Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Автоматизації проектування обчислювальної техніки
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)
(рівень вищої освіти)

Система безпеки, контролювання та управління доступом в кіберуніверситеті
.
.
(тема)

Виконав: студент 2 курсу, групи СКСм-18-1
Гарбузов Д.С.
(прізвище, ініціали)
Спеціальність 123 Комп`ютерна інженерія
(код і повна назва спеціальності)
Тип програми Освітньо - професійне
(освітньо-професійна або освітньо-наукова)
Освітня програма Спеціалізовані комп`ютерні системи
(повна назва освітньої програми)
Керівник доц. каф. АПОТ Немченко В.П.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Чумаченко С. В .
(підпис) (прізвище, ініціали)

20__ р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
Кафедра Автоматизації проектування обчислювальної техніки
Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Тип програми Освітньо-професійна
Освітня програма Спеціалізовані комп'ютерні системи

(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Гарбузову Дмитру Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Система безпеки, контролювання та управління доступом в кіберуніверситеті

затверджена наказом по університету від 04 11 2019 р. № 1624ст
2. Термін подання студентом роботи до екзаменаційної комісії 15 12 2019 р.
3. Вихідні дані до роботи
Node js
Mongo DB
Express js

4. Перелік питань, що потрібно опрацювати в роботі
Теоретичний аналіз
Система контролювання та управління доступом
Система безпеки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

13 слайдів

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	03.09.2019 – 04.09.2019	
2	Аналіз предметної області	05.09.2019 – 28.09.2019	
3	Аналіз джерел з проблемної галузі	28.09.2019 – 18.10.2019	
4	Дослідження системи кібер-університету	18.10.2019 – 26.10.2019	
5	Аналіз СКУД	26.10.2019 – 5.11.2019	
6	Проектування системи	5.11.2019 – 15.11.2019	
7	Реалізація підсистеми	15.11.2019 – 27.11.2019	
8	Оформлення пояснювальної записки	27.11.2019 – 06.12.2019	
9	Оформлення графічного матеріалу	06.12.2019 – 07.12.2019	
10	Перевірка виконаного проекту керівником	07.12.2019 – 14.12.2019	

Дата видачі завдання 03.09.2019

Студент _____
(підпис)

Керівник роботи _____ доц. Немченко В.П.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить: сторінок 59, рисунків 13, 24 джерел за переліком посилань.

SMART CYBER UNIVERSITY, ID, ХМАРНІ ОБЧИСЛЮВАННЯ, СКУД, СКД

Мета науково-атестаційної роботи – аналіз існуючих систем контролю та управління доступом. Розгляд СКУД в контексті системи безпеки та поєднання з іншими системами для забезпечення надійної безпеки.

Формування моделі підсистеми. Аналіз структури СКУД на основі інфраструктури університету.

Розробка тестової підсистеми для надання та розмежування доступу для різних типів відвідувачів.

Розгляд недоліків та переваг бездротової СКУД. Зробити висновок опираючись на аналіз і виконану роботу.

Об’єкт дослідження – процеси та компоненти підсистеми контролю та управління доступом для робітників та студентів університету.

Предмет дослідження – процедури та функції систем контролю та управління доступом в приміщення.

ABSTRACT

The explanatory note contains: pages 59, figures 13, 24 sources in the list of references.

SMART CYBER UNIVERSITY, ID, Cloud Computing, CMS

The purpose of the scientific-certification work is to analyze the existing access control and control systems. Consideration of ACSD in the context of a security system and interfacing with other systems to ensure reliable security

Formation of subsystem model. Analysis of the structure of the ACSD based on the university infrastructure.

Development of a test subsystem to provide and differentiate access for different types of visitors.

Consideration of the disadvantages and benefits of wireless ACS. Make a conclusion based on the analysis and the work done.

The object of study is the processes and components of the access control and management subsystem for university workers and students.

Subject of research - procedures and functions of systems of control and management of access to the premises.

ЗМІСТ

ВСТУП

В світі вже давно існують різноманітні види технічних і інформаційних систем, які роблять роботу людей більш легшою,коректнішою та безпечнішою. А саме допомагають у пілотуванні літаками, управлінні дорожнім рухом, охороні різноманітних об’єктів, у веденні бухгалтерського звіту, і багато інших. Люди звикли до покращення та облегшення своєї роботи, тому різноманітні системи управління чи контролю зустрічаються практично в усіх галузях.

В більшості компаній і закладах є охорона або інша відповідальна особа, яка займається пропуском співробітників, та записує у журнал час прибуття, або відвідувачів, які не являються працівниками об’єкту, але повинні потрапити до закладу чи компанії по діловим справам або на конференцію. Після перевірки списків чи зв’язком з працівником компанії у якої повинна бути зустріч з відвідувачем, охорона пропускає в середину відповідної будівлі.

Подібна ідентифікація людини потрібна для запобігання неправомірних дій зі сторони відвідувачів та контролюванні руху на пропускній.

Для того щоб оптимізувати роботу, збільшити рівень фізичної безпеки та зменшити ризик некоректної роботи охоронного персоналу, застосовують системи контролю та управління доступом.

Замок, електромеханічний або електромагнітний, електромеханічна защіпка, турнікет, шлагбаум являються пристроями які виконують задачу блокування чи розбракування дверей чи проходу. Основними задачами кожної СКД є розмежування для надання проходу чи ні, при умові успішної ідентифікації людини або навпаки. Система надає змогу фіксувати та реєструвати момент успішного пересування осіб в реальному часі, а також

реагувати в випадку неправильної ідентифікації чи неправомірного проникнення.

Однією з головних цілей роботи є проектування СКУД на основі інфраструктури університету. Включаючи всі умовні входи-виходи та їх положення. В свою чергу інфраструктура є частиною ресурсів розумної структури кібер-університету.

Розумний кібер-університет – метрична культура соціально-технологічних відносин, яка об’єднує в мережу кадри та розумну інфраструктуру, для виконання актуальних наукових дослідів і підготовки затребуваних ринком спеціалістів з академічними та науковими ступенів шляхом адекватного моніторингу та хмарного управління оцифрованними науково-освітніми процесами та явищами в цілях залучення інвестицій та досягнення високої якості життя співробітників.

Проектування подібної системи дозволить зробити оцінку поточного стану пропускних пунктів університету, побачити зв’язок компонентів системи.

Реалізація підсистеми дозволить детальніше розглянути та проаналізувати дані, їх зв’язок та оптимізацію у проектованій системі.

1 ХМАРНІ ОБЧИСЛЕННЯ

Хмарними обчисленнями називають принцип забезпечення віддаленого доступу через мережу до обчислювальних ресурсів.

Прикладом таких служб можуть слугувати сервера, бази даних, сховища та комунікаційні мережі,аналітика та інтелектуальний аналіз, які можуть бути швидко надані користувачеві.

Такі служби прискорюють впровадження інновацій, підвищують гнучкість ресурсів і забезпечують економію завдяки високій масштабованості.

Хмарні обчислювання дозволяють уникнути серйозних витрат на покупку необхідного обладнання та програмного забезпечення, налаштування та використання локальних центрів обробки даних.

Найбільші хмарні обчислюванні служби працюють в світовій мережі безпечних центрів обробки даних. Це забезпечує різноманітні переваги в порівнянні з використанням корпоративного центру обробки даних, включаючи зменшення затримки в мережі для прикладних програм та більшу економію від масштабу.

В плані надійності хмарні обчислювання роблять резервне копіювання даних, аварійне відновлення та неперервність процесів більш легшими та менш затратними, бо дані можна відобразити на декількох дублюючих сайтах в мережі провайдера хмарних служб.

Зазвичай для локальних центрів обробки даних потребується багато серверів, а також налагоджень виконуваного обладнання, оновлення прикладних програм, що вимагає багато часу. Хмарні обчислювання дозволяють уникнути багато з цих задач.

2 ІННОВАЦІЙНІ СЕРВІСИ РОЗУМНОГО КІБЕР - УНІВЕРСИТЕТУ

Інноваційні сервіси, які формують розумній кібер-університет як структурний прототип глобального науково – освітнього віртуального кібер-простору Global Smart Cyber University (рисунок 2.1).

Хмарно-мобільні сервіси Розумного Кібер Університету			
Безбумажний електронний документообіг	Сервіс електронного голосування	Сервіс управління персоналом	Сервіс управління кафедрою
Сервіс тестування знань	Сервіс управління наукою	Сервіс управління освітою	Управління навчанням студента
Сервіс управління захистами	Сервіс управління ліцензуванням	Сервіс доступу до інфрастуктури	Сервіс кібер безпеки

Рисунок 2.1 – Інноваційні сервіси розумного кібер-університету

– хмарний кібер-сервіс захищеного електронного документообігу для цифрового моніторингу та інтелектуального кіберуправленія науково-освітніми процесами (створення, реалізація та утилізація документа), в форматі замкнутого циклу: «факт - вимір - оцінка - дія», який повністю виключає паперові носії шляхом використання Cloud-Mobile Service Computing, баз даних, цифрового підпису, ID-card, пошти та мобільного телефону;

– хмарний кібер-сервіс мобільного голосування e-voting для моніторингу громадської думки; реалізації студентських опитувань; прийняття рішень на оперативних нарадах, засіданнях вченої ради, конференціях трудового колективу; проведення виборів експертів,

студентського сенату, керівного та науково-педагогічного складу при заміщенні вакантних посад;

– хмарний кібер-сервіс управління персоналом на основі online моніторингу, вимірювання, рейтингування та накопичення цифрових метрик компетенцій для оцінювання діяльності: студентів і всіх категорій співробітників з метою вироблення прозорих регуляторних моральних і матеріальних стимулів, вибору переможців з претендентів на вакантні позиції керівників і науково-педагогічних посад;

– хмарний кібер-сервіс управління структурним підрозділом на основі online моніторингу, вимірювання й нагромадження цифрових метрик компетенцій кафедри, пов'язаних з науково-освітнім процесом для вироблення регуляторних дій, що управляють і генерування пакета документів, необхідних для життєдіяльності;

– хмарний кібер-сервіс оцінки якості освітніх процесів і компонентів, online тестування знань і умінь, що виключає нелегітимні відносини між викладачем і студентом при здачі іспитів і заліків;

– хмарний кібер-сервіс управління науковими процесами на основі цифрового оцінювання діяльності вчених, підрозділів, наукових результатів, проектів і пропозицій по метриках, розробленим експертами, з метою прозорого та легітимного розподілу фінансових, кадрових і часових ресурсів між підрозділами і співробітниками;

– хмарний кібер-сервіс надання про разовательних послуг у вигляді MOOC online і onsite курсів, а також управління освітнім процесом на основі прозорого розподілу фінансових і тимчасових (кредитних) ресурсів між підрозділами і співробітниками в суворій відповідності з метричних оцінюванням вкладу кожного суб'єкта в актив і імідж університету;

– хмарний кібер-сервіс моніторингу та управління науково-освітнім процесом студента в реальному масштабі часу, генерування і зберігання електронних документів для його супроводу в часі і просторі за допомогою

створення персонального віртуального кабінету, пов'язаного з мобільним пристроєм і e-mail;

– хмарний кібер-сервіс вимірювання і супроводу бакалаврських, магістерських та дисертаційних робіт, а також конкурсних проектів на основі інтеграції міжнародних метрик оцінювання наукової та практичної значущості результатів проведених досліджень з внутрішніми критеріями якості, розробленими експертами;

– хмарний кібер-сервіс ліцензування та акредитації спеціальностей на основі вимірювання науково-освітньої діяльності кафедр і подальшого генерування пакета документів, необхідного для зовнішнього оцінювання якості навчальних процесів;

– хмарний кібер-сервіс електронного 24/7 доступу та моніторингу присутності співробітників і студентів в інфраструктурних аудиторіях університету на основі використання мобільних пристроїв і ID-card, а також електронний банкінг для оплати освітніх послуг і використання корпоративних кафедральних карт для придбання товарів і послуг в межах зароблених кафедрою засобів;

– хмарний кібер-сервіс захисту інформаційно-фізичного простору університету і санкціонування електронного доступу в усі кіберфізіческіе компоненти і процеси, пов'язані з життєдіяльністю вузу.

