МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет)_ Автоматизації і комп'ютерних систем
Кафедра Інформаційних систем_____

«До захисту в ЕК»		**«До захисту допущено»**	
Директор інституту(декан факультету)		Завідувач кафедри	
_____ (підпис)	___Андрій Форсюк__ (ім'я та прізвище)	_____ (підпис)	__Сергій Чумаченко (ім'я та прізвище)
«___» _____ 2022р.		«___» _____ 2022р.	

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

зі спеціальності__122 «Комп'ютерні науки»_____
(код та назва спеціальності)
освітньо-професійної програми:__Інформаційні управляючі системи та технології
_____
на тему Дослідження та розроблення підсистеми моніторингу працівників ПРАТ Оболонь'

Виконав: здобувач_2__ курсу, групи__ІС-2-4М___

___Олійник Олександр Олександрович_____
(прізвище, ім'я, по батькові повністю) (підпис)

Керівник М'якшило Олена Михайлівна _____
(прізвище , ім'я та по батькові повністю) (підпис)

Консультанти_____ _____
(ім'я та прізвище) (підпис)

_____ _____
(ім'я та прізвище) (підпис)

_____ _____
(ім'я та прізвище) (підпис)

Рецензент __Олег Клименко__ _____
(ім'я та прізвище) (підпис)

Я як здобувач(ка) Національного університету харчових технологій розумію і підтримую політику університету з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволеної допомоги під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач_____
(підпис)

Київ - 2022р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет) Автоматизації і комп'ютерних систем
Кафедра Інформаційних систем
Освітній ступінь Магістр
Спеціальність 122 «Комп'ютерні науки»
(код і назва)
Освітньо-професійна програма Інформаційні управляючі системи та технології
(назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри Чумаченко С.М.

"____" _____2022року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА

Олійника Олесандра Олександровича
(прізвище, ім'я, по батькові)

1. Тема Дослідження та розроблення підсистеми моніторингу працівників ПРАТ Оболонь'

керівник роботи доцент, кандидат технічних наук М'якшило Олена Михайлівна,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від "11"листопада 2021року №**884-кс**
2. Строк подання здобувачем роботи 28.01.2022
3. Вихідні дані до роботи Дані працівників, програмне забезпечення, апаратне забезпечення, база даних.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Дослідити проблеми моніторингу працівників на ПРАТ «Оболонь». Дослідити загрози щодо інформаційної безпеки підприємства. Дослідити, обрати та запропонувати методи і рішення щодо покращення моніторингу працівників ПРАТ «Оболонь». Розробити структуру та модель удосконаленої електронної перепустки працівника.

5. Перелік графічного матеріалу
В роботі представлено 31 ілюстрації. 21 скріншоти програмного забезпечення, 5 ілюстрації апаратного забезпечення та 5 додатків

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 11.11.2021

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів виконання кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Ознайомлення з об’єктом автоматизації	4	днів
	Аналіз об’єкту автоматизації	3	днів
	Аналіз програмного забезпечення	5	днів
	Постановка задачі	2	днів
	Обґрунтування доцільності проектування й розроблення системи	6	днів
	Розробка інтерфейсу	3	днів
	Розробка елементів керування	1	днів
	Реалізація функцій системи	10	днів

Здобувач _____ Олійник О.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ М’якшило О.М
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MS- Microsoft Server

ПЗ- Програмне забезпечення

ІТ- Інформаційні технології

ПрАТ- Приватне акціонерне товариство

ІС- Інформаційна система

SQL – Мова структурних запитів

C# - Об’єктно орієнтована мова програмування

ВСТУП

Актуальність теми. Ефективний процес моніторингу працівників дозволяє значно підвищити інформаційну безпеку та удосконалити процес отримання рівнів доступ до підприємства та систем керування. Адже питання інформаційної безпеки гостро стоїть в усіх сферах діяльності особливо там де є конфіденційна інформація.

Аналіз інформації є невід'ємною частиною процесу моніторингу працівників. Відню дає змогу забезпечення захист даних та швидко провести ідентифікацію персоналу та виявити збіги або розбіжності під час розшифрування інформації і порівняння ключів доступу. Актуальність проблеми доведена практичним дослідженням, де були опрацьовані дані підприємства та проведено аналіз витоку персональних або конфіденційних даних. Найчастіше дані аналізи проводять у сфері безпеки та інформаційної безпеки об'єкту або підприємства.

Моніторинг працівників дозволяє не лише підвищити рівень безпеки даних та захисту працівників, а й дозволяє показати шляхи більш оптимального використання ресурсів підприємства

Моніторинг працівників це – процес, який складається з двох елементів. Перший елемент, як можна здогадатись, сам процес моніторингу працівників. Він дозволяє значно підняти захист даних на підприємстві. Другий елемент моніторингу працівників - це слідкування за діями працівників, в плані захисту інформації від витоку або пошкодження. Система буде відслідковувати ресурси, якими користується працівник і не дозволить інсталювати шкідливе програмне забезпечення, допоможе в підтримці та захисту персональних даних і багато чого іншого.

Ефективне використання систем моніторингу працівників дозволяє підвищити безпеку та збільшити ефективність роботи підприємства за рахунок зменшення витоку інформації на підприємстві.

Зв'язок роботи з науковими програмами, планами, темами. Дана наукова кваліфікаційна робота написана та виконана з дотримання всіх вимог згідно з планом та програмою наукових досліджень на кафедрі інформаційних систем Національного університету харчових технологій за тематикою **«**Дослідження та впровадження інформаційних технологій у галузях харчової промисловості та освіті, № держреєстрації 0117U003475.».

Об'єкт дослідження – процес моніторингу працівників на ПРАТ «Оболонь» .

Предмет дослідження – методи та засоби моніторингу працівників в рамках системи управління підприємством.

