу, радикально змінюються у навчанні для наступного прикладу. Попередні приклади при навчанні наступних просто забуваються. В результаті система повинна навчатись всьому разом, знаходячи найкращі вагові коефіцієнти для загальної множини прикладів.

Головним компонентом для успішної роботи мережі є представлення і кодування вхідних і вихідних даних. Штучні мережі працюють лише з

числовими вхідними даними, отже, необроблені дані, що надходять із зовнішнього середовища повинні перетворюватись. Важливою є нормалізація даних, тобто приведення всіх значень даних до єдиного діапазону. Нормалізація виконується шляхом ділення кожної компоненти вхідного вектору на довжину вектору, що перетворює вхідний вектор в одиничний. Попередня обробка зовнішніх даних, отриманих за допомогою сенсорів, у машинний формат є спільною і легко доступною для стандартних комп'ютерів.

Якщо після контрольованого навчання нейромережа ефективно опрацьовує дані навчальної множини, важливим стає її ефективність при роботі з даними, які не використовувались для навчання. У випадку отримання незадовільних результатів для тестової множини, навчання продовжується. Тестування використовується для забезпечення запам'ятовування не лише даних заданої навчальної множини, але і створення загальних образів, що можуть міститись в даних.

Неконтрольоване навчання може бути великим надбанням у майбутньому. Воно проголошує, що комп'ютери можуть самонавчатись у справжньому роботизованому сенсі. На даний час, неконтрольоване навчання використовується в мережах відомих, як самоорганізовані карти. Мережі не використовують зовнішніх впливів для коректування своїх ваг і внутрішньо контролюють свою ефективність, шукаючи регулярність або тенденції у вхідних сигналах та здійснюють адаптацію відповідно до навчальної функції. Навіть без повідомлення правильності чи неправильності дій, мережа повинна мати інформацію відносно власної організації, яка закладена у топологію мережі та навчальні правила.

Алгоритм неконтрольованого навчання скеровано на знаходження близькості між групами нейронів, які працюють разом. Якщо зовнішній сигнал активує будь-який вузол в групі нейронів, дія всієї групи в цілому збільшується. Аналогічно, якщо зовнішній сигнал в групі зменшується, це приводить до гальмуючого ефекту на всю групу.

Основу для навчання формує конкуренція між нейронами. Навчання конкуруючих нейронів підсилює відгуки певних груп на певні сигнали. Це пов'язує групи між собою та відгуком. При конкуренції змінюються ваги лише нейрона-переможця.

Незважаючи на переваги нейронних мереж в певних областях над традиційними обчисленнями, існуючі нейромережі не є досконалими рішеннями. Вони навчаються і можуть робити «помилки». Окрім того, не можна гарантувати, що розроблена мережа є оптимальною мережею.

Застосування нейромереж вимагає від розробника виконання ряду умов:

– наявність репрезентативної та достатньої за розміром множини даних для навчання й тестування мережі;
– розуміння базової природи проблеми, яка буде вирішена;
– вибір функції суматора, передатної функції та методів навчання;
– розуміння інструментальних засобів розробника;
– відповідна потужність обробки.

2.5.2 Мережа Кохонена

Мережа розпізнає кластери в навчальних даних і розподіляє дані до відповідних кластерів. Якщо в наступному мережа зустрічається з набором даних, несхожим ні з одним із відомих зразків, вона відносить його до нового кластеру. Якщо в даних містяться мітки класів, то мережа спроможна вирішувати задачі класифікації. Мережі Кохонена можна використовувати і в задачах, де класи відомі - перевага буде у спроможності мережі виявляти подібність між різноманітними класами. Мережа Кохонена має всього два прошарки: вхідний і вихідний. Схема мережі зображена на рисунку 2.1.