3 СИСТЕМА БЕЗПЕКИ

Системи безпеки - це сукупність взаємопов'язаних організаційних заходів і технічних засобів, об'єднаних каналами зв'язку для забезпечування підтримки та збереженням цілісності безпечного стану об'єкта, виявлення і ліквідацію загроз та інформації.

До складу систем безпеки в якості технічних засобів забезпечення безпеки входить комплексна система - сукупність технічних засобів та систем. Що забезпечують виконання комплексу завдань системи безпеки.

Більшість компаній пропонують своїм замовникам надійні і сучасні рішення в побудові наступних систем безпеки:

- охоронне відеоспостереження;
- системи контролю доступу;
- охоронна сигналізація.

3.1 Охоронне відеоспостереження

Відеоспостереження стало невід'ємною функцією комплексної системи безпеки, оскільки сучасне відеоспостереження дозволяє не тільки спостерігати і записувати відео, але і програмувати реакцію всієї системи безпеки при виникненні тривоги.

Охоронна система відеоспостереження призначена для візуального спостереження за об'єктом, що охороняється за допомогою відеокамер. Охоронне відеоспостереження дозволяє стежити одночасно за одним або кількома об'єктами. Камери відеоспостереження можна встановити як всередині приміщення, так і зовні. Завдання охоронного відеоспостереження складається в наочному поданні відеоінформації про оперативну обстановку на контрольованому об'єкті в реальному часі.

Елементарна охоронна система відеоспостереження формується з одної або кількох відеокамер та засобів моніторингу. Камери відео спостереження найчастіше встановлюватися на поворотних пристроях для зміни положення куту огляду.

Розташовуються камери зовні та всередині приміщення для кращого спостереження за територією або будівлею, що охороняється. Дуже часто разом з охоронною системою впроваджують до системи безпеки, різноманітні датчики.

У системах відеоспостереження, розрахованих на використання декількох відеокамер, на екрані одного монітора можна одночасно відображати зображення від усіх відеокамер.

Для послідовного виведення зображень використовуються мультиплексори, які послідовно підключають відеокамери до монітора або телевізора.

Охоронна система відеоспостереження дозволяє створити гнучку систему безпеки, в яку можуть входити не тільки компоненти охоронного відеоспостереження, а й охоронно-пожежної сигналізації і системи контролю доступу.

Існують два типи систем відеоспостереження: аналогове і цифрове.

Аналогові системи відеоспостереження використовують для відеоспостереження з одночасним записом інформації. Для забезпечення безпеки об'єктів використовують цифрові системи відеоспостереження, які добавляються в вже існуючі комплексні системи безпеки. Подібні комплексні системи фіксують дані, записують і аналізують інформацію, що надходить від відеокамер та датчиків, а також різноманітно реагують для найкращого захисту об'єкту.

На сьогоднішній день найбільш часто створюються саме цифрові системи відеоспостереження.

На даний момент найбільше застосування отримали відеокамери на основі ПЗЗ-матриць. У більшості випадків використовуються

короткофокусні об'єктиви типу фікс-фокус, які не потребують фокусування, і автоматичне керування експозицією.

Їх використання дозволило створити вкрай дорогі за ціною і досить високоякісні вироби широкого застосування. Зазвичай різниця між камерами, заснованими на матрицях різних виробників, проявляється в складних умовах освітлення. У лінійці кожного виробника присутні як дешеві і стандартні за параметрами матриці, так і матриці підвищеного дозволу або підвищеної чутливості.

Мінівідеокамера - відеокамери в квадратних або циліндричних корпусах, які звичайно застосовуються як готовий виріб для установки всередині приміщень.

Корпусні відеокамера - найбільш поширений форм-фактор пристроїв, званий також камера стандартного дизайну або Box camera. Переважаюче кількість пристроїв даного типу поставляється без об'єктива і кріплення, залишаючи споживачеві можливість найбільш гнучкого конфігурування пристрою, при використанні з термокожухом можливе використання пристрою поза приміщенням.

Мініатюрна відеокамера, Dome camera - являє собою півсферу або кулю, прикріплений до основи. Може бути виконана як з пластика, так і з металу.

Модульна відеокамера - бескорпусном пристрій у вигляді одношарової друкованої плати, найбільш поширений розмір 32 × 32 мм, призначена для установки в термокожухи, півсфери.

Керовані - комбінований пристрій, що складається з камери, трансфокатора і поворотного пристрою. Найбільшого поширення набули так звані інтегровані камери, виконані у вигляді купола.

Гіростабілізовані відеокамери - відеокамери, які використовуються на рухомих об'єктах з метою отримання стабілізованого зображення.

За типом вихідного сигналу відеокамери підрозділяють на аналогові і цифрові. Більшість цифрових камер передають сигнал за стандартною комп'ютерної мережі типу Ethernet - так звані IP-камери.

За способом передачі даних відеокамери діляться на дротові і бездротові. Бездротові мають в своєму функціоналі передавальний пристрій і антену. Бездротовими в тому числі є цифрові IP-камери, що передають зображення по радіоканалу мережі Wi-Fi - так звані Wi-Fi-відеокамери.

3.2 Охоронна сигналізація

При здійсненні правопорушення або недозволених дій, в деяких випадках може здійнятися охоронна сигналізація. Охоронна сигналізація може бути пристроєм, який при порушенні починає голосити на проблемній ділянці чи на пункті охорони.

Охоронна система розрахована на те щоб попередити про порушення несанкціонованого доступу в приміщення або при незаконних чи небезпечних ситуаціях.

Звичайно до охоронної сигналізації також входять різноманітні датчики для протидії з порушеннями.

В основу принципу дії будь-якого датчика покладено визначення та реєстрація впливу на прилад певних факторів, після чого формується сигнал. Залежно від характеру виникають впливів розрізняють наступні типи пристроїв:

До магнітно-контактних датчиків відносяться пристрої, що реагують на відкривання вікон, дверей та інших можливих проходів в приміщення за допомогою магнітних установок - геркона і магніту. Принцип дії полягає в тому, що в пасивному стані контакти між собою знаходяться в замкнутому положенні, а при активних діях зловмисників контакти розмикаються і активується передача сигналу;

Інфрачервоні датчики, основним завданням подібних датчиків є фіксація змін обстановки в робочому діапазоні пристрою.

Найчастіше представлені прилади називають як датчики руху, які використовують як для внутрішнього, так і для зовнішнього контролю за територією або будівлею, що охороняється. Завдяки різноманітності моделей можна вибрати зовнішній охоронний датчик активної або пасивної групи.

Вібраційні датчики існують для забезпечення надійного захисту об'єкту охорони, використовують представлені датчики, що виключають ймовірність непомітного пролому, розбиття скляних поверхонь.

Завдяки наявності акустичних датчиків можна своєчасно виявити розбиття скла. Особливість його роботи полягає в перетворенні звукового сигналу в електричний.

Для безперебійної роботи пристроїв важливо враховувати умови подальшої експлуатації, тому для зовнішнього контролю необхідно встановлювати вуличний охоронний датчик. Він має більш міцний корпус, здатний захистити механізм від зовнішніх впливів, погодних умов і пилу.

Система пожежної сигналізації - установки пожежної сигналізації, змонтовані на одному об'єкті і контрольовані з загального пожежного поста. При цьому термін "пожежна сигналізація" означає процес отримання, обробки, передача і уявлення інформації про пожежу в заданому вигляді споживачам за допомогою автоматичної установки пожежної сигналізації.

Системи пожежної сигналізації є різновидом вимірювальних інформаційних систем, включають в себе вимірювальні пристрої та засоби обробки інформації. На відміну від більшості вимірювальних систем, установки пожежної сигналізації визначають не кількісне значення контрольованого параметра, а лише його відхилення в бік більше допустимої.

Обробка результатів зводиться в основному до отримання даних про місце виникнення небезпечної ситуації при пожарі. Вимоги до швидкодії систем є вкрай жорсткими поряд з майже повною відсутністю вимог до накопичення інформації.

Охоронна сигналізація забезпечує наступні заходи безпеки:

- виявлення зловмисника;
- поетапна оцінка ситуації;
- відеодокументування;
- реагування.

Сучасні системи безпеки зможуть своєчасно інформувати вас про проникнення сторонніх осіб на територію, що знаходиться під охороною.

Формування повної системи безпеки, яка включає у собі систему відеоспостереження, систему сигналізування та систему контролю доступу на основі кібер-університету, дозволяє забезпечити повномірне контролювання візитів на пропускних пунктах та запобігає основним проблемам неправомірного руху та ідентифікації осіб.

Система безпеки не обмежується тільки пропускними пунктами, камерами, сигналізацією. Використання датчиків,обробка даних зберігання та правила управління. Встановлення замків до кабінетів це все розширює функціонал і коректність роботи системи безпеки.

При необхідності надання повноважень доступу в кабінети/аудиторії в яких встановлені електронні або магнітні замки необхідно включати всі три категорії систем на ділянку,встановлювати відповідні правила для аналізу даних та забезпечувати особам відповідний статус.

4 ІНФОРМАЦІЙНА БЕЗПЕКА

Інформаційна безпека, як сфера зайнятості, значно розвинулася і виросла в останні роки. У ній виникло безліч професійних напрямків, наприклад, таких, як безпека мереж і пов'язаної інфраструктури, захисту програмного забезпечення та баз даних, аудит інформаційних систем, виявлення електронних записів.

Інформаційна безпека - практика запобігання несанкціонованому доступу, використання, розкриття, спотворення, зміни, дослідження, записи або знищення інформації.