Мета та задачі дослідження. Головною цілю роботи є підвищення ефективності моніторингу працівників ПРАТ «Оболонь» для забезпечення захисту особистих даних та інформації підприємства. Для досягнення мети мають бути виконані наступні завдання:

– Дослідити проблеми моніторингу працівників на ПРАТ «Оболонь»;
– Дослідити загрози щодо інформаційної безпеки підприємства;
– Знайти, дослідити та провести аналіз існуючих систем моніторингу працівників;
– Дослідити, обрати та запропонувати методи і рішення щодо покращення моніторингу працівників ПРАТ «Оболонь»;
– Розробити структуру та модель удосконаленої електронної перепустки працівника;
– На основі отриманих результатів створити програмне забезпечення підсистеми моніторингу працівників ПРАТ «Оболонь».

Методи дослідження. В роботі використано метод системного аналізу на основі структурного моделювання бізнес- процесів; метод класифікації загроз щодо

інформації підприємства; проведення аналізу систем моніторингу працівників методом порівняння за визначеними критеріями.

Наукова новизна отриманих результатів полягає в наступному:

- Вперше запропоновано модель та структуру електронної перепустки для ПРАТ «Оболонь» на основі двох чипів;
- Запропоновано алгоритм обробки інформації, що надходить від електронної перепустки при її ініціалізації.

Практичне значення отриманих результатів. Підприємство отримає покращення в сфері моніторингу працівників та створить системи електронних замків що приведе до зростання рівня інформаційної безпеки та захисту інформації працівників, а також дозволить покращити контроль за працівниками.

Апробація роботи

Дана робота була представлена на двох наукових конференція «VIII Міжнародній науково-технічній Internet-конференції» листопад 2021р., м.Київ. Та “IV Міжнародній науково-практичній конференції” лютий 2021р., м.Київ.

Структура та обсяг магістерської роботи. Магістерська робота складається з 5 розділів та вступу, списку використаної літератури та додатків всього 89 сторінки. Робота включає 31 ілюстрацій.

РОЗДІЛ 1 . ДОСЛІДЖЕННЯ ПРОБЛЕМ ПРОВЕДЕННЯ МОНІТОРИНГУ ПРАЦІВНИКІВ НА ПІДПРИЄМСТВІ

1.1 Загальна характеристика підприємства

Головним видом діяльності підприємства є створення та збут алкогольних, слабоалкогольних та безалкогольних напоїв.

Продукція підприємства завоювала лідерство на ринку України і сильні позиції на ринку Європи, а також представлення у більшості країнах світу..

На теперішній час ПрАТ Оболонь продовжує нарощувати потужність та збільшувати присутність на ринках країн світу. Із створення Оболонь створив та впровадив в продаж значну кількість видів напої.

Розпочавши свій шлях із алкогольних напоїв компанія експериментувала , що призвело до появи слабоалкогольних та безалкогольних напоїв. Такий підхід дозволив збільшити присутність на ринку і підняти прибуток..

Компанія використовує лише артезіанські свердловини для видобутку води, а також лише якісні інгредієнти з яких виготовляє напої. Такий підхід дозволяє бути впевненим в якості виготовленої продукції

ПАТ "Оболонь" Має всі необхідні ліцензії та дозволи для роботи як на території України так і за її межами.

Лише у 2009 році приватне акціонерне товариство «Оболонь» реалізувало 96,1 млн літрів алкогольних напої, 14,8 млн літрів безалкогольних напоїв та 2,4 млн літрів слабоалкогольних напоїв та ще 8,3 млн літрів мінеральної води. Величезні обсяги виробництва та продажу дають можливість приватному акціонерному товариству «Оболоні» стати одним із лідерів на різних ринках, де підприємство реалізує власну продукцію.

В ПрАТ Оболонь працює величезна кількість людей і саме в таких випадках виникає гостра потреба проводити моніторинг працівників. Так, як кожний працівник має доступ до певних елементів контролю чи окремих елементів інформації розповсюдження який може підірвати довіру до

підприємства через втрату даних які пре назначені лише для внутрішнього користування. Також звернувши(взявши) до уваги найбільш сильні позиції на ринку.

1.1.1 Організаційна структура підприємства

Структура згідно якої працює та відбуваються бізнес процеси показує модель підприємства і призначена для детального вивчення та проведення теоретичних робіт. Схему верхнього рівня структури приватного акціонерного товариства Оболонь можна переглянути та ознайомитись рис.1

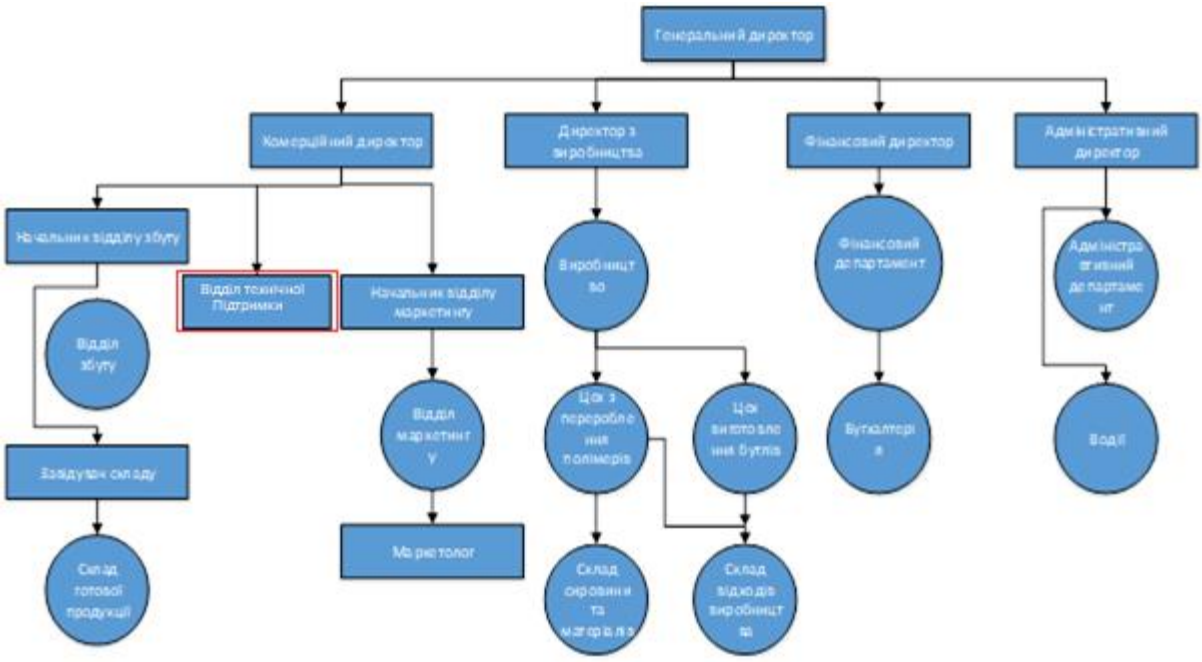


Рис. 1.1. Верхній рівень організаційної структури підприємства

У відділі технічної підтримки є 11 працівників. Начальник відділу, 3 програміста, 2 системних адміністратори, 1 net розробник, 1 Hardware інженер, 3 працівники підтримки користувачів.