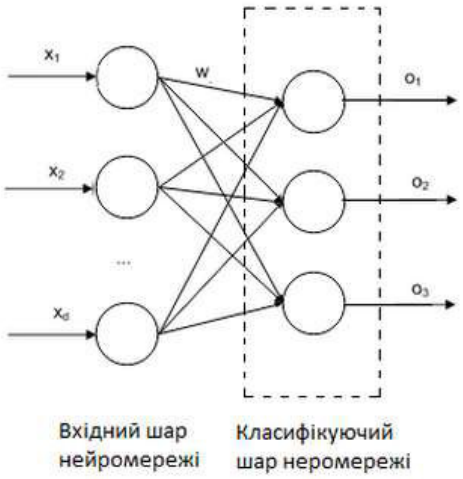

Рисунок 2.1 – Мережа Кохонена

Мережа Кохонена навчається методом послідовних наближень. Починаючи з випадковим чином обраного вихідного розташування центрів, алгоритм поступово покращується для кластеризації навчальних даних.

Проте, алгоритм може працювати і на іншому рівні. В результаті ітеративної процедури навчання мережа організовується таким чином, що елементи, які відповідають центрам, розташованим близько один від одного в просторі входів, будуть розташовані близько один від одного і на топологічній карті.

Топологічний прошарок мережі можна уявити як двовимірну штахету, яку потрібно так відобразити в N-вимірний простір входів, щоб по можливості зберегти вихідну структуру даних. Звісно ж, при будь-якій спробі відтворити N-вимірний простір на площині буде загублено багато деталей, але такий прийом дозволяє користувачу візуалізувати дані, що неможливо зрозуміти іншим засобом.

Основний ітераційний алгоритм Кохонена послідовно проходить ряд епох, на кожній епосі опрацьовується один навчальний приклад. Вхідні сигнали - вектори дійсних чисел - послідовно пред'являються мережі. Бажані вихідні сигнали не визначаються. Після пред'явлення достатнього числа вхідних векторів, синаптичні ваги мережі визначають кластери. Крім того, ваги організуються так, що топологічне близькі вузли чуттєві до схожих вхідних

сигналів. Для реалізації алгоритму необхідно визначити міру сусідства нейронів (окіл нейрона-переможця).

Після того, як мережа навчена розпізнаванню структури даних, її можна використовувати як засіб візуалізації при аналізі даних.

Області застосування. Кластерний аналіз, розпізнавання образів, класифікація.

Недоліки. Мережа може бути використана для кластерного аналізу тільки в тому випадку, якщо заздалегідь відоме число кластерів.

Переваги. Мережа Кохонена здатна функціонувати в умовах перешкод, тому що число кластерів фіксоване, ваги модифікуються повільно, налаштування ваг закінчується після навчання.

2.5.3 Дерево прийняття рішень

Дерево прийняття рішень (також можуть називатися деревами класифікацій або регресійними деревами) — використовується в галузі статистики та аналізу даних. Структура дерева містить такі елементи: лист і гілка [17]. На ребрах (гілках) дерева прийняття рішення записані атрибути, від яких залежить цільова функція, в листі записані значення цільової функції, а в інших вузлах — атрибути, за якими розрізняються випадки. Щоб класифікувати новий випадок, треба спуститися по дереву до листа і видати відповідне значення. Подібні дерева рішень широко використовуються в інтелектуальному аналізі даних. Мета полягає в тому, щоб створити модель, яка прогнозує значення цільової змінної на основі декількох змінних на вході.

Дерева рішень, бувають двох основних типів:

1 Аналіз дерева класифікації, коли прогнозований результат є класом, до якого належать дані.

2 Регресійний аналіз дерева, коли прогнозований результат можна розглядати як дійсне число (наприклад, ціна на будинок, або тривалість перебування пацієнта в лікарні).

Згадані вище терміни вперше були використані Брейманом та іншими [16].

Проблема отримання оптимального дерева рішень є NP-повною з точки зору деяких аспектів оптимальності навіть для простих завдань [18, 19, 26]. Таким чином, практичне застосування алгоритму дерев рішень засноване на евристичних алгоритмах, таких як алгоритм «жадібності», де єдино оптимальне рішення вибирається локально для кожного вузла. Такі алгоритми не можуть забезпечити оптимальність всього дерева в цілому.