Це універсальне поняття застосовується незалежно від форми, яку можуть приймати дані (електронна або, наприклад, фізична). Основне завдання інформаційної безпеки - збалансована захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації.

Це досягається, в основному, за допомогою багатоетапного процесу управління ризиками, який дозволяє ідентифікувати основні засоби та нематеріальні активи, джерела загроз, уразливості, потенційну ступінь впливу і можливості управління ризиками. Цей процес супроводжується оцінкою ефективності плану з управління ризиками.

В основі інформаційної безпеки лежить діяльність по захисту інформації - забезпечення її конфіденційності, доступності та цілісності, а також недопущення будь-якої компрометації в критичній ситуації.

До таких ситуацій належать природні, техногенні і соціальні катастрофи, комп'ютерні збої, фізичне викрадення і тому подібні явища. У той час, як діяльність більшості організацій в світі досі базується на паперових документах, що вимагають відповідних заходів забезпечення інформаційної безпеки, спостерігається неухильне зростання числа ініціатив по впровадженню цифрових технологій в університеті.

4.1 Загрози і заходи протидії

Загрози інформаційної безпеки можуть приймати різноманітні форми. Найбільш серйозними вважаються загрози пов'язані з «злочином як послугою», Інтернетом речей, ланцюгами поставок і ускладненням вимог регуляторів. «Злочин як послуга» є модель надання зрілими злочинними співтовариствами пакетів кримінальних послуг на даркнет-ринку за доступними цінами початківцям кіберзлочинцям.

Це дозволяє здійснювати хакерські атаки, раніше недоступні через високу технічну складність або дорожнечі, роблячи кіберзлочинність масовим явищем. Організації активно впроваджують Інтернет речей, пристрої якого часто спроектовані без урахування вимог безпеки, що відкриває додаткові можливості для атаки. До того ж, швидкий розвиток і ускладнення Інтернету речей знижує його прозорість, що в поєднанні з нечітко визначеними правовими нормами і умовами дозволяє організаціям використовувати зібрані пристроями персональні дані своїх клієнтів на власний розсуд без їх відома. Крім того, для самих організацій проблематично відстежувати, які із зібраних пристроями Інтернету речей даних передаються у поза. Загроза ланцюгів поставок полягає в тому, що організації, як правило, передають своїм постачальникам різноманітну цінну і конфіденційну інформацію, в результаті чого втрачають безпосередній контроль над нею. Таким чином, значно зростає ризик порушення конфіденційності, цілісності або доступності цієї інформації. Все нові і нові вимоги регуляторів значно ускладнюють управління життєво-важливими інформаційними активами організацій. Наприклад, введений в дію в 2018 році в Євросоюзі Загальний регламент захисту персональних даних, вимагає від будь-якої організації в будь-який момент часу на будь-якій ділянці власної діяльності або ланцюга поставок, продемонструвати, які персональні дані і для з якою метою є там в наявності, як вони обробляються, зберігаються і захищаються. Причому ця інформація повинна бути надана не

тільки в ході перевірок уповноваженими органами, а й на першу вимогу приватної особи - власника цих даних. Дотримання такого комплексу вимагає відволікання значних бюджетних коштів і ресурсів від інших завдань інформаційної безпеки організації. І хоча впорядкування обробки персональних даних передбачає в довгостроковій перспективі поліпшення інформаційної безпеки, в короткостроковому плані ризики організації помітно зростають.

Основними способами протидії загрозам інформаційної безпеки або інформаційним ризикам є:

– зниження - впровадження заходів безпеки і протидії для усунення вразливостей і запобігання загрозам;

– передача - перенесення витрат, пов'язаних з реалізацією загроз на третіх осіб: страхові або аутсорсингові компанії;

– прийняття - формування фінансових резервів у разі, якщо вартість реалізації заходів безпеки перевищує потенційний збиток від реалізації загрози;

– відмова - відмова від надмірно ризикованої діяльності.

4.2 Тріада CIA

Порушення безпеки поділяється на три основні категорії: неавторизоване розкриття інформації, неавторизоване зміна інформації і неавторизований відмову в доступі до інформації. Пізніше ці категорії отримали короткі найменування і стандартизовані визначення:

– confidentiality - «конфіденційність» - властивість інформації бути недоступною або закритою для неавторизованих осіб, сутностей або процесів;

– integrity - «цілісність» - властивість збереження правильності і повноти активів;

– availability - «доступність» - властивість бути доступним і готовим до використання за запитом авторизованого суб'єкта.

У сукупності ці три ключові принципи інформаційної безпеки іменуються тріадою CIA (рисунок 4.1).

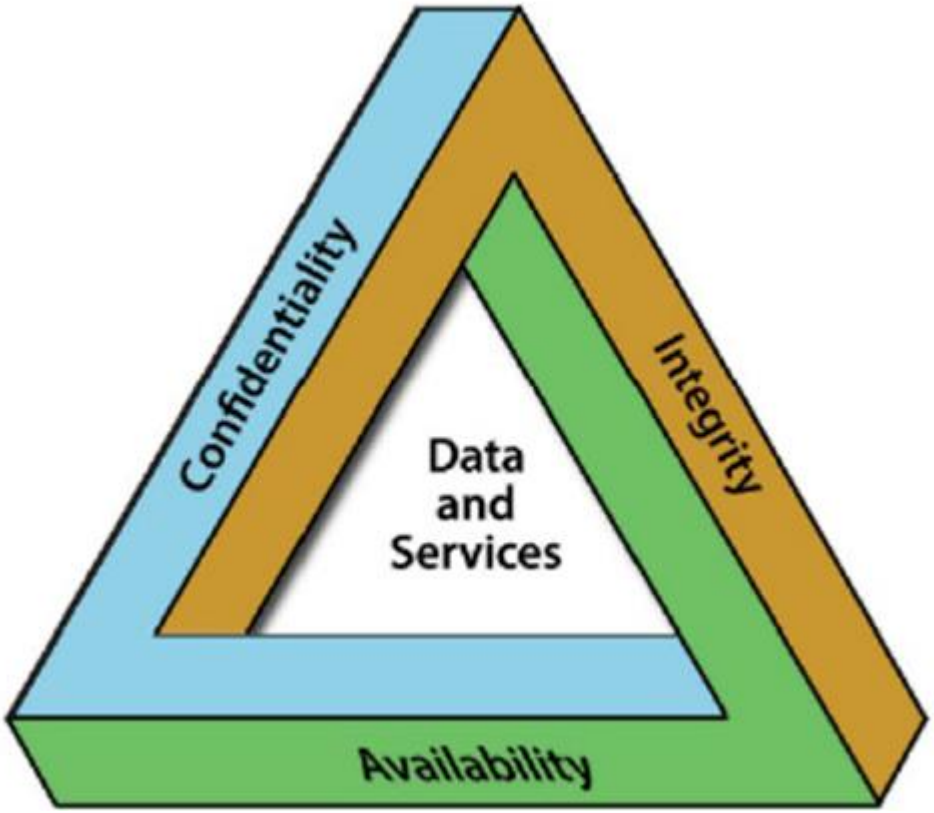

Рисунок 4.1 – тріада CIA

Вона зафіксована в національних і міжнародних стандартах і увійшла в основні освітні та сертифікаційні програми з інформаційної безпеки, такі як CISSP і CISM. Деякі російські автори використовують кальку з нього - «тріада КЦД». В літературі все її три складових: конфіденційність, цілісність і доступність синонімічно згадуються, як принципи, атрибути безпеки, властивості, фундаментальні аспекти, інформаційні критерії, найважливіші характеристики або базові структурні елементи.

Тим часом, не припиняються дебати про відповідність тріади CIA стрімко розвиваються технологій і вимогам бізнесу. В результаті цих

дискусій з'являються рекомендації про необхідність установки взаємозв'язку між безпекою та недоторканністю приватного життя, а також затвердження додаткових принципів. Деякі з них вже включені в стандарти Міжнародної організації по стандартизації (ISO):

– справжність - властивість, що гарантує, що суб'єкт або ресурс ідентичні заявленим;

– підзвітність - відповідальність суб'єкта за його дії і рішення;

– неможливість відмови - здатність засвідчувати мало місце подія або дія і їх суб'єкти так, щоб ця подія або дія і суб'єкти, які мають до нього відношення, не могли бути поставлені під сумнів;

– достовірність - властивість відповідності передбаченому поведінки і результатів.

Конфіденційність інформації досягається наданням до неї доступу с найменшими привілеями виходячи з принципу мінімальної необхідної поінформованості. Іншими словами, авторизована особа повинна мати доступ тільки до тієї інформації, яка йому необхідна для виконання своїх посадових обов'язків. Злочини проти недоторканності приватного життя, такі, як крадіжка особистості, є порушеннями конфіденційності.

Однією з найважливіших заходів забезпечення конфіденційності є класифікація інформації, яка дозволяє віднести її до строго конфіденційної, або призначеної для публічного, або внутрішнього користування

Шифрування інформації - характерний приклад одного із засобів забезпечення конфіденційності

Чітке здійснення операцій або прийняття вірних рішень можливо лише на основі достовірних даних, що зберігаються в файлах, базах даних або системах, або трансльованих по комп'ютерних мережах. Іншими словами, інформація повинна бути захищена від навмисного, несанкціонованого або випадкового зміни в порівнянні з вихідним станом, а також від будь-яких спотворень в процесі зберігання, передачі або обробки. Однак її цілісності

загрожують комп'ютерні віруси і логічні бомби, помилки програмування і шкідливі зміни програмного коду, підміна даних, неавторизований доступ.

Крім навмисних дій, в багатьох випадках неавторизовані зміни важливої інформації виникають в результаті технічних збоїв або людських помилок через помилку або через недостатню професійну підготовку. Наприклад, до порушення цілісності ведуть: випадкове видалення файлів, введення помилкових значень, зміна налаштувань, виконання некоректних команд, причому, як рядовими користувачами, так і системними адміністраторами.

Для захисту цілісності інформації необхідно застосування безлічі різноманітних заходів контролю і управління змінами інформації і обробних її систем. Типовим прикладом таких заходів є обмеження кола осіб з правами на зміни лише тими, кому такий доступ необхідний для виконання службових обов'язків.

При цьому слід дотримуватися принципу розмежування повноважень, згідно з яким зміни в дані або інформаційну систему вносить одна особа, а підтверджує їх або відхиляє - інша. Крім того, будь-які зміни в ході життєвого циклу інформаційних системи повинні бути узгоджені, протестовані на предмет забезпечення інформаційної цілісності та внесені в систему тільки коректно сформованими транзакціями.

Оновлення програмного забезпечення необхідно здійснювати з дотриманням заходів безпеки. Будь-які дії, що тягнуть зміни, повинні бути обов'язково протокольовані.

Згідно з цим принципом, інформація повинна бути доступна авторизованим особам, коли це необхідно. Основними факторами, що впливають на доступність інформаційних систем, є DoS-атаки, атаки програм-вимагачів, саботаж.