Схема роботи досить проста. Для відділу відкривається тікет(завдання) на виконання завдання. Система реєструє звернення працівників або керівництва та генерує спеціальну форму. Всі згенеровані форми поміщаються в систему і працівник самостійно може обрати завдання. Якщо завдання потрібно негайно

виконати, керівник відділу в екстреному порядку назначає відповідного за виконання або декілька осіб якщо завдання досить складне. Такий підхід створює гнучку та лояльну до працівників схему роботи відділу.

Безпека в сучасному світі відіграє найбільш ключову ролів в розвитку будь якого напрямку діяльності. Підприємства не є виключенням. Моніторинг персоналу може здаватись не дуже важливим елементом, але поступово будь який бізнес чи підприємство розширяється і залучає більшу кількість працівників. Збільшення кількості людей які мають доступ до елементів контролю, інформацію, або можуть прямо вплинути на роботу підприємства значною мірою підриває безпеку та довіру до підприємства.

1.1.2 Загальні положення

-Відділ підтримки здійснює підтримку та розробку програмного забезпечення для підприємства.

-Працівники відділу займається підтримку та налаштування Інформаційної система яку використовує підприємство.

-Відділ технічної підтримки очолюється керівником який був призначений на посаду генеральним директором або радою директорів.

-Кількість працівників, їх обов’язки та графік роботи визначається регламентом підприємства.

-У випадку екстрених випадків чи понаднормової роботи в звичному режимі робочий час працівників оцінюється погодинно з розрахунку вартості години роботи працівників згідно його заробітної плати.

Працівник отримує право на користування службовим транспортом у вигляді таксі за рахунок компанії або відшкодування коштів витрачених на паливо як що працівник використав власний автомобіль для виконання службових завдань.

1.1.3 Завдання відділу технічної підтримки

1 Керівник відділу слідку за зайнятістю персоналу(слідкує щоб не було вільних працівників та заявок одночасно)

2 Програмісти займаються написанням та підтримкою програмних продуктів(модулів) які працюють на підприємстві самостійно або в парі з основною інформаційною системою.

3 Системні адміністратор займаються підтримкою персональних комп'ютерів працівників та різного роду периферійного обладнання.

4 Нет розробник займається розробкою та підтримкою сайту компанії та різного роду мережевих додатків.

5 Hardware інженер працює з різного роду пристроями особливо працюючи із деталями проводячи їх обслуговування та заміну у разі необхідності.

6 Працівники підтримки користувачів здіснюють реєстрацію скарх та намагаються вирішити проблеми по мірі можливості не скидаючи завдання на інших працівників.

1.1.4 Функції

Моніторинг звернень персоналу та подальша реакція на повідомлення від працівників які звернулись по допомогу.

Створення програмного забезпечення за вимогою керівництва .

Проведення профілактичних робіт з обладнанням.

Створення та підтримка діяльності веб сервісів підприємства.

Проведення різних навчальних заходів для персоналу.

Підтримка працездатності основної інформаційної системи та всіх модулів і програм які працюють поряд.

Написання звітної документації.

Написання документації для користувачів.

Розроблення та впровадження нових програмних продуктів.

1.1.5. Взаємовідносини з іншими підрозділами

Взаємодія з бухгалтерією:

- Звіти про додаткові години(перепарювання);
- Платіжні рахунки працівників(для отримання заробітної плати);
- Особисті дані працівників;
- Номер трудової домовленості та додатки;
- Різна нормативна документація.

Відділом безпеки:

- Рівні доступу до інформації та електронних замків на підприємстві;
- Особисті дані працівників;
- Угода про заборону розголошення конфіденційної інформації;
- Угода про заборону публікації будь якого матеріалу що стосується підприємства без попередньої згоди ;
- Спеціальні ключ-перепустки;
- Звітна інформація про використання комп'ютерної техніки.

З відділом стратегії та розвитку:

- Плани на майбутній розвиток програмного забезпечення;
- Плани на майбутній розвиток; комп'ютерно периферійного парку підприємства
- Плани на розвиток веб ресурсів;
- Кошторису витрат на рекламу;
- Обґрунтування вибору комплектуючих.

Відділ кадрів:

- Вимоги до кандидатів.
- Додаткова інформація про працівників.

1.1.6 Функції працівників відділу технічної підтримки

Керівник відділу технічної підтримки

Функції:

- Керування працівниками;
- Розподілення завдання між працівниками;
- Визначення пріоритетності завдань;
- Організація навчальних семінарів;
- Робота для підтримки позитивної атмосфери в команді.

Програмісти

Функції:

- Прийом заявок на розробку, оновлення або підтримку програмного забезпечення;
- Підтримка програмного забезпечення;
- Оновлення застарілих додатків;
- Створення нових додатків;
- Інтеграція систем безпеки;
- Підтримка діяльності підсистем.

Системний адміністратор

Функції:

- Прийом завдань пов’язаних з налаштуванням комп’ютерної техніки;
- Проведення профілактичних робіт на програмному рівні;
- Здійснення установку, перестановку та оновлення програмного забезпечення;
- Здійснює встановлення антивірусного програмного забезпечення.