Ті, хто вивчає метод дерева прийняття рішень, можуть створювати занадто складні конструкції, які недостатньо повно представляють дані. Дана проблема називається перенавчанням. Для того, щоб уникнути цієї проблеми, необхідно використовувати метод «регулювання глибини дерева».

Існують концепти, які складно зрозуміти з моделі, так як модель описує їх складним шляхом. Дане явище може бути викликано проблемами XOR, парності або мультіплексарності.

У цьому випадку ми маємо справу з непомірно великими деревами. Існує кілька підходів вирішення даної проблеми, наприклад, спроба змінити репрезентацію концепту в моделі (складання нових суджень) або використання алгоритмів, які більш повно описують і репрезентують модель.

Серед інших методів аналізу даних, метод дерева прийняття рішень має кілька переваг:

1 Простий в розумінні та інтерпретації. Люди здатні інтерпретувати результати моделі дерева прийняття рішень після короткого пояснення.

2 Не вимагає підготовки даних. Інші техніки вимагають нормалізації даних, додавання фіктивних змінних, а також видалення пропущених даних.

3 Здатний працювати як з категоріальними, так і з інтервальними змінними. Інші методи працюють лише з тими даними, де присутня лише один тип змінних.

4 Використовує модель «білого ящика». Якщо певна ситуація спостерігається в моделі, то її можна пояснити за допомогою булевої логіки. Прикладом «чорного ящика» може бути штучна нейронна мережа, так як результати даної моделі майже не піддаються поясненню.

5 Дозволяє оцінити модель за допомогою статистичних тестів. Це дає можливість оцінити надійність моделі.

6 Є надійним методом. Метод добре працює навіть в тому випадку, якщо були порушені початкові припущення, включені в модель.

7 Дозволяє працювати з великим об'ємом інформації без спеціальних підготовчих процедур. Даний метод не вимагає спеціального обладнання для роботи з великими базами даних.

2.5.4 Баєсівський класифікатор

Наївний баєсівський класифікатор — класифікатор, що використовує теорему Баєса для визначення ймовірності приналежності спостереження (елемента вибірки) до одного з класів C за умови того, що залежні змінні приймають задані значення P (C | F1 , … , Fn).

Тобто, якщо на основі значень змінних можна однозначно визначити, якого класу належить спостереження, байєсівский класифікатор повідомить, що ймовірність приналежності до цього класу дорівнює 1.

У проміжних же випадках, коли спостереження може з різною ймовірністю належати до різних класів, результатом роботи класифікатора буде вектор, компоненти якого є ймовірностями приналежності до того чи іншого класу. Можна бачити, що ідеальний байєсівский класифікатор в якомусь сенсі є оптимальним. Його результат не може бути поліпшений, так як у всіх випадках, коли можливий однозначну відповідь, він його дасть — а в тих випадках, коли відповідь неоднозначна, результат кількісно характеризує міру цієї неоднозначності [21].

Разом з тим, в оптимальності криється і основний недолік ідеального байєсівського класифікатора: для його побудови потрібно вибірка, що містить всі можливі комбінації змінних — а розмір такої вибірки експоненційно зростає із зростанням числа змінних. Для подолання описаної вище проблеми на практиці використовують наївний байєсівский класифікатор — класифікатор, побудований на основі припущення про незалежність змінних, тобто

припущення про те, що використання цього припущення дозволяє не вивчати взаємодію всіх можливих поєднань змінних, обмеживши лише впливом кожної змінної окремо на приналежність образу до одного з класів.

Перевагою цього підходу є те, що вимоги до розміру вибірки скорочуються від експоненційних до лінійних.

Недолік — це те, що модель точна лише у випадку, коли виконується припущення про незалежність. В іншому випадку, строго кажучи, обчислені ймовірності вже не є точними (і навіть більше того, їх сума може не дорівнювати одиниці, через що потрібно нормувати результат). Однак на практиці незначні відхилення від незалежності призводять лише до незначного зниження точності, і навіть у разі істотної залежності між змінними результат роботи класифікатора продовжує корелювати з істинною приналежністю образу до класам.