Крім того, джерелом загроз доступності є ненавмисні людські помилки через помилку або через недостатню професійну підготовку: випадкове видалення файлів або записів в базах даних, помилкові настройки систем;

відмова в обслуговуванні в результаті перевищення допустимої потужності або нестачі ресурсів устаткування, або аварій мереж зв'язку; невдало проведений оновлення апаратного або програмного забезпечення; відключення систем через аварії енергопостачання. Істотну роль в порушенні доступності грають також природні катастрофи: землетруси, смерчі, урагани, пожежі, повені і тому подібні явища.

У всіх випадках кінцевий користувач втрачає доступ до інформації, необхідної для його діяльності, виникає вимушений простій. Критичність системи для користувача і її важливість для виживання організації в цілому визначають ступінь впливу часу простою.

Недостатні заходи безпеки збільшують ризик ураження шкідливими програмами, знищення даних, проникнення через поза або DoS-атак. Подібні інциденти можуть зробити системи недоступними для звичайних користувачів.

Термін «неможливість відмови» - неправомірну відмову від зобов'язань. У контексті комп'ютерної безпеки це може бути, наприклад, заперечення однією із сторін факту відправки, прийому, авторства, або змісту електронного повідомлення.

В контексті інформаційної безпеки «неможливість відмови» розуміється як підтвердження цілісності та оригінального походження даних, що виключає можливість підробки, яке може бути в будь-який момент перевірено сторонніми особами, або як встановлення ідентичності (особистості, документа, об'єкта), яке з високим ступенем достовірності може вважатися справжнім і не може бути спростовано

4.3 Безпека туманних обчислень

Туманні обчислення використовуються для підвищення зручності використання хмарної платформи і збільшення її потенціалу.

З появою широкої застосовності туману і аналогічних технологій, таких як граничні обчислення (Edge computing), хмарки (Cloudlets) і мікроцентр даних (Micro-data center), збільшується і кількість атак, які можуть поставити під загрозу конфіденційність, цілісність і доступність інформації, що обробляється в них.

Ці проблеми безпосередньо впливають на розподілений, загальний характер хмарних обчислень. Будучи віртуалізованим середовищем, такий же як хмара, платформа туману також може бути порушена тими ж погрозами.

Безпека туманних обчислень це практика запобігання несанкціонованому доступу,використання,розкриття,спотворення,зміни, дослідження,записи або знищення інформації,що обробляється в інфраструктурі туманних обчислень.

Основне завдання безпеки туманних обчислень - збалансована захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності інфраструктури.

Це досягається, в основному, за допомогою багатоетапного процесу управління ризиками, який дозволяє ідентифікувати основні засоби та нематеріальні активи, джерела загроз, уразливості, потенційну ступінь впливу і можливості управління ризиками.

Після визначення критичних проблем безпеки, характерних для конкретної реалізації інфраструктури туманних обчислень, виробляються необхідні політики безпеки, розробляються і реалізуються стратегії з метою зниження ймовірності реалізації ризику і мінімізації можливих негативних наслідків.

Цей процес супроводжується оцінкою ефективності плану з управління ризиками.

4.4 Програмно-технічні засоби забезпечення інформаційної безпеки

Першим етапом для забезпечення інформаційної безпеки є захист від некоректного та неправомірного доступу. Для запобігання подібних проблем є декілька захисних засобів. До відповідних протидій входять засоби авторизації. Ресурсом або системою повинна надаватися змога авторизуватися особі, яка планує потрапити на територію університету.

Авторизація - надання певній особі або групі осіб прав на виконання певних дій; а також процес перевірки даних прав при спробі виконання цих дій. Часто можна почути вираз, що якийсь чоловік «авторизований» для виконання даної операції - це значить, що він має на неї право.

Авторизацію не слід плутати з аутентифікацією - процедурою перевірки легальності користувача або даних, наприклад, перевірки відповідності введеного користувачем пароля до облікового запису паролю в базі даних, або перевірка цифрового підпису листи по ключу шифрування, або перевірка контрольної суми файлу на відповідність заявленої автором цього файлу. Авторизація ж виробляє контроль доступу до різних ресурсів системи в процесі роботи легальних користувачів після успішного проходження ними аутентифікації.

Система повинна надавати різні рівні доступу до особистих даних та їх управління залежно від ролі управляючого, повинне існувати чітке розмежування обов’язків. Усі дії, зміна даних або зміна у системі повинні документуватися та вноситися до аудиту. Мандатне управління доступом - розмежування доступу суб'єктів до об'єктів, засноване на призначення мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допуску) суб'єктам на звернення до інформації такого рівня конфіденційності.

Кожна система повинна виявляти та запобігати вторгненням та витокам інформації. Подібні маніпуляції виконує система моніторингу мереж.

Для того щоб не втратити дані через неочікувані збої впроваджується система резервного копіювання та автоматичного збереження інформації. Подібна система копіює дані на віддалені сервери чи фізичну пам’ять ,при внесенні змін до даних ,вони автоматично зберігаються. Але не завжди вистачає тільки копіювання даних. При ситуації різкого перепаду чи втрати напруги, подібні системи можуть не встигнути зреагувати.

Щоб вирішити цю проблему, формують систему безперебійного живлення, яка складається з трансформаторів, акумуляторів та генераторів,залежно від розміру системи, виконують розмежування навантаження.

Системи аутентифікації повинні правильно зчитувати дані при спробі потрапити на територію або будівлю, ідентифікувати особу. Особа може аутетифікуватися та підтвердити свою належність до структури ключем доступу, картою, біометрією, залежно від зчитувачів.

Для швидкого виявлення порушника або своєчасного реагування на спробу проникнути до інфраструктури, без прав доступу, впроваджуються засоби контролю та управління доступом. Тільки працівники або студенти університету, які зареєстровані у системі мають право доступу.

Кожна система повинна перевірятися на коректність роботи завдяки засобам аналізу систем захисту, зазвичай через встановлений інтервал часу.

Для забезпечення безпеки програм використовують антивіруси. Антивірусна програма – спеціалізована програма для виявлення комп'ютерних вірусів, а також небажаних програм і відновлення заражених такими програмами файлів і профілактики - запобігання зараженню файлів або операційної системи шкідливим кодом.

5 СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

5.1 Можливості СКУД

СКУД представляє собою сукупність програмно-апаратних технічних коштів контролю та коштів управління, маючих за ціль обмеження та реєстрацію входу-виходу об’єктів (людей або транспорту) на заданій території через ” точки проходу ” : двері ,ворота,КПП.

Основною задачею будь-якого СКУД є управління доступом на задану територію. Включаючи :

- обмеження доступу на задану територію;
- фіксування пересування.

За допомогою системи контролю доступу досягається:

- ідентифікація осіб, що мають право доступу;
- розмежування доступу до різних приміщень;
- керування автоматичними режимами;
- реєстрація часу перебування особи на об’єкті;
- обробка інформації та ведення статистики.

Впровадження СКУД дозволяє організувати безпеку та контроль об’єктів. Ідентифікування без залучення великої кількості працівників охорони та стабільну роботу автоматизованих систем у режимі 24/7 (рисунок 5.1).

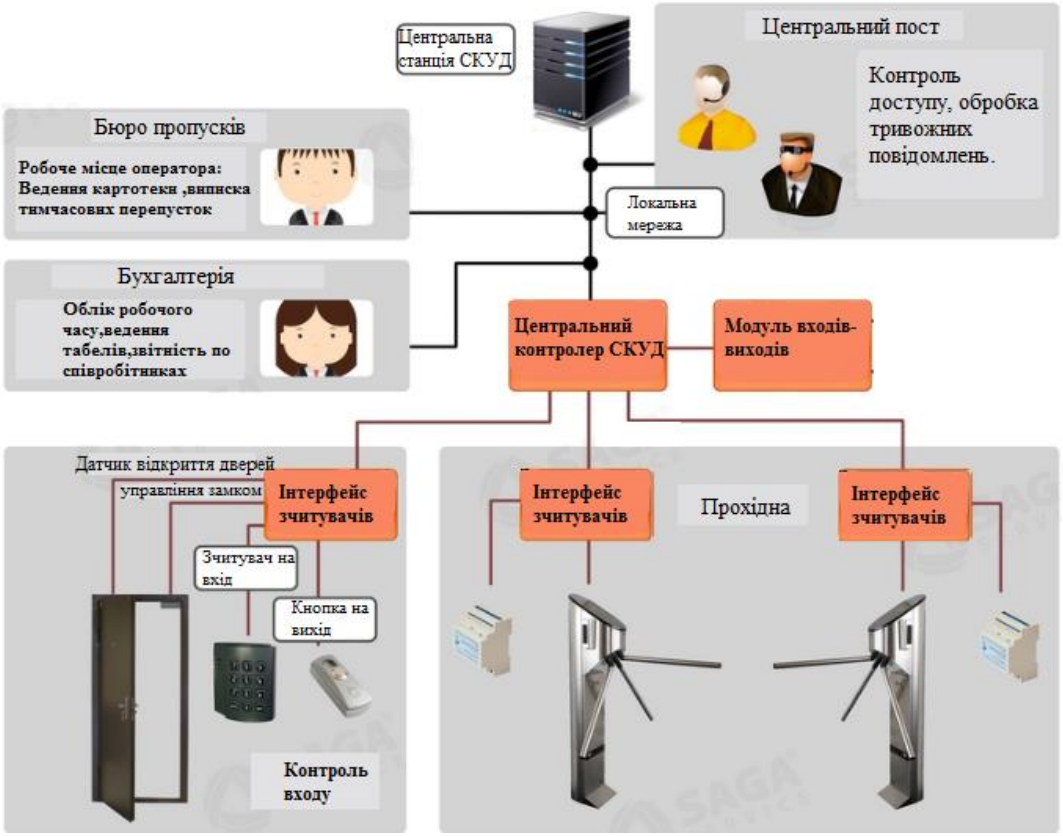

Рисунок 5.1 – Структура інтегрованої СКУД

Також важливою складовою є інтеграція з системою безпеки:

– з системою відео спостереження для суміщення архівів подій систем,передачі камерам сигналу про необхідність починати запис для фіксування підозрілих дій;

– з системою охоронної сигналізації, для обмеження доступу до приміщення, які знаходяться під охороною;

– з системою пожарного сигналізування, для отримання інформації про стан пожежних сирен, автоматичного розблокування евакуаційних виходів.

На об’єктах з високою відповідальністю мережа пристроїв СКУД виконується фізично не зв’язано з іншими інформаційними мережами.

До основних функціональних можливостей відносяться: можливість оперативного перепрограмування. схемно-технічний і програмний захист від вандалізму і саботажу; високий рівень секретності; автоматична

ідентифікація;розмежування повноважень співробітників і відвідувачів по доступу в приміщення і на об'єкт в цілому; надійне механічне замикання контрольованих місць з можливістю аварійного ручного відкриття; автоматичний збір і аналіз даних; вибіркове роздрукування даних.