NET розробник

Функції:

- Займаються розробкою веб сайту;
- Розробляє веб інтерфейси;
- Забезпечує коректну роботу веб сервісів;
- Усуває помилки в веб додатках.

Hardware інженер

Функції:

- Здійснює прийом та встановлення комп'ютерного та серверного обладнання;
- Займається налагодженням роботи комп'ютерної та серверної техніки(на Hardware рівні) ;
- Складає акти про прийом та повернення техніки;

Працівники підтримки користувачів

Функції:

- Первина реакція на заявку;
- Проведення аналізу та оцінювання складності завдання;
- Погоджує з редакторами замічені стилістичні погрішності.
- Проводить обговорення проблеми.
- Моніторинг завдавань.

1.2. Загрози втрати інформації на підприємстві

Спроби викрадення інформації зародилися ще в давні часи. Спершу все були крадіжки документації чи інших цінних речей які могли нанести значну шкоду підприємству. Згодом коли з'явилися комп'ютерні системи крадіжки інформації та інформаційна безпека вийшла на новий рівень. Адже з'явилося дуже багато нових можливостей крадіжки та захисту інформації.

В світі існує досить багато трактувань що таке інформаційна безпека. Її елементи можна розглядати як:

- Систему відносин.
- Сукупність дій які мають бути виконані для захисту важливої інформації та проведення превентивних заходів для навчання персоналу.
- Ряд процесів в середні підприємства які націлені на підтримку безпеки та навчання спеціалізованого персоналу.
- Ряд процесів контролю за працівниками.
- Створення рівнів доступу до інформації.
- Процесів моніторингу працівників.

На теперішній час гостро стоїть проблема захисту підприємства(інформаційної безпеки так , яка вона повною мірою залежить від ступеню захисту підприємства. Різні рівні Інформаційної безпеки прямо впливають на створення та впровадження найновіших напрацювань в сфері ІТ.

Всі підприємства та бізнеси перебувають у постійному русі та розвиваються збільшуючи свою потужність та вплив. Із збільшення підприємства збільшується його вартість що в свою чергу призведе до збільшення вартості інформації яку можна викрасти. Для забезпечення безпеки створюють різні системи перепусток та різні рівні достоту а також системи моніторингу працівників. Глобальні процеси сприяють розвитку таких систем через бажання захистити важливу інформацію.

В сучасному світі будь яке підприємство рано чи пізно почне використовувати Інформаційні технології для успішного розвитку. З початком використання буде поставлено питання про захист даних та навчання персоналу який буде проводити захист.

Зловмисники можуть бути як зовнішні так і внутрішні:

Внутрішні зловмисники це люди які розпочали працювати в компанії та намагаються отримати дані.

Зовнішні зловмисники це люди які намагаються отримати доступ до комп'ютерних систем підприємства як із середини.

Внутрішні зловмисники діють наступним чином:

– Копіюють дані підприємства (документи, звіти, журнали тощо);

– Здійснюють спроби викрадення носіїв інформації;

– Викрадають персональні дані працівників;

– Роблять пошкодження комп'ютерної або іншої техніки;

– Викрадають плани на майбутнє підприємства;

– Викрадають дані акціонерів;

– Проводять негативні агітації серед персоналу;

– Створюють погану атмосферу на робочих місцях.

Зовнішні зловмисники діють наступним чином:

–Залишають носій інформації, на який записане вірусне програмне забезпечення, для зараження вірусами різної комп'ютерної техніки для отримання інформації.

– Намагаються зламами захист підприємства для отримання інформації за допомогою мережі інтернет.

Якщо не використовувати систему моніторингу співробітників, то виникає ризик отримати наступні внутрішні загрози як крадіжка інформації, спроба заразити вірусами комп'ютерну техніку підприємства, або видалити чи пошкодити службові документи підприємства.

Існує ймовірність спроби завдати шкоди підприємству власними співробітниками. Такі випадки можуть виникнути через наступні причини.

– Психологічні обставини працівника через складнощі на роботі;

– Занадто низький або незадовільний рівень фінансового забезпечення співробітників;

– Погані відносини в структурі керування та працівників з керівництвом ;

Нажаль, через невеликий рівень заробітної плати працівники можуть перейти на сторону конкурента.

Захист інформації є найбільш пріоритетним завданням особливо якщо звертати увагу на співробітників, які мають доступ до секретних та закритих даних. Небезпека втрати даних, в першу чергу, може сильно зашкодити репутації підприємства, що, в свою чергу, приведе до фінансових витрат, так як деякі партнери можуть перестати користуватись послугами. Моніторинг працівників буде використовуватись не лише для контролю переміщення працівників, а для контролю за рівнем доступу до інформації.

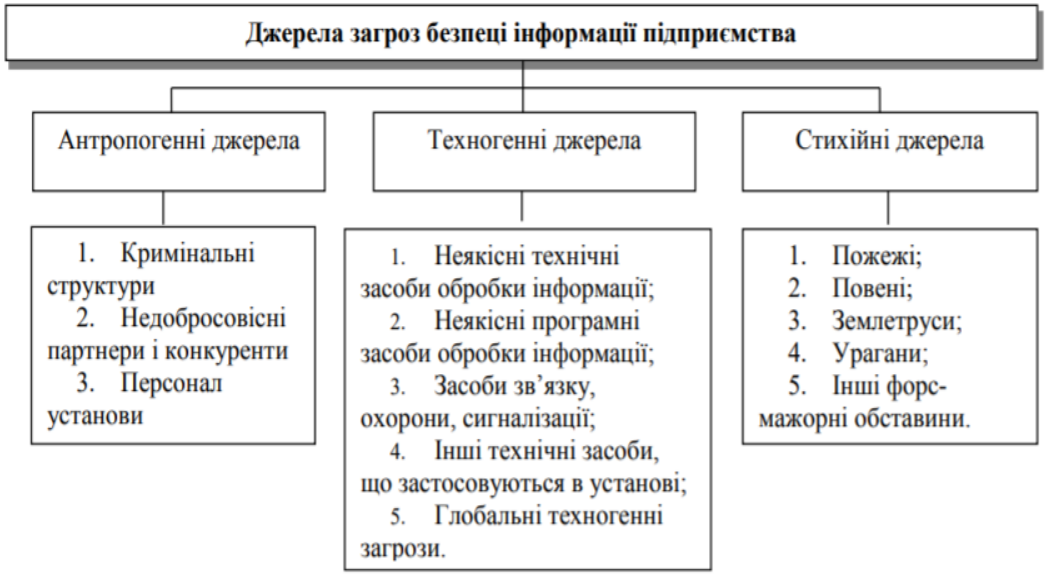


Рис 1.1 Джерела загроз інформаційній безпеці підприємства.