При цьому достоїнства класифікатора (висока швидкість роботи, простота і масштабованість, помірні вимоги до пам'яті) часто переважують недоліки.

2.5.5 Таблиця прийняття рішень

Таблиця рішень - спосіб компактного представлення моделі зі складною логікою. Аналогічно умовним операторам в мовах програмування, вони встановлюють зв'язок між умовами і діями. Але, на відміну від традиційних мов програмування, таблиці рішень в простій формі можуть представляти зв'язок між безліччю незалежних умов і дій.

Таблиці прийняття рішень, як правило, поділяються на чотири квадранта, як показано у таблиці 2.1 [23, 27].

Таблиця 2.1 – Схема таблиці рішень

Умови	Варіанти виконання умов
Дії	Необхідність дій

У простому випадку тут «Умови» - список можливих умов, «Варіанти виконання умов» - комбінація з виконання та / або невиконання умов з цього списку. «Дії» - список можливих дій, «Необхідність дій» - вказівка треба чи не треба виконувати відповідну дію для кожної з комбінацій умов.

Перевагами даного способу є наглядна структура, та відсутність потребу у нормалізації даних. Недоліком є великий обсяг даних у який вироджується таблиця. Важливим негативним чинником також є той факт, що практична реалізація створюється для кожного конкретного випадку окремо.

2.5.6 Порівняльний аналіз інтелектуальних методів обробки даних

Для моделювання було обрану наступні методи інтелектуального аналізу вибірки: нейромережі Кохонена (з автоматичною кластеризацією на три кластери та з ручним навчанням мережі) та дерево рішень.

Для вище згаданих методів використовувалась однакова початкова вибірка. Навчальна та тестові вибірки формувались із початкової випадковим методом. Обсяг вибірки для навчання становив 95% від початкової вибірки у 3456 елементів. Тестова вибірка складала 5%, тобто 173 елементи.

Для мережі Кохонена у режимі ручного навчання мережі виконується налаштування ваг мережі так, щоб виходили узгоджені вихідні вектори, тобто щоб пред'явлення досить близьких вхідних векторів давало однакові виходи. Процес навчання, отже, виділяє статистичні властивості навчальної множини і групує подібні вектори в класи. Пред'явлення на вхід векторів з даного класу дасть визначений вихідний вектор, але до навчання неможливо передбачити, який вихід буде вироблятися даним класом вхідних векторів. Отже, виходи мережі повинні трансформуватися в деяку зрозумілу форму, зумовлену процесом навчання.

На вхід нейромережі необхідно подавати нормалізовані параметри, тобто результати виконання тестових функцій необхідно подавати у вигляді

зрозумілому нейронній мережі. Після нормування вектор вхідних значень подається на вхід нейромережі. Ці елементи не виконують ніяких вирішальних функцій, а тільки передають сигнали у наступний шар мережі. Вибір числа входів – для будь-якої нейронної мережи – одне з найважливіших завдань, тому що при малому розмірі вхідного вектору можлива втрата важливої для класифікації інформації, а при великому істотно підвищується складність обчислень (при моделюванні на комп’ютерах, в реальних нейронних мережах це невірно, тому що всі елементи працюють паралельно). Одним з принципів нейромережевої обробки інформації є здатність до апроксимації даних, тобто мережа може доволі точно спрогнозувати належність того чи іншого вхідного вектору до одного з визначених класів в умовах для навчання мережі була обрана репрезентативна вибірка та процес навчання мав випадковий характер подання векторів на вхід мережі. Логічним є припущення що вихід мережи може давати похибку. Особливістю автоматичного режиму кластеризації для мережі Кохонена, є той факт, що мережа сама групує вектори, а значення відповідних еталонних класів порівнюються лише на етапі підрахування похибки. Результати аналізу мережі Кохонена подані у таблиці 2.2.

Для побудови дерева рішень було обрано автоматичний алгоритм формування дерева C4.5, побудований Джоном Квінланом [24, 26]. Даний алгоритм є алгоритмом побудування дерева із керованим навчанням.