За технічними характеристиками і функціональними можливостями СКУД умовно підрозділяються на чотири класи. Залежно від особливостей об'єкту, конфігурації СКУД, фірми виробника набір функцій в кожному класі може змінюватися і доповнюватися функціями з інших класів.

5.2 Класифікація СКУД

Якість СКУД формується основними технічними характеристиками і функціональними можливостями. Основними технічними характеристиками є:

- ступінь та рівень ідентифікації;
- кількість контрольних пунктів;
- пропускна спроможність системи;
- кількість користувачів;
- умови використання;
- інфраструктура.

За умовами використання розрізняють системи для роботи:

- чи закриті та опалювані приміщення;
- під навісом на вулиці в умовах помірно-холодного клімату;
- на вулиці в умовах помірно-холодного клімату;
- у особливих умовах (підвищена вологість, запилена і тому подібне).

5.3 Обладнання та принцип роботи

5.3.1 Ідентифікатор

Основні типи виконання - картка, брелок, мітка. Є базовим елементом системи контролю доступу, оскільки зберігає код, який служить для визначення прав власника. Це може бути Touch memory, безконтактна картка, або застаріваючий тип карт із магнітною смугою.

В якості ідентифікатора може виступати так само код, що вводиться на клавіатурі, а також окремі біометричні ознаки людини - відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення обличчя.

Надійність системи контролю доступу в значній мірі визначається типом використовуваного ідентифікатора: наприклад, найбільш поширені безконтактні карти proximity можуть вдавати в майстернях з виготовлення ключів на обладнанні, що є у вільному продажу. Тому для об'єктів, що вимагають вищого рівня захисту, подібні ідентифікатори не підходять. Принципово вищий рівень захищеності забезпечують RFID-мітки, в яких код карти зберігається в захищеній області і шифрується.

Крім безпосереднього використання в системах контролю доступу, RFID-мітки широко застосовуються і в інших областях. Наприклад, в локальних розрахункових системах (оплата обідів в їдальні та інших послуг), системах лояльності і так далі.

5.3.2 Контролер

Автономний контролер - це «мозок» системи: саме контролер визначає, пропустити чи ні власника ідентифікатора в двері, оскільки зберігає коди ідентифікаторів зі списком прав доступу кожного з них у власній незалежній пам'яті. Коли людина пред'являє (підносить до зчитувального пристрою) ідентифікатор, лічений з нього код порівнюється з зберігаються в базі, на підставі чого приймається рішення про відкриття дверей.

Мережевий контролер об'єднується в єдину систему з іншими контролерами і комп'ютером для можливості централізованого контролю і управління. У такому випадку рішення про надання доступу може прийматися як контролером, так і програмним забезпеченням головного комп'ютера. Найчастіше об'єднання контролерів в мережу здійснюється за допомогою промислового інтерфейсу RS-485 або локальної мережі Ethernet.

У випадках, коли необхідно забезпечити роботу контролера при аваріях електромережі, блок контролера забезпечується власним акумулятором, або зовнішнім блоком резервного живлення.

Час роботи від акумулятора може зайняти від декількох годин до декількох діб (рисунок 5.2).

Рисунок 5.2 – Контролер E500U

Інформація яка надходить до контролера надалі зберігається в пам’яті системи. Подальше використання даних надає змогу в різних аспектах, а саме

складання звітів, ведення статистики відвідуваності університету, врахування робочого часу та часу відвідувань.

5.3.3 Зчитувач

Зчитувачем є пристрій, задачею якого є зчитування даних з ID-карт для ідентифікації особи, після піднесення до відповідної ділянки. Після зчитування код передається до контролеру. Принцип роботи зчитувачів інтегрованих СКУД залежить від типів карт які він обробляє. Наприклад, якщо переносний ідентифікатор у формі пластикової або силіконової таблетки з чіпом, зчитувач являє собою два контакти у відповідній формі.

Для біометричних ідентифікацій зчитувач повинен містити в своєму функціоналі камеру.

При потрібності установки зчитувача ззовні будівлі, треба враховувати різні кліматичні та фізичні подразники, які можуть суттєво вплинути на коректність роботи компоненту (рисунок 5.3).

Рисунок 5.3 – Зчитувач

5.3.4 Конвертери середовища

Конвертери середовища необхідні для зв’язування елементів системи СКУД між собою та головним виконуючим комп’ютером.

В деяких подібних системах вже існує Ethernet, який дає змогу легко та без додаткових компонентів виконувати подібний зв’язок між компонентами та головним виконуючим комп’ютером. Це задовольняє умови при якій контрольний пункт знаходиться в одному місці і не вимагає великої кількості ресурсів.

5.3.5 Програмне забезпечення

Не є обов'язковим елементом системи контролю доступу, використовується в разі, коли потрібна обробка інформації про проходах, побудова звітів, або коли для початкового програмування, управління та збору інформації в процесі роботи системи необхідно мережеве програмне забезпечення, яке встановлюється на один або кілька ПК, з'єднаних в мережі.

Зазвичай програмне забезпечення впроваджується для обробки та контролю великої кількості компонентів, аналізу даних та виконанні великої кількості функціоналу.

5.3.6 Пристрої для регулювання входу та виходу

Коли потребується забезпечувати обмеження доступу до аудиторій чи службових кабінетів, існують електромагнітні замки та електромеханічні замки, які встановлюються на вхідні двері.

При використанні електромагнітних замків, враховується що вони працюють від напруги. В свою чергу електромеханічні більш міцніші та стійкіші, та регулюються вбудованим в замок клапаном.

Коли потребується регулювати рух в коридорах, проїздах чи проходах,найчастіше використовуються турнікети. Подібні компоненти що встановлюються на широкому просторі слід розглядати в проектованому прикладі, разом з електромагнітними замками для допуску в аудиторії.

Турнікети можна розглядати двох типів: поясні, тобто висотою до одного метру та турнікети повного зросту ,висотою більше ніж півтора метри. Зазвичай турнікети повного зросту використовуються в ситуаціях коли необхідно забезпечити більшу безпеку. Тому в роботі розглядається перший варіант подібних пристроїв (рисунок 5.4).

Рисунок 5.4 – Турнікет

Якщо умовна інфраструктура включає в наявність в'їзду на територію або паркову, слід розглядати ймовірність впровадження автоматично або механічно регулюючих воріт або шлагбаумів. Які частіше за все встановлюються на в'їздах до території.

При цьому якщо встановлення подібних компонентів на відкритій ділянці, то слід зауважити що системи які реагують на транспорт та управляють відкриттю або закриттю шлагбауму повинні бути міцними та готовими до експлуатації в різні кліматичні умови.

Контроль доступу на подібних ділянках працює інакше. Система повинна виконувати деякі додаткові умови зчитування та ідентифікації номерних знаків або використовувати датчики руху, які будуть змушувати реагувати систему при наближенні транспорту до пропускного пункту.

Для запобігання несанкціонованого проїзду транспорту через подібні пункти існують різноманітні бар'єри.

5.4 Огляд існуючих систем

Різноманіття наявних на ринку виробників СКУД обумовлено спробою задовольнити безліч потреб замовників. У кожного виробника свій напрямок діяльності по функціоналу обладнання і програмного забезпечення. Хтось пропонує великі, складні сі-стеми, що підтримують інтеграцію з пожежними системами, системами відеоспостереження, і т.д., а хтось має спрямованість на невеликі будівлі і приміщення з невеликим числом співробітників.

Розглянемо характеристики найбільш потужних, з точки зору можливостей розширення і інтеграції в автоматизовані системи підприємства, СКУД представлених на ринку.

З моменту свого заснування в 2001-му році, компанія SALTO Systems, Іспанія, пройшла шлях від новачка до визнаного лідера в області розробки і виробництва сучасних інноваційних систем контролю доступу.

SALTO System запропонували ринку концепцію СКУД, засновану на власних розробках сучасних технологіях, таких як Віртуальна Мережа SALTO (SVN) і Бездротова СКУД (SALTO Wireless), а також лінійку інноваційних продуктів платформи XS4: електронні замки і циліндри, настінні зчитувачі і контролери , замки для шафок і підсистеми енергозбереження.

Suprema Inc. - глобальний лідер ринку біометричних технологій безпеки. Компанія Suprema здатна постійно розробляти і виробляти надійні продукти, які є лідерами у своїй галузі. Великий портфель продукції Suprema включає в себе термінали СКУД і УРВ, сканери відбитків пальців для цивільної ідентифікації, що вбудовуються модулі відбитків пальців, а також програмні платформи, що дозволяють ефективно вести облік робочого часу і

відвідуваності. Нове покоління терміналів СКУД і УРВ Suprema додатково підтримують функцію виявлення підроблених відбитків.

СКУД Suprema забезпечує максимальну зручність і безпеку для користувачів шляхом вирішення проблем інших традиційних систем контролю доступу, в яких застосовуються радіочастотні карти або паролі. Відбиток пальця неможливо втратити, забути вдома або передати колезі.

Системи можуть працювати в умовах як невеликих, так і дуже великих підприємств, а купивши спочатку один модуль для системи контролю доступу (СКД), споживач завжди може доповнити його системою відеоспостереження, охоронної, пожежної сигналізації та ін. Охоронними системами.

Слід зазначити, що більшість виробників СКУД не пропонують типових рішень. Архітектура конкретного проекту ґрунтується на за потребою замовника. У більшості випадків на ринку пропонується обладнання, що дозволяє конструювати системи під будь-які потреби.

5.4.1 Централізовані системи

Залежно від поставлених задач та обсягів охоплення території для пунктів надання доступу існують два типи систем контролю та управління: централізовані системи та автономні.

Використовуючи централізовані системи спершу треба проаналізувати об’єми та задачі системи. Подібні системи зручно впроваджувати на великих за площею об’єктах, в яких декілька пропускних пунктів та великий обсяг вхідних даних. В централізованих системах всі компоненти та контролери управляються за допомогою головного комп’ютера, який різними методами надає змогу управління великою кількістю дверей або турнікетів які включено до системи.

Існує ряд ситуацій коли централізовані системи незамінні у функціональності.

При необхідності обробляти складні алгоритми ідентифікації та допуску різноманітних осіб з різними видами функцій доступу та ідентифікації в різні контрольовані системою точки університету і мати необхідність змінювати дані в реальному часі.

Якщо треба забезпечити систему зберіганням та документуванням старої інформації. Прикладом може бути формування журналу відвідувань кожного з осіб які зареєстровані та внесені до бази. В такому випадку при вдалій ідентифікації можна відстежувати дані особи та всі його пересування через контрольний пункт.

При формуванні системи віддаленого моніторингу присутності студентів в аудиторіях або на території університету.