Як можна побачити з рисунку 1.1 людський фактор представляє серйозну небезпеку для інформаційної безпеки підприємства.

Інформаційна безпека співробітників являє собою захист персональних даних та внутрішню інформацію компанії.

Отже захист персональних даних працівників підприємства, в різних інформаційних системах, є не лише обов'язком компанії. Працівник повинен

самостійно підтримувати персональну безпеку та безпеку підприємства, де він працює, та виконує службові обов'язки. Оскільки будь яка компанія це в першу чергу люди встановлений антивірус не дає повної гарантії безпеки.

Більшість компаній проводить спеціальні тренінги де намагаються навчити персонал як правильно використовувати системи безпеки та генерувати паролі. Але, нажаль, більшість співробітників проходить інструктаж і вже через місяць- два робить типові помилки навіть не звертаючи увагу на застереження.

Такі дії співробітників можуть привести до злому комп'ютерної техніки працівників і вже через його персональний комп'ютер заразити всю систему

Найбільші помилки співробітників:

- Створення занадто легкого паролю без використання малих та великих літер, не використання цифр та символів, створення занадто короткого паролю;
- Використання справжніх слів або дати;
- Якщо підприємство надає можливість, то користуйтесь робочою технікою;
- Користувачі записують паролі в телефон або на листочок;
- Працівники використовують один і той самий пароль для всіх облікових записів.

Електрона пошта використовується скрізь і для різних цілей. Як правило, найчастіше використовують електрону пошту для листування та автентифікації людини в різних місцях (сайти, банки, пристрої, робоче програмне забезпечення). Більшість сервісів, так чи інакше, пов'язані з поштовою скринькою і втрата її може призвести до неприємних наслідків. Особливо як що у працівників зламують корпоративний поштовий ящик. Хакер таким чином може отримати доступ до внутрішнього листування компанії та обійти системи автентифікації та перевірки і заразити вірусами значну кількість користувачів, або розпочати надсилати спам співробітникам. Найбільш поширені помилки - це перехід за різними сумнівними

посиланнями , листування з клієнтам за допомогою персонального клієнта, встановлення програмного забезпечення, яке пропонуються в листі від невідомої компанії.

Типові помилки працівників:

- Працівники досить рідко перевіряють хто відправив листа;
- Працівники не перевіряють файли на віруси за допомогою антивірусів;
- Працівники відключають антивірусне програмне забезпечення, коли це просто зробити;
- Працівники не фільтрують пошту на довірені та загальні і з цікавості відкривають листи зі спаму;
- Натискають на різні кнопки всередині сумнівних листів.
- Використовують одну поштову скриньку для всіх завдань.

Деякі працівники при спробі зекономити звертаються до сумнівних джерел для скачування безкоштовного програмного забезпечення:

- Всі сайти де розповсюджують не ліцензійне програмне забезпечення є небезпечними та можуть призвести до зараження комп'ютерних систем.
- Будь які переходи за рекламними об'явами з сумнівним змістом скорше за все призведуть до зараження вірусним програним забезпеченням.
- Скачування та встановлення піратського програмного забезпечення.
- Встановлення сумнівних розширень в браузери особливо повязані з пошуком та паролями.

Також працівники досить часто люблять порушувати правила поведінки в всесвітній мережі інтернет:

- Генерують занадто прості паролі для службових облікових записів та ігнорують прості попередження про невідповідність пароля.
- Не використовують брандмауер.

- Використовують обліковий корпоративний запис з іншими людьми.
- Самостійно здійснюють налаштування спеціалізованого програмного забезпечення.
- Ігнорують або з якихось причин не встановлюють оновлення безпеки.
- Здійснюють установку піратського програмного забезпечення.
- Використовують невідомий USB девайс.
- Не використовують крипто шифрування системного диску на робочому ноутбуці або персональному комп'ютері.
- Не змінюють паролі після втрати пристрою.
- Ігнорують пропозиції створення резервної копії даних.
- Ігнорують хмарні сховища в корпоративному поштовому ящику.
- Ігнорують правило "3-2-1". А саме не роблять 3 резервних копії даних(1 в хмарному середовищі, 2 на пристрої, 3 на фізичному носієві із шифруванням) .

Мобільні телефони можуть стати причиною злому так як вони не поступаються персональним комп'ютерам і більшість програм мають версію під телефон. Але навіть тут є ризики. Типові помилки працівників які можуть призвести до викрадення даних :

- Ігнорування систем захисту (відбиток та пароль).
- Використовують занадто простий пароль.
- Дають телефон із таємною інформацією невідомим людям.
- Ставлять великий тайм аут для блокування дисплея.
- При використані графічного ключа генерують ключ на 2-3 рухи.
- Здійснюють установку піратського програмного забезпечення.
- Здійснюють установку програм з сумнівних джерел.
- Надають повний доступ сумнівним додаткам.

В теперішній час розвиток IT технологій дуже стрімкий, І Інформаційна безпека постійно розширюється і стрімко розвивається. Більшість експертів говорять про розширення Інформаційної безпеки та заміни визначення на Кібербезпеку. Це повязано із збільшенням ризиків викрадення даних.

Кібербезпека — є ледь не єдиним захистом від вірусів, втручань в роботу систем, викрадення та підробки даних, а також кібер атак.. Оскільки віруси, після потрапляння на один єдиний комп'ютер в мережі, здатний заразити всі системи та знищити, пошкодити або вкрасти дані. У кібербезпеці захист розділили на три елементи: комп'ютерні системи, різні процеси в мережі, найбільш небезпечні люди. Більшість заражень відбувається саме через людський чинник. Кібербезпека через стрімкий розвиток технологій стала невід'ємною частиною систем безпеки будь яких підприємств. Навіть на найнижчому рівні - встановлення антивірусного програмного забезпечення.