Інформація про об'єкти, що підлягають класифікації повинні бути представлені як обсяг атрибутів об'єкту, що може мати дискретне чи числове значення. Кількість атрибутів має бути незмінною для всіх об'єктів. Множина класів повинна бути скінченою. Обсяг вибірки має бути значно більшим за кількість класів, кожен об'єкт повинен бути асоційований із певним класом.

Порівняльний аналіз результатів побудови дерева розв’язків поданий в таблиці 2.2. На основі отриманих результатів можна зробити певні висновки:

– кількість та властивості атрибутів об'єктів вибірки є несприйнятливі для нейромережевого аналізу;

– дерево розв'язків дозволяє проаналізувати об'єкти, що мають атрибути різного характеру.

Для оцінювання результатів роботи мережі використовується тестова вибірка, що містить тестові приклади, тобто приклади, які використовуються не для навчання моделі, а для перевірки його результатів. Приклади тестової множини так само, як і навчальна вибірка, можуть пред'являються моделі в процесі навчання, але не використовуються для підстроювання її параметрів. Мета застосування тестової вибірки - перевірити, як навчена модель буде працювати з новими даними, тобто придбала чи вона здатність до узагальнення. Помилка моделі, отримана на тестовому безлічі, називається помилкою узагальнення.

Таблиця 2.2 – Похибка інтелектуальних методів обробки даних

у відсотках

Тип вибірки	Дерево розв'язків	Мережа Кохонена у режимі автоматичної класифікації	Мережа Кохонена (навчання із вчителем)
Тестова	1,15	45,31	22,1
Навчальна	1,58	42,12	20,61

Якщо помилки на тестовому і навчальної множини досить малі, то це з достатньою часткою впевненості дозволяє стверджувати, що модель придбала здатність до узагальнення і може використовуватися для роботи з новими даними. Якщо мала помилка досягнута тільки на навчальній множині, а на тестовому вона велика, то це дозволяє припустити низьку здатність до узагальнення.

При поділі вибірки даних на навчальну і тестову вибірки, головне - забезпечити репрезентативність навчальної множини, а решту прикладів можна використовувати в якості тестових.

Крім цього, перевірка помилки на тестовій вибірці дозволяє не допустити перенавчання моделі. Якщо помилка на навчальній множині монотонно падає, то на тестовій множині, після деякого числа ітерацій, вона може почати зростати, що говорить про перенавчанні моделі. Тому, щоб уникнути перенавчання, доцільно зупинити навчання, як тільки помилка на тестовому безлічі починає зростати.

Тестування запропонованих моделей виконувалося за допомогою пакету математичних додатків Deductor Studio [25]. За результатами аналізу мережі стає очевидним, що навіть із великим обсягом вибірки – результати роботи нейронної мережі є незадовільними, і величина похибки становить від 22 до 45% для тестової вибірки. При збільшенні числа ітерацій навчання нейромереж становиться очевидним, що у разі достатньої репрезентативності вибірки – обсяг вибірки не сильно впливає на результат роботи мережі. Похибка у роботі дерева розв’язків становить 1,15%, що є сприйнятливим результатом.

2.6 Висновок

У даному розділі були надані рекомендації щодо підвищення рівня захищеності інформації, що має бути забезпечений в системі водопостачання. Було проведено аналіз існуючих методів класифікації даних, проаналізовано моделі нейромережевого класифікатора та дерева розв’язків для класифікації станів АСУ ТП водопостачання та доцільність її використання.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

В роботі надані рекомендації щодо підвищення рівня захищеності інформації, що має бути забезпечений в системі водопостачання, проведено аналіз існуючих методів класифікації даних, проаналізовано моделі нейромережевого класифікатора та дерева розв’язків для класифікації станів АСУ ТП водопостачання та доцільність її використання.