При взаємодії з іншими системами безпеки, як відео спостереження, сигналізування, дані з датчиків та інформаційна безпека.

Для керування централізованими системами є ймовірність формування спеціального відділу, який буде займатися адмініструванням, обробками даних та їх взаємодією з одного місця. Це свідчить про масштабність та вагомість подібних систем але тільки у випадку інтеграції на великих за площею об’єктах.

Подібне нововведення надає змогу управляти різними пунктами та робочими місцями, розділяти основні задачі системи на відповідальних за це людей.

Великим кроком вперед в сучасному управлінні централізованими системами СКУД є впровадження туманних обчислень, для швидкого реагування системи та зручною оптимізацією великої кількості інформації від відвідувачів.

Також популярним є впровадження хмарних або бездротових технологій для економії ресурсів на матеріали для формування СКУД на великих територіях.

Слід зазначити, що подібні інтеграції та нововведення слід реалізовувати при особливих ситуаціях, коли є необхідність в економії

ресурсів на впровадження системи великого масштабу в тому числі на витратні матеріали. Неможливість з'єднання декількох віддалених компонентів системи для обов'язкового рішення поставлених задач системі на великій відстані без прокладання кабелю локального зв'язку .

Можна перелічити декілька з'єднань які здатні виконати задачі системи не порушуючи цілісність роботи СКУД і інших інтегрованих підсистем.

Bluetooth представляє собою бездротове з'єднання компонентів для обміну даними в системі. Але суттєвим недоліком подібного з'єднання є мала відстань досяжності сигналу між компонентами, тобто неможливо з допомогою подібного зв'язку зв'язати елементи системи, які розташовуються на великій відстані між собою чи від керуючого пристрою. Подібне підключення виконує роль підключення Ethernet тільки з допомогою бездротового зв'язку.

Підключення Wi-Fi спроможне зв'язувати елементи підсистем, які знаходяться на відстані сотень метрів, що вирішує проблеми з якими не спроможний впоратися Bluetooth, але не завжди вистачає і такої відстані, тому перед інтеграцією подібних підключень треба враховувати всі ці фактори та враховувати приблизну відстань між об'єктами зв'язку.

Бездротове з'єднання GSM. Використовування GSM забезпечує майже повне покриття умовної території, та забезпечує зв'язок між компонентами підсистеми. Зв'язок може забезпечувати передачу інформації на великі відстані з допомогою GPRS. Типовим недоліком може бути швидкість передачі даних в великих об'ємах.

5.4.2 Автономні системи

Централізовані системи встановлюються на великих об'єктах для забезпечення та коректної роботи декількох пропускних пунктів та управління іншими підсистемами, але не завжди потрібно формувати повноцінну централізовану систему.

Автономні системи дають можливість вирішувати більш прості задачі, а саме інтегрувати часткову систему, реалізовуючи автономні пункти в довільних точках, які потребують контролю доступу. Рішенням в подібних ситуаціях є інтеграція автономного контролеру замість керуючого комп'ютера. Наслідком впровадження подібної системи є послідовне підключення деякої кількості точок доступу, які потребують контролю. Це дозволить контролеру самостійно обробляти певну кількість відвідувачів у різних місцях за менші витрати.

Подібну систему легко доповнювати та змінювати різноманітним функціоналом, не порушуючи загальну роботу.

Формування автономних систем займає менше часу та ресурсів. Легше контролювати вихідну систему не використовуючи при цьому велику кількість допоміжних компонентів. При цьому використовуючи управління контролером замість зв'язком з комп'ютером.

Але подібна простота автономних систем не дозволяє використовувати достатню обробку даних, як це можливо за допомогою комп'ютера у централізованих системах.

При необхідності забезпечити високою безпекою автономні системи слід дотримуватися умови ,що зчитувач даних знаходиться віддалено від контролеру для застереження злому та порушенню роботи електронного замку.

Система повинна мати резервне живлення, для коректної роботи контролеру при збоях загального живлення (рисунок 5.5). Для таких випадків в автономні системи інтегрують резервні генератори електроенергії або акумулятори (рисунок 5.6).

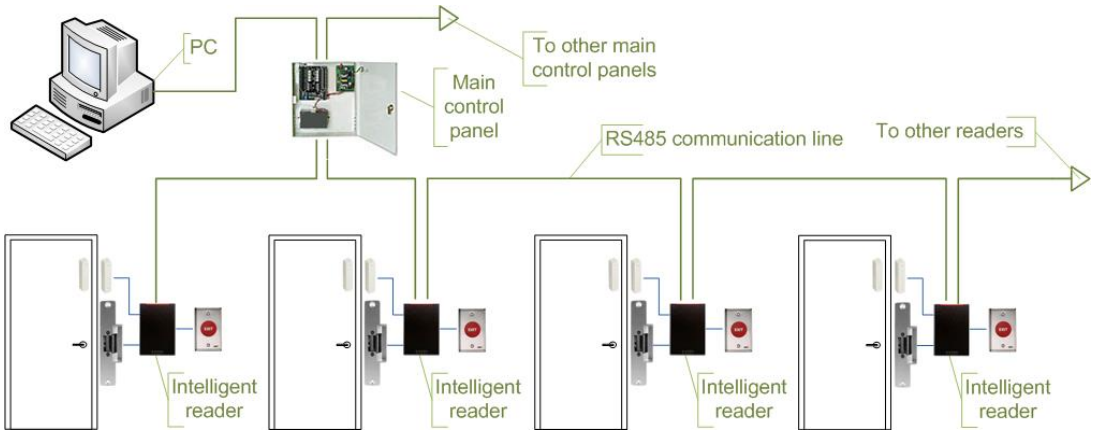

Рисунок 5.5 – Система контролю доступу з послідовним зв’язком

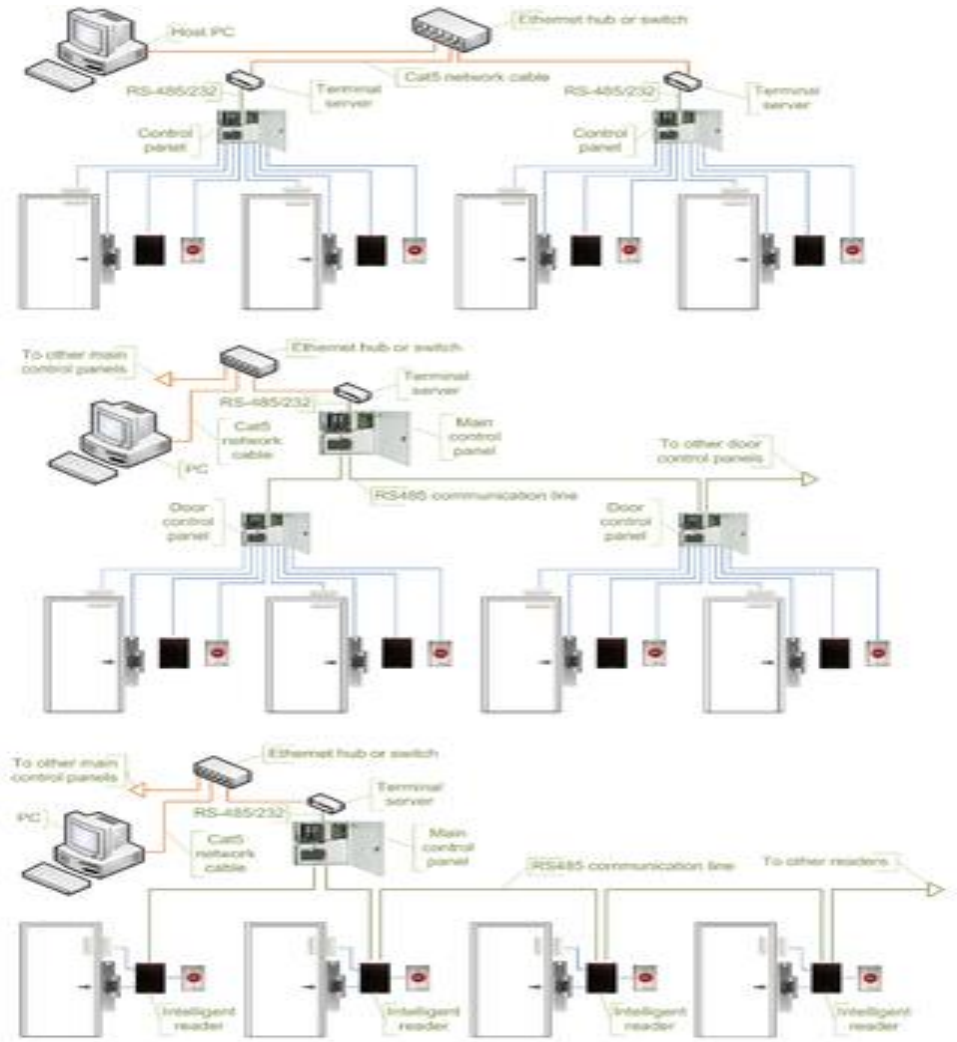

Рисунок 5.6 – СКД з використанням контролерів і серверів терміналів.

6 ПРОЕКТУВАННЯ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Інфраструктура позволяє моделювати систему СКУД на вхідних пунктах у двох наукових корпусах та на в'їзді на ділянку університету.

Відштовхуючись від різного місцезнаходження ділянок, запропоновано моделювати три підсистеми, які в свою чергу залежать від типу відвідувачів та від загальної(Глобальної бази відвідувачів). Кожна з підсистем має свій ідентифікаційний номер,та оброблює різні типи відвідувачів таких як:

- студент;
- відвідувач;
- викладач;
- адміністрація та персонал.

Глобальна база СКУД зберігає данні з усіх підсистем, данні в свою чергу формуються з ID особи та дати ,коли здійснився вхід на територію університету.

Глобальна база формується з усіх підсистем(прохідних пунктів), та сортує за часом відвідування, за ID – відвідувача та ID – контрольного пункту. Це може дозволити адміністратору звернутися до ID – особи та визначити через який пункт і коли, відвідувач потрапив на територію університету.

У кожного типу відвідувачів рекомендується вводити певну пропускну карту в зв'язку з різними повноваженнями та посадами. Виділяється особливий клас відвідувачів, ті які не працюють в закладі та не являються студентами університету.

Мається на увазі, що подібний критерій людей має тимчасову перепустку, яку отримують з сайту, якщо це конференція або ділова зустріч. Для обробки інформації людей, які не мають перепустки потрібен термінал,

який в свою чергу допомагає авторизуватися з внесенням особистих даних до бази відвідувачів,через заповнені поля форми.

Студенти мають відповідну карту, яка на контрольній точці допомагає ідентифікувати особу та реєструє відвідування.

Викладачі мають свою відповідну карту, яка окрім реєстрації та ідентифікації може надати допуск до аудиторій з електромагнітними замками, якщо такі є.

Співробітник університету не відрізняється новим функціоналом,теж можуть мати змогу допуску до кабінетів в яких працюють.