Враховуючи вище написаний матеріал можна з впевненістю сказати, що одна із великий проблем інформаційної безпеки є працівники (люди), які представляють внутрішню загрозу.

Саме така загроза є однією із найнебезпечніших. Адже без систем контролю керівництво може навіть не зрозуміти ким та коли саме була здійснена крадіжка даних. Це є серйозною проблемою, адже втрата та публічне розголошення деяких даних може спричинити резонанс та підірвати довіру до компанії і нанести фінансову шкоду. Підрив довіри може призвести до банкрутства оскільки з таким підприємством не захочуть мати справу інвестори та партнери.

Але в ручному режимі контролювати працівників на всі 100% просто неможливо або фінансово не вигідно. А повний контроль може погано вплинути на працездатність усіх працівників. Саме тому потрібно знайти баланс між контролем персоналу та ефективністю роботи.

1.3 Стан автоматизації на підприємстві

Приватне акціонерне товариство Оболонь вже багато років присутнє на ринку України та світу. І як всі сучасні компанії намагається створити та запровадити системи інформаційної безпеки та захисту даних. Система моніторингу працівників є одним із таких проектів який знаходиться в планах на розробку

Система моніторингу працівників повинна мати наступні автоматизовані елементи :

- Системи ідентифікації користувача;
- Систему роботи перепусток та електронних ключів;
- Захист від спроби доступу до контролю над системою із зовнішнього джерела;
- Керування інформацією всередині бази даних;
- Спеціальна розсилка на різні рівні;
- Контроль за доступом;
- Захист від “дурня”;
- Резервну систему яка зможе отримати контроль к випадку проблем із основним модулем.

Для коректної роботи моніторингу працівників система повинна мати доступ до інформації про працівників всіх відділів.

Будь яка інформацію повинна шифруватись та проходити перевірку за допомогою цифрових підписів.

В екстрених ситуаціях програмне забезпечення робить розсилку до всіх працівників служби підтримки.

1.4 Створення функціональної моделі бізнес процесів підприємства”as-is”

Для створення моделі діяльності відділу ведення звітності було використано програмне забезпечення AllFusion Process Modeler 7 (BPwin)[5]. Модель створена за допомогою AFPM показує діяльність відділу технічної підтримки з точки зору. Для показу та представлення всіх функцій з достатнім рівне деталізації кожного

процесу та показу всіх взаємодій. В загальному моделі створено та представлено лише три рівні декомпозиції. Головною діаграмою є авторизація працівника.

Вхідними стрілками до діаграми є:

- ID перепустки;

Стрілками контролю є:

- Спеціальні нормативні документи
- Договір про використання персональних даних
- Договір про нерозголошення

Стрілками механізмів є:

- Програмне забезпечення;
- Інформаційна система
- Модуль моніторингу працівників;

Вихідними стрілками є:

- Рішення система автентифікації;

Основна діаграма проходить декомпозицію та розбивається на нижчій рівні Перший рівень декомпозиції описує більш точно процес аутентифікації (дивись рис. Б2 у додатку):

- Внесення даних в систему;
- Аналіз;
- Зрівняння цифрових підписів перепустки та ключа в базі даних;
- Проведення перевірки працівника;
- Аналіз отриманих даних
- Висновок.

«Внесення даних в систему» – Процес цифрової передачі даних про працівника та ключів доступі через спеціальне програмне та технічне забезпечення.

«Аналіз» - Модуль моніторингу працівників проводить аналіз та дешифрування даних для перетворення в тип який зможе зрозуміти програмне забезпечення.

«Зрівняння цифрових підписів перепустки та ключа в базі даних» - Після отримання дешифрованих даних модуль зрівнює хеш суми інформації отриману з перепустки із даними які знаходяться в базі даних. А також зрівнює спеціальні ідентифікатори та ключі доступу.

«Аналіз отриманих даних» - Інформація проходить порівняння та записується в БД де додатково порівнюється.

«Висновок» - Результат на основі якого відбувається позитивна або негативна автентифікація працівника.

«ID перепустки» - Спеціальна карта ключ на які зберігається інформація необхідна для автентифікації та отримання доступу до підприємства та інших елементів.

«Спеціальні нормативні документи» -Документація яка підтверджує статус працівника та певні правилами які генеруються для відділів персонально.

«Договір про використання персональних даних» - Документ який підписуються працівники перед прийомом на роботу. Він надає компанії дозвіл на використання наступних даних:

-Паспортні дані

-Ідентифікаційний код

-Платіжні дані.

«договір про нерозголошення інформації» - це документ після підписання якого будь яке розголошення конфіденційної інформації працівник може отримати штраф від компанії або навіть понести адміністративне покарання .

«Програмне забезпечення» - Набір програм та модулів які прцють для виконання поставленого завдання.

«Інформаційна система» - Програмне забезпечення яке використовує підприємство на основі отримання ліцензійної копії.

«Модуль моніторингу працівників» - сервісний додаток який виконує функції контролю доступу.

1.4.1 Виявлені проблеми під час функціонального моделювання

Провівши аналіз та створивши функціональну модель відділу були виявлені такі зауваження:

- Процедура контролю працює не ефективно так як працівник в ручному режимі перевіряє перепустки та вирішує чи надавати доступ чи ні. .
- Проведення ручного внесення даних витрачає значну кількість часу та може призвести до помилки у введених даних або видача доступу людині яка не відпоститься до підприємства та має погані наміри.
- Неможливість працювати в реальному часу та проводити автентифікацію в декілька етапів одночасно;
- Відсутність можливості отримати детальну інформацію про працівника в момент аутентифікації;
- Відсутність захисту для окремих кімнат підприємства.

1.5 Моніторинг працівників

В сучасному світі інформаційна безпека відіграє одну із найбільш важливих ролей. А контроль за працівниками займає одну з лідируючих позицій в цій сфері.