Метою цього розділу є обґрунтування економічної доцільності застосування нейромережевих методів самотестування для підвищення рівня захищеності АСУ водопостачанням. Для досягнення поставленої мети необхідно здійснити наступні розрахунки:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект;

– показники економічної ефективності застосування нейромережевих методів самотестування для підвищення рівня захищеності АСУ водопостачанням.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

3.1.1. Визначення витрат на створення програмних засобів захисту інформації

3.1.1.1 Визначення трудомісткості застосування нейромережевих методів самотестування для підвищення рівня захищеності АСУ водопостачанням

Трудомісткість тестування застосування нейромережевих методів самотестування визначається тривалістю кожної робочої операції:

$$t = tmз + tв + ta + tз + tобр + tд, \text{ годин,}$$

де $tmз$ – тривалість складання технічного завдання, $tmз = 10$;

$tв$ – тривалість вивчення ТЗ, літературних джерел за темою тощо, $tв = 30$;

ta – тривалість аналізу поточного стану захищеності автоматизованої системи керування процесом водопостачання міста, $ta = 15$;

$tз$ – тривалість синтезу та аналізу загроз інформації, що циркулює на ОІД, $tз = 18$;

$tобр$ – тривалість обрання профілю захищеності та аналіз реалізації послуг в АС, $tобр = 16$;

$tд$ – тривалість підготовки технічної документації, $tд = 8$.

Таким чином,

$$t = 10 + 30 + 15 + 18 + 16 + 8 = 97 \text{ годин,}$$

3.1.1.2. Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту ***Кпз*** складаються з витрат на заробітну плату виконавця програмного забезпечення *Ззп* і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 10864 + 19{,}44 = 10883{,}44 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 97*112 = 10864 \text{ грн.}$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = (t_{опр} + t_{д}) \cdot С_{мч} = 8 \cdot 2{,}43 = 19{,}44 \text{ грн.}$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}8 \cdot 1 \cdot 1{,}64 + \frac{3800 \cdot 0{,}5}{1920} + \frac{2400 \cdot 0{,}1}{1920} = 2{,}43 \text{ грн.}$$

Тестування запропонованих моделей виконувалося за допомогою пакету математичних додатків Deductor Studio, які безкоштовні версії у вільному доступі, що відповідає вимогам щодо виконання поставлених задач.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 10883{,}44 + 4000 = 14883{,}44 \text{ грн.}$$

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

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, $К_{н}$=4000 грн.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн.$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_{н} = 0$ грн.).

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), складає:

$$С_{з} = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного системного адміністратора на місяць складає 9000 грн. Для виконання тестування працюватиме один інженерно-технічний спеціаліст. Додаткова заробітна плата – 9% від основної заробітної плати. Отже,

$$С_з = 9000*12 + 9000*12*0,09= 117720 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2016 р. складає 22%.

$$С_{єв} = 11772 *0,22 = 25898,4 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,4 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,4*1920*1,64 = 4408,32 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос = 14883,44*0,01=148,83 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 117720 + 25898,4 + 4408,32 + 148,83 = 148175,55 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 148175,55 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Впровадження автоматизованої системи управління на об'єктах житлово-комунального комплексу, зокрема водопостачання, таких як системи «MasterEnergy», надає наступні переваги: економія електроенергії до 30%; економія до 30% втрат води за рахунок високої точності підтримки графіка тиску в мережах тепло- і водопостачання.

Використання такої автоматизованої системи дозволяє значно підвищити якість послуг і збільшити ресурс експлуатації трубопроводів і обладнання в 1,5-2 рази. З використанням цієї системи знижується ризик технологічних інцидентів і аварій на об'єктах, оскільки управління об'єктами здійснюється в автоматичному режимі за встановленим графіком. Тим самим знижуються ризики, пов'язані з людським фактором, зменшується еконагрузка на навколишнє середовище і скорочується чисельність персоналу. На виникнення позаштатних ситуацій можна реагувати в режимі реального часу.