Залежно від типу карти, у кожного типу свій колір,для легшої класифікації відвідувачів. На адміністративній панелі де відображається та реєструється прохід, тип відвідувачів також виділяється відповідним кольором (рисунок 6.1).

Рисунок 6.1 – Схема проектованої СКУД

7 ТЕСТОВИЙ СЕРВІС СКУД

7.1 Реалізація підсистеми

Проектована система контролю та управління доступом,включає багато різних технологій та метрик для реалізації основних задач. Система повинна бути легко інтегрованою та спроможною розширювати свій функціонал.

Основними етапами тестової СКУД є :

– зчитування даних з носія;

– перевірка коректності вхідних даних;

– ідентифікація особи ,перевірка у базі даних;

– фіксування дати входу та виходу особи у будівлю університету;

– зберігання журналів пересування у базі даних.

Вхідними даними слугує інформація з чіп карт або мобільного телефону у вигляді JSON об’єкту.

JSON - текстовий формат обміну даними. Як і багато інших текстові формати, JSON легко читається людьми.

Незважаючи на походження від JavaScript, формат вважається незалежним від мови і може використовуватися практично з будь-якою мовою програмування. Для багатьох мов існує готовий код для створення і обробки даних в форматі JSON.

Запропонований вид представлення даних був вибраний з метою легко маніпулювати структурою файлу та для порівнянності з базою даних та мовою програмування.

Поля, які містить файл с вхідними полями,не являється остаточним варіантом, це означає що при необхідності доповнити чи змінити структуру для покращення функціоналу та проведенні більшої кількості логічних маніпулювань саме такий формат уявлення даних являється зручним для користування (рисунок 7.1).

Рисунок 7.1 – Тестові вхідні дані студента

Подібне уявлення даних є тестовим, але дозволяє моделювати відвідувачів, легко ідентифікувати особу, надавати права доступу, та класифікувати вхідні параметри, можливо легко встановити більшу кількість рядків об'єкту, або навпаки зменшити.

Згодом зчитувач,відправляє дані до тестової локальної програми,яка в свою чергу звертається до бази даних,шукає по полю "id" особу з таким же полем але у заздалегідь створені базі відвідувачів вузу.

Якщо даний відвідувач існує у базі даних,то формується ще один документ в який записується дата та час успішної ідентифікації.

Подібний блок СКУД реалізовувався на основі Node.js - програмна платформа, заснована на движку V8, який перетворює JavaScript.

Node.js додає можливість JavaScript взаємодіяти з пристроями введення-виведення через свій API, підключати інші зовнішні бібліотеки, написані на різних мовах, забезпечуючи виклики до них з JavaScript-коду. В основі бвблвотеки Node.js лежить концепт подієво-орієнтованого та асинхронного програмування.

З веб-серверу підключення відбувається до бази даних MongoDB - документоорієнтована система управління базами даних (СКБД) з відкритим вихідним кодом, яка не потребує опису схеми таблиць. Класифікована як NoSQL, використовує JSON-подібні документи і схему бази даних. Написана на мові C ++.

Система підтримує ad-hoc-запити: вони можуть повертати конкретні поля документів і призначені для користувача JavaScript-функції. Підтримується пошук за регулярними виразами. Також можна налаштувати запит на повернення випадкового набору результатів.Є підтримка індексів.

Система може працювати з набором реплік, тобто, містити дві або більше копії даних на різних вузлах. Кожен екземпляр набору реплік може в будь-який момент виступати в ролі основної або допоміжної репліки. Всі операції запису і читання за замовчуванням здійснюються з основною реплікою. Допоміжні репліки підтримують в актуальному стані копії даних. У разі, коли основна репліка дає збій, набір реплік проводить вибір, яка з реплік повинна стати основною. Другорядні репліки можуть додатково бути джерелом для операцій читання.

Система масштабується горизонтально, використовуючи техніку сегментування об'єктів баз даних – розподіл їх частин з різних вузлів кластера. Адміністратор вибирає ключ сегментування, який визначає, за яким критерієм дані будуть рознесені по вузлах (в залежності від значень хеш ключа сегментування). Завдяки тому, що кожен вузол кластера може приймати запити, забезпечується балансування навантаження.

Система може бути використана в якості файлового сховища з балансуванням навантаження і реплікацією даних. Надаються програмні засоби для роботи з файлами і їх вмістом.

В MongoDB відвідувачі формують собою документи набір яких утворює колекцію для зберігання даних які заносилися заздалегідь.

Після перевірки даних та зрівнянням в базі параметрів відвідувача, система генерує новий документ, в якому описуються час входу та виходу, а також ідентифікаційний номер власника журналу (рисунок 7.2).

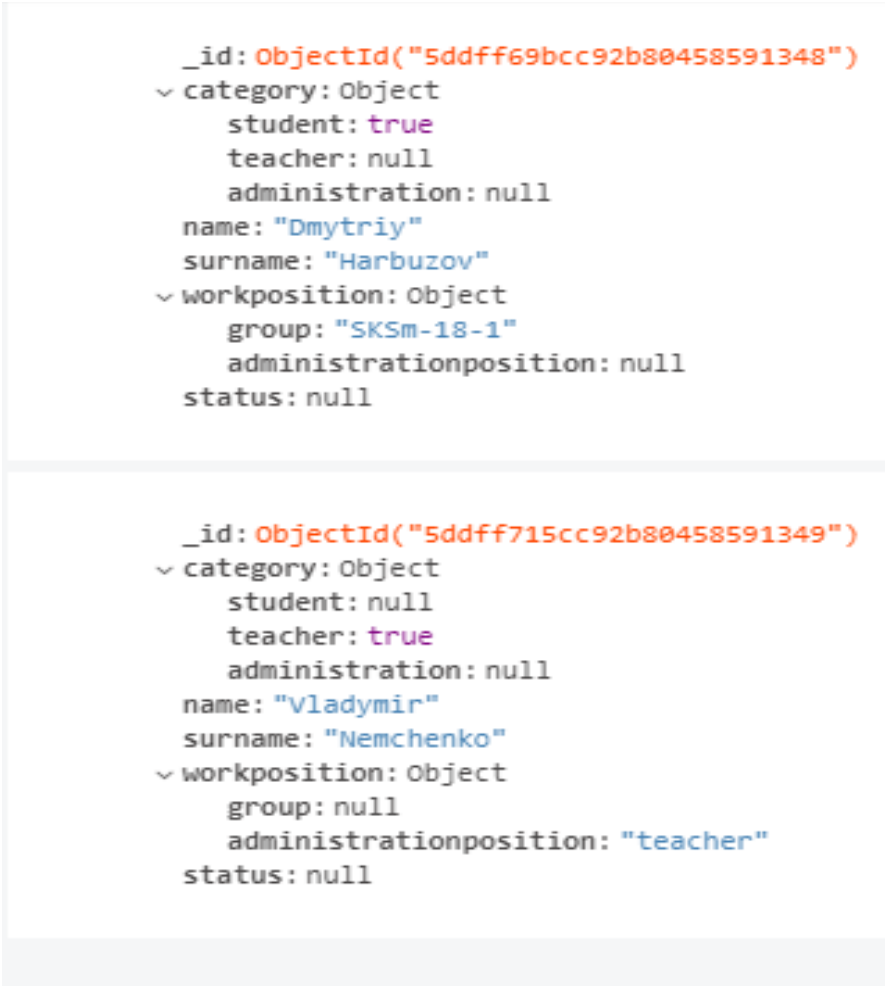

Рисунок 7.2 – Список усіх відвідувачів у базі даних

Таким чином при кожному успішному вході – виході особи через пункт, генерується кожен раз новий документ, а колекція представляє собою набір усіх візитів кожного відвідувача.

Крім того запис містить свій ідентифікаційний номер, який генерується самостійно базою даних MongoDB, містить поле з датою та часом успішного пересування через контрольний пункт.

Для зв’язком з колекцією відвідувачів, а саме с відвідувачем який умовно є в базі даних та проходить через пропускний пункт існує поле “owner_id”, яке прив’язує наш журнал до конкретної особи. Статус являє собою положення успішного пересування (рисунок 7.3).

Рисунок 7.3 – Журнал відвідування у базі даних

Умовою тестової системи є встановлення двох окремих терміналів на вхід і на вихід. Подібна умова дозволяє встановити двопоточний рух осіб, а також встановлювати контролювання та моніторинг пересування.

При виході особи через пропускний пункт зчитування здійснюється так само як і при вході.

До бази даних відправляється запит, по ідентифікаційному ключу особи, з колекції журналів пересування дістається останній сформований журнал, який став результатом успішного проходу, та записується час виходу до відповідного поля документу і зберігається.

7.2 Покращення та недоліки системи

Проектована система обробляє різноманітні типи відвідувачів, та вдало виконує основні функції надання доступу та ідентифікації осіб. Основними недоліками впровадження подібної системи є великі витрати на ресурси та необхідні технічні компоненти.

Інтегрування з системою відеоспостереження та системою сигналізації теж важкий але необхідний процес для більш якісного запобігання правопорушень та проникнень на територію чи будівлю університету.

Системи які маніпулюють великою кількістю даних важливим питанням залишається швидкодія та коректність роботи. Захист інформації та запобігання ризиків.

Для проектованої системи потрібно вводити спеціальні правила та норми управління даними. База даних повинна оновлюватися, студенти які закінчили навчання видаляються з реєстру, нові вносяться.

Окрім цього треба мати на увазі оптимізацію журналів відвідувань, дані повинні виноситися до віддалених серверів,чи на зовнішню пам’ять,щоб запобігти перевантаженню та великій обчислювальній складності.

Запропоновано використовувати туманні обчислення для оптимізації роботи з великою кількістю даних. Основна ідея туманних обчислень - з'єднати хмарні обчислення і IoT. Іншими словами, «туман» - це міст між хмарами і IoT

Частина даних буде оброблятися локально - на так званій кордоні, а частина піде в хмару.

До переваг туманних обчислень можна віднести:

– надають компаніям більше можливостей по обробці даних. У деяких випадках,наприклад,при забезпеченні безпеки (розпізнавання осіб);

– підключення машини повинні реагувати миттєво і не повинно бути ніяких затримок;

– дозволяють створювати мережеві з'єднання з низькою затримкою, а обробка частини даних на локальних пристроях зменшує необхідну пропускну здатність - адже якщо дані відправляти на обробку в хмару, а потім пересилати назад, це створить величезні потоки трафіку.

З огляду на особливості «туману», його можна використовувати в місцях, де пропускна здатність недостатня, тому дані обробляються в тому місці, де вони були створені.

Туман знайшов свою нішу в системах забезпечення безпеки - вони повинні миттєво реагувати на все, що відбувається в приміщенні. Затримки тут неприпустимі, тому доводиться обробляти частина даних локально

При інтеграції з іншими системами, як моніторинг та аналіз відвідуваності студентів чи персоналу, кількість вхідних даних та даних на обробку буде тільки зростати в геометричній прогресії. Не враховуючи відеоматеріали з камер спостереження і багато іншого.