Адже Моніторинг працівників дозволяє значно збільшити рівень безпеки на підприємстві формування товарних запасів підприємства. Згідно закритою інформації майже 50% витоків або розповсюдження конфіденційної інформації стається через поганий нагляд та моніторинг працівників. В якихось випадках стороні люди потрапляють на території та отримують доступ до закритих даних.

Для уникнення таких ситуацій більшість підприємств намагаються покращити контроль за працівниками та шукають способи ефективного моніторингу.

Підсистема моніторингу працівників дозволить вже на перших рівнях відсіяти потенційно небажаних гостей. Адже дана система не лише проводить розшифрування та порівняння даних і ключів. Вона також на основі спеціальних електронних ключів підтягує інформацію про працівника. Що дозволяє більш детально ознайомити та у випадку проблем знати хто саме винен в різних ситуаціях.

В теорії керування працівниками може здійснювати спеціально навчений персонал без використання програмного забезпечення та додаткових інвестицій в програмне та комп'ютерне забезпечення.

Але для підприємства де працює велика кількість людей такий підхід є невиправданим та малоефективним.

Можна проаналізувати діяльність підприємства та визначити проблеми моніторингу працівників які присутні на підприємстві:

- Відсутній автоматизований журнал відвідувань;
- Відсутня ідентифікація працівників;
- Працівники служби безпеки не можуть швидко переглянути детальну інформацію про підприємство;
- Відсутні гостьові перепустки;
- Відсутня немає перевірки електронних ключі та хеш суми;
- Всі дані зберігаються в єдиному екземплярі;
- Будь який працівник може отримати доступ;
- Інформація не може бути редагована;
- Складна процедура додавання та видалення;

1.5.1 Існуючі системи моніторингу працівників

1.5.1.1 YAWARE TIME TRACKER

YAWARE TIME TRACKER є інструментом моніторингу працівників та являє собою систему підрахунків робочого часу працівників з подальшою оцінкою ефективності роботи працівників компанії за персональним комп'ютером. Дане програмне забезпечення показує повну картину діяльності персоналу з можливістю створення завдань та подальшого звітування використовуючи внутрішні інструменти.

Однією з сильних сторін даного програмного забезпечення є автоматизований облік робочого часу працівників для створення спеціальних звітів. На основі яких, проводиться аналіз даних та визначається скільки насправді годин провів співробітник виконуючи свої службові обов'язки. Переглядати які програми запущені та чим займається співробітник в реальному часі.

Система дозволяє проводити контроль та заборонити використання певних програмних засобів чи веб ресурсів для підвищення продуктивності роботи.

Програмне забезпечення дозволяє:

- Вести автоматичний облік робочого часу(час початку та закінчення роботи, запізнення та незавершені завдання, відсутність співробітників на робочих місцях).
- Здійснювати моніторинг програм та веб ресурсів які використовуються, або були використані.
- Ведення електронного календаря (терміни робіт, зустрічі та інші важливі події).
- Можливість зробити скріншот робочого столу працівника.

- Система ефективних інструментів(пошта чи програми в яких працюють є ефективними, а Facebook чи YouTube ні)
- Повідомлення про систематичне використання неефективних інструментів на пошту або мобільний телефон за допомогою viber керівникові відділу.
- Можливість розділення проекту по різних відділах чи групах у межах одного відділу.
- Індивідуальні налаштування.
- Різний рівень привілеїв в середні системи.
- Вести особисту статистику.
- Здійснювати керування проектами.

Слабкими сторонами даного програмного забезпечення є:

- Занадто проста ідентифікація(система не вимагає ніяких підтверджень після введення коду)
- Немає контролю за персональними комп'ютерними пристроями.
- Немає контролю за використанням веб ресурсів(лише перегляд)
- Будь яке відлучення від персонального комп'ютера вважається порушенням(навіть як що, це було здійснено в службових цілях)
- Система розраховує вартість згідно кількості працівників.

1.5.1.2 BITRIX24

BITRIX24 Комплекс програмного забезпечення яке включає в себе елементи системи моніторингу працівники. Головною перевагою бітрікс24 є можливість повної інтеграції CRM в дане програмне забезпечення. Система дозволяє створити надійний рівень захисту шляхом обмеження доступу до інформації чи певних програм. Має досить гнучкі налаштування, які дозволяють провести баланс між ефективність, захистом та надійністю. Система резервує дані та створює дві копії для відновлення.

Програмне забезпечення має широкий функціонал з можливістю інтеграції більшість популярних програм починаючи від пошти закінчуючи складним програмним забезпеченням по типу 1С підприємство.

Бітрікс дозволяє швидко та безпечно впровадити потужні інструменти CMR на більшості підприємств та компаній. Аде інколи інтеграція проходить в декілька етапів, як що підприємство не може одночасно перервати роботу всіх сервісів. Через це програмне забезпечення підтримує модульний або поступовий перехід клієнтів в середовище. Це означає що, навіть система яка не можу бути зупинена буде може бути переміщена в середовище BITRIX24 методом часткового копіювання та створення дзеркал.

Головними перевагами BUTRIX24:

- Гнучкі інструменти керування.
- Можливість швидкого та безпечного перенесення ІС та інших елементів в середовище Bitrix24.
- Можливість використовувати інструменти контролю виконання проектів.
- Календар подій.
- Створення завдань та відслідковування виконання.
- Можливість створення завдання та на значення відповідального , або поставити завдання для відділу де воно буде оброблено та розподіллено між працівниками.
- Інтеграція різних програм для аналізу та прогнозування.
- Величезна кількість шаблонів.
- Можливість автоматизації бізнес процесів.

Слабкими сторонами даного програмного забезпечення є:

- Значна кількість інструментів які не будуть використані але враховані у вартості програмного забезпечення.
- Мало функціональний модуль моніторингу працівників.

- Після інтеграції підприємство змушене слідувати внутрішнім та регламенту планам бітрікса.
- Додавання стороннього програмного забезпечення неможливе.
- Конфіденційна інформація зберігається на серверах Бітрікс.