Таким чином, головними можливими збитками є витрат електроенергії, які становлять близько 30% в собівартості підприємства з водопостачання. Відповідно до публічних форм фінансової звітності підприємств з водопостачання, а саме Звіту про фінансові результати за , за дев’ять місяців

2018 р. величина собівартості реалізованої продукції склала 359272 тис. грн. Виходячи з цього, можливі річні витрати U електроенергії можуть становити на рік:

$$U = 359272 * 1,25 * 0,3 = 134727 \text{ тис. грн.}$$

Таким чином, загальний збиток підприємства з водопостачання складатиме як мінімум B=134727 тис. грн.

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (20%);

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

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 134727 * 0,2 - 148,17 = 26797,23 \text{ тис грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на

впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{26797{,}23}{144{,}88} = 184{,}96, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (\text{N}_{\text{деп}} - \text{N}_{\text{інф}})/100),$$

де $\text{N}_{\text{деп}}$ – річна депозитна ставка, (17 %);

$\text{N}_{\text{інф}}$ – річний рівень інфляції, (10%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$921{,}81 > (17 - 10)/100 = 7{,}05 > 0{,}07.$$

Термін окупності капітальних інвестицій $\text{T}_{\text{о}}$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{184{,}96} = 0{,}005, \quad \text{років.}$$

3.4 Висновок

Результатом проведеної роботи в даному розділі є обґрунтування економічної доцільності застосування нейромережевих методів самотестування для підвищення рівня захищеності АСУ водопостачанням.

Розраховані поточні витрати на експлуатацію системи інформаційної безпеки становлять 148175,55 грн. Можлива величина відверненого збитку може скласти 134727 тис. грн. за рахунок економії витрат електроенергії, які становлять близько 30% в собівартості підприємства з водопостачання.

ВИСНОВКИ

Після дослідження питань пов’язаних із станом захищеності автоматизованих систем керування процесами водопостачання можна зробити певні висновки:

1 Проведено аналіз поточного стану захищеності автоматизованої системи керування процесом водопостачання міста, виконано обстеження ОІД та установи де він знаходиться, описано умови функціонування АС, її структуру та оброблювану інформацію.

2 Виконано вибір функціонального профілю захищеності від несанкціонованого доступу та проведено аналіз критеріїв обраного профілю.

3 Надано рекомендації щодо підвищення рівня захищеності інформації, що має бути забезпечений в системі водопостачання.

4 Проаналізовані існуючі інтелектуальні методи аналізу даних та можливість їх використання у системах захисту.

5 Обґрунтовано економічну доцільність впровадження запропонованих проектних рішень.

ПЕРЛІК ПОСИЛАНЬ

1 Соков М.А. Водопроводные сети и сооружения. М.: Стройздат, 2003. — 129 с.

2 Обзор участия частного сектора в водоснабжении и водоотведении стран ВЕКЦА. Институт экономики города. 2010.

3 Подготовка питьевой воды (Електрон. ресурс) / Спосіб доступу: URL: http://vodokanal.dp.ua/index.php?lang=ru&class=publication&id=7 – Загол. з екрана.

4 Очистка сточных вод (Електрон. ресурс) / Спосіб доступу: URL: http://vodokanal.dp.ua/index.php?lang=ru&class=publication&id=19 – Загол. з екрана.

5 Абрамов Н.Н. Водоснабжение: Учебник для вузов. 3-е изд., перераб. и доп. М.: Стройиздат, 1982.

6 В. А. Петросов. Стійкість водопостачання. — Х.: Фактор, 2007. — 360 с.

7 Водопостачання. Зовнішні мережі та споруди. Основні положення проектування: ДБН В.2.5-74:2013 / Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України. – Київ, 2013. –287 с.

8 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу / ДСТСЗІ СБ України – Київ, 1999.

9 НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

10 НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

11 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України – Київ, 1999.

12 Механизмы контроля целостности данных (Електрон. ресурс) / Спосіб доступу: http://www.iso27000.ru/chitalnyi-zai/kriptografiya/mehanizmy-kontrolya-celostnosti-dannyh – Читальный зал. Криптография.

13 MD5 (Електрон. ресурс) / Спосіб доступу: URL: http://uk.wikipedia.org/wiki/MD5 – Загол. з екрана.

14 Електронні системи: навчальний посібник / Й. Й. Білинський, К. В. Огороднік, М. Й. Юкиш. – Вінниця : ВНТУ, 2011. – 208 с.