Враховуючи необхідність оптимізації та обробки даних, необхідно проводити тестування коректності та швидкості роботи системи,моделюючи різні обставини.

Зазвичай жодна система не впроваджується у життя без тестування основних компонентів системи та їх зв’язку між собою та системою.

Для економії ресурсів на інтеграцію та встановлення подібних систем до інфраструктури на сьогоднішній день існують бездротові СКД які інтегруються у вже існуючі провідні системи для розширення доступу в середину об’єктів (рисунок 7.4).

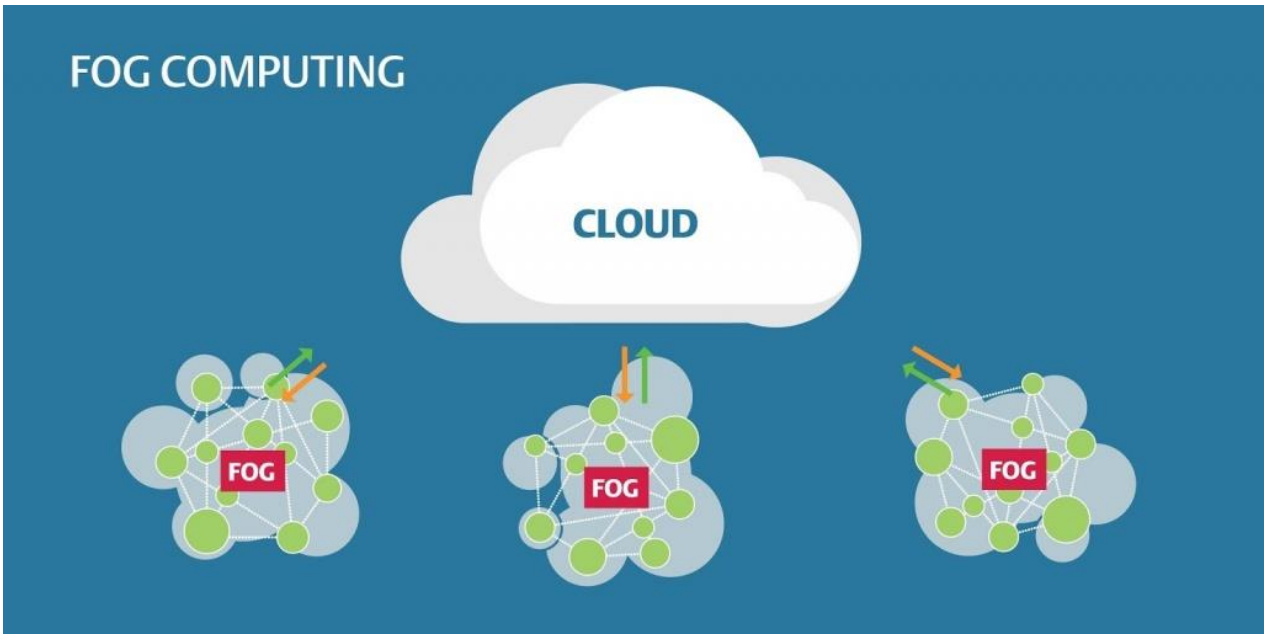

Рисунок 7.4 – принцип дії туманних обчислень

ВИСНОВОК

Для забезпечення високого рівня безпеки всіх виробничих процесів-важлива задача для функціонування будь якої структури.

Проаналізувавши існуючі системи СКУД їх види та класифікацію, можна зробити висновок, що вибір СКУД сильно залежить від поставлених задач до системи.

Були розглянуті основні компоненти систем контролю доступу,основні задачі для забезпечення безпеки, способи та види ідентифікації осіб на пропускних пунктах.

Несанкціоновані проходи, порушення пропускного режиму і трудової дисципліни, нецільове використання робочого часу все це несе потенційну загрозу, здатну привести до істотних матеріальних проблем.

В результаті виконання атестаційної роботи проведено дослідження потрібних технологій. Проведено аналіз проблемної галузі, та виконана дослідницьку частина.

Для забезпечення контролю доступу в університет необхідно впровадження сучасної СКУД, до складу якої будуть входити різні засоби (зчитувачі карт, біометричні зчитувачі і ідентифікатори), контролери та виконавчі пристрої.

Кожному працівнику та студенту визначається рівень доступу, видаються персональні ідентифікатори, за допомогою яких вони можуть проходити на територію університету і в приміщення, де мають право перебувати. Були проаналізовані основні функції системи контролю та управління доступом.

Розглянуті складові системи. Покращення, недоліки та пропозиції щодо інтегрування подібної системи до інфраструктури кібер-університету.

Сформована модель і структура підсистеми.

Проектована система дозволяє провести аналіз необхідних комплектуючих системи, провести аналіз маніпулювання даними в системі, та запобігти несанкціонованому проникненню до університету.

Розглянута кіберсоціальна система Smart Cyber University (CyUni). На основі сервісу доступу до інфраструктури, яка має своє місце серед сервісів кібер-університету.

В цьому сервісі запропонована ідея доступу та моніторингу присутності студентів та співробітників в аудиторіях на основі використання мобільних пристроїв і ID-карт.

У роботі запропоновано використання туманних обчислень для формування повноцінної системи безпеки яка включає декілька пропускних пунктів, аудиторії з магнітними або електронними замками моніторинг умовних пунктів та аналіз обміну даними між ними.

При використанні туманних обчислень, дані обробляються швидше, відбувається економія ресурсів на інтегрування системи. Через мережеві з’єднання з низькою затримкою відбувається обмін даними, що суттєво покращує оптимізацію роботи системи та її швидкодію.

Розглянуто можливість покращення систем безпеки та ідентифікацію осіб які пересуваються інфраструктурою ВНЗ.

ПЕРЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Не типові функції СКУД [Електронний ресурс]. Режим доступу: http: //www.secuteck.ru/articles2/sys_ogr_dost/netipichnye-funktsii-skud/ – Назва з екрану.

2. Огляд можливостей СКУД [Електронний ресурс]. Режим доступу: http://www.sistema-dostupa.ru/i03.htm/ – Назва. з екрану.

3. Рижова В.А. Проектування і дослідження комплексних систем безпеки[Текст] /С.– Пітерб. : НІУІТМО, 2012. – 157с.

4. Система контролю доступу на підприємстві. Особливості впровадження [Електронний ресурс]. - Режим доступу: http://www.cleper.ru/articles/description.php?n=441 – Назва з екрану.

5. Система контролю і управління доступом. Принцип дії [Електронний ресурс]. Режим доступу: http://www.intersyst.ru/solutions/165/460/ – Назва з екрану.

6. Сорокін К. Застосування біометричних технологій в забезпеченні інформаційної безпеки бізнесу [Текст] / СКУД. Антитероризм-2013, 2013 – С : 46-47с.

7. Функції універсальних СКУД: що потрібно споживачу [Текст] /Тіхонов О.О., Малишева А.С., Шаповалов А.В., Гамбург А.Е., Стасенко Л.А, Курілін А.С. / Системи безпеки 2011 No 4. – С. : 108-119.

8. Хаханов В.І., Чумаченко С.В., Літвінова Е.І., Міщенко А.С. / В.І. Хаханов, С.В.Чумаченко, Е. І. Літвінова, А. С. Міщенко / Радиоэлектроника и информатика. - 2015. - № 3. - С. 39-44. - [Електронний ресурс] Режим доступу: http://nbuv.gov.ua/UJRN/reii_2015_3_9. - Назва з екрану.

9.Кашкаров А. П. Системи безпеки та пристрої кодового доступу: просто про складне[Текст] / А.П.Кашкаров. – М : ДМК-Пресс, 2014. – 58-60с.

10.Дшхунян В.Л. Електронна ідентифікація. Безконтактні електронні ідентифікатори та старт-карти[Текст] : учб.посібн. / Шаньгін В.Ф. – М.: АСТ,2004 – 659с.

11. Классификация СКУД [Електронний ресурс] – Режим доступу: http://www.fortnet.ru – Загл. с экрана.

12. «Интернет вещей»: Беспроводные сенсорные сети. Белая книга, – Wireless Sensor Networks, – 2014г, [Електронний ресурс] – Режим доступу: http://www.iec.ch/whitepaper/pdf/IEC_WP_Internet_of_Things_Wireless_Sensor_Networks_Ru_LR.pdf – Загл. с экрана.

13. Ворона В.А. Системы контроля и управления доступом / ВоронаВ. А., Тихонов В. А. – М.: 2010. -272 с.

14. Идентификация и аутентификация, управление доступом [Identification and authentication, access control]. [Електронний ресурс] – Режим доступу: http://citforum.ru/security/articles/galatenko/ – Загл. с экрана.

15. Сайт компании «SMART Technologies» [Електронний ресурс] Режим доступу: https://home.smarttech.com/– Загл. с экрана.

16. ГОСТ 12.4.009-83 "Система стандартов безопасности труда. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание" Приложение 1 [Текст] – Введ. 01-12-2014. – М : Изд-во стандартов, 12-09-2018 – 27с.

17. Иванов И.В.Охрана периметров-2 [Текст] — М.: Паритет Граф, 2000, 50-56с.

18. Шкуропат И. И. Системы видеорегистрации для локомотивов [Текст] / Локомотив: журнал - С .: 2018, 2-3с.

19. Герман Кругль. Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового видеонаблюдения [Текст].–М: «Секьюрити Фокус», 2010. – 640 с. –ISBN 978-5-9901176-2-4.

20. Концептуальные основы безопасности Российской Федерации [Текст] / Шушков Г. М., Сергеев И. В. // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных

трудов III Всероссийской заочной научно-практической конференции (23.11.2015 - 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой; редколл .: Е.А. Куренкова. – М. : ИИУ МГОУ, 2016. - ISBN 978-5-7017-2532-2.

21. B.R. Mehta.Programmable automation controller [Текст]/ Industrial Process Automation Systems. — Elsevier, 2015. — С. 301–306. — ISBN 978-0-12-800939-0.

22. Uchit Vyas. OpenStack Deployment [Текст]/ Applied OpenStack Design Patterns. - Berkeley, CA: Apress, 2016. - S. 31-50. - ISBN 978-1-4842-2453-3

23. L. M. Varalakshmi A selective encryption and energy efficient clustering scheme for video streaming in wireless sensor networks [Текст] // G. Florence Sudha, G. Jaikishan / Telecommunication Systems. - 2013-08-31. - Т. 56, no. 3. - S. 357–365.

24. Gillam, Lee. Cloud Computing: Principles, Systems and Applications [Тест] / Nick Antonopoulos, Lee Gillam. - L .: Springer, 2010 .-- 379 p.