15 Методы и средства защиты информации (Електрон. ресурс) / Спосіб доступу: URL: http://scanner.narod.ru/link/Safe/miszi.htm – Загол. з екрана.

16 Classification and regression trees. Breiman, Leo; Friedman, J. H., Olshen, R. A., & Stone, C. J. (1984). Monterey, CA: Wadsworth & Brooks/Cole Advanced Books & Software.

17 Дерево принятия решений (Електрон. ресурс) / Спосіб доступу: URL: http://ru.wikipedia.org/wiki/Дерево_принятия_решений– Загол. з екрана.

18 Hyafil, Laurent; Rivest. Constructing Optimal Binary Decision Trees is NP-complete (Електрон. ресурс) / Спосіб доступу: http://barbra-coco.dyndns.org/eiyou/data/NPComplete.pdf – Binary decision trees.

19 Murthy S. Automatic construction of decision trees from data: A multidisciplinary survey. Data Mining and Knowledge Discovery (Електрон. ресурс) / Спосіб доступу: http://www.cs.uiuc.edu/class/fa05/cs591han/papers/98murthy.pdf – Data mining and knowledge discovery.

20 Інтелектуальні методи обробки даних. (Електрон. ресурс) / Спосіб доступу: URL: http://www.victoria.lviv.ua/html/oio– Загол. з екрана.

21 Наївний баєсівський класифікатор (Електрон. ресурс) / Спосіб доступу: URL: http://uk.wikipedia.org/wiki/Наївний_баєсівський_класифікатор – Загол. з екрана.

22 Аналитические технологии (Електрон. ресурс) / Спосіб доступу: URL: http://www.neuroproject.ru/neuro.php – Загол. з екрана.

23 Таблица принятия решений (Електрон. ресурс) / Спосіб доступу: URL: http://uk.wikipedia.org/wiki/Таблица_принятия_решений – Загол. з екрана.

24 Quinlan J. R. C4.5: Programs for Machine Learning. — San Mateo: Morgan Kaufmann Publishers Inc., 1993. — 302 p.

25 Deductor studio (Електрон. ресурс) / Спосіб доступу: URL: http://www.basegroup.ru/deductor/ – Обработка данных.

26 Decision tree (Електрон. ресурс) / Спосіб доступу: URL: http://www.saedsayad.com/decision_tree.htm – Загол. з екрана.

27 Decision table (Електрон. ресурс) / Спосіб доступу: URL: http://classes.soe.ucsc.edu/cmps115/Spring05/supplements/DecisionTables.htm – Загол. з екрана.

28 Decision Tree Induction (Електрон. ресурс) / Спосіб доступу: URL: http://www.tutorialspoint.com/data_mining/dm_dti.htm– Загол. з екрана.

29 Методичні вказівки до виконання економічної частини дипломного проекту (для студентів напряму підготовки 1701 Інформаційна безпека)/ Упорядн.: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро – 17 с.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	27	
6	А4	2 Розділ	27	
7	А4	3 Розділ	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:
Нейромережеві методи самотестування для підвищення рівня захищеності АСУ водопостачанням
студента групи 125м-17-1
Гончарова Станіслава Олександровича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерела та __ додатка.

Актуальність теми полягає в необхідності впровадження методів інтелектуального аналізу даних, як засобу підвищення рівня інформаційної безпеки системи АСУ водопосточанням.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

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

Робота виконана самостійно. У роботі було виконаний аналіз стану захищеності систем водопостачання; проектні рішення щодо підвищення захищеності об’єкта досліджень; розглянуті основні підходи щодо реалізації послуг захисту від НСД автоматизованої системи керування процесами водопостачання; запропоноване використання інтелектуального аналізу даних, як складового елемента послуг безпеки

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Гончаров Станіслав Олександрович заслуговує на оцінку «_____».

Керівник дипломної роботи,
к.т.н., доц. кафедри БІТ С.В. Флоров