1.5.1.3 Проведення аналізу програмних засобів методом порівняльного аналізу.

Перед початком розробки власного програмного засобу було проведено аналіз порівняльним методом готових рішень. Проведено аналіз функцій які присутні в готових програмних продуктах та порівняно з функціями які будуть присутні у власному.

Порівняння систем аналогів

Табл. 1 Порівняння систем аналогів

	YAWARE TIME TRACKER	**BITRIX24**	**Модуль моніторингу працівників**
База даних з інформацією працівників	+	+	+
Зручний та зрозумілий інтерфейс	+	+	+
Швидка обробка інформації	+	+	+
Просте редагування даних працівника	-	+	+

Захист даних від помилок	+	-	+
Забезпечення веб захисту	-	-	+
Контроль інсталяції програмного забезпечення	-	-	+
Гнучкі інструменти контролю	-	+	-
Автоматизоване ведення журналу	-	-	+
Різні рівні доступу	+	-	+
Велика кількість різних інструментів	+	-	-
Забезпечення конфіденційності даних	-	-	+
Контроль за робочим простором працівників	+	-	-
Ціна програмного забезпечення	45440$ за 5680 людей(~1300230₴) на місяць	5000₴ на місяць+(~568000) по 100₴ за працівника щорічно	150000₴ за розробку та тестування модулю.

Після ознайомлення з готовими рішеннями та проведеного аналізу була створена спеціальна таблиця з порівнянням. Готові рішення представляють перспективне програмне забезпечення, як що підприємство планує повністю

перейти на використання даних інструментів, або має меншу кількість персоналу. YAWARE TIME TRACKER та BITRIX24 справді володіють привабливим функціоналом, але вартість занадто велика для підприємства з великою кількістю працівників.

Особливо враховуючи те, що підприємство не планує повну інтеграцію в ці програмні засоби. Таким чином розробка власного програмного забезпечення вартість якого значно менша ніж використання вже готових рішень дозволяє більш ефективно використовувати ресурси підприємства.

Крім того власне програмне забезпечення можна розвивати в будь яких напрямках що дозволяє значно розшири вплив та інтегрувати більше бізнес процесів.

1.6 Постанова завдання

Створення власного програмного продукту дозволить приватному акціонерному товариству Оболонь отримати програмне забезпечення, яке буде створене з врахуванням всіх нюансів роботи підприємства та різних внутрішніх бізнес процесів.

Такий підхід дозволить створити лише необхідні елементи тим самим зменшивши навантаження на систему, а можливість інтеграції в середовище основного програмного забезпечення дозволяє безпечно ввести експлуатацію новий програмний продукт без шкоди для старого.

Такий підхід дозволить зосередитись на основних завданнях та створити наступні рішення:

- Автоматизувати ведення журналу відвідувань;
- Автоматизувати ідентифікацію працівників;
- Здійснювати швидкий перегляд даних про працівників;
- Створення спеціальних гостьових перепусток із обмеженими правами доступу;
- Здійснювати попередження про різні хеш суми даних;

- Створення резервної копії даних;
- Доступ до програмного забезпеченню лише вузькому колу працівників;
- Можливість внесення коректив в інформацію;
- Можливість видалення або додавання без складних процедур;

Створюючи власне програмне забезпечення можна максимально зменшити кількість негативних елементів як в процесі створення прототипів так і в майже готовому програмному забезпечені. А повне володіння програмним забезпеченням дозволяє вільно розвивати та вносити корективи без узгодження з сторонніми сторонами.

Висновок 1

Для успішного виконання поставленого завдання проведено ознайомлення із загальною характеристикою підприємства. Ознайомлено з організаційною структурую, функціями та завданнями відділу технічної підтримки, загальними положеннями, загрозами втрати інформації. Проведено огляд стану автоматизації на підприємстві та аналіз програмних засобів для моніторингу працівників з подальшим порівнянням програмних забезпечень. Здійснено постановку завдання для подальшої роботи.

РОЗДІЛ 2. МОДЕЛІ ТА ІНСТРУМЕНТИ МОНІТОРИНГУ ПРАЦІВНИКІВ

2.1 Моделі моніторингу працівників

Серцем будь якого підприємства є працівники. Саме тому значна кількість компаній та підприємств вкладають значні кошти в різни системи контролю та моніторингу за працівниками для отримання найбільшого рівня інформаційної безпеки та захисту працівників, а також отримання максимальної продуктивності з мінімальними витратами.

Вирішення проблем моніторингу працівників вимагає прийняття важливих рішень. Є різні варіанти розвитку. Можливо використати вже готові рішення або створити власне. Варто відзначити відразу створення власного рішення є більш складним та ресурсо вимогливим, але власне програмне забезпечення має найбільший рівень захисту та збереження конфіденційної інформації.

Моніторинг працівників складається з двох модулів які мають різні завдання та обов’язки. Перший модуль повинен забезпечити захист та ідентифікацію працівників. Тобто забезпечити процес контролю за працівниками, гостями підприємства та незваними гостями. Створити різні рівні доступу до приміщень, створити спеціальні електронні замки для захисту окремих відділів чи кімнат від втручання.

Другий модуль забезпечує захист працівників на робочому місці. Головною логікою роботи є обмеження прав та доступу до певних веб- ресурсів. Такий підхід забороняє проводити глобальні зміни в персональних налаштування комп’ютера користувачів та захищає від потенційних загроз в глобальній мережі інтернет.

В теперішній час є наступні методи моніторингу:

Моніторинг та автентифікація працівників – Дана модель не потребує складних схем чи сильних витрат після впровадження. Завдання даної моделі

зчитати дані з перепуски та провести їхнє дешифрування, після чого зрівняти дані та електроні ключи із даними які знайдені в базі даних. Як що даних в базі немає або в процесі синхронізації та перевірки стався збій або хеш суми даних не ідентичні система повідомить охорону та відмовить в доступі. Головним недоліком цієї системи є механізм перепусток. Незвані гості можуть зчитати дані з карти та відтворити дублікат і таким чином проникнути на підприємство. Для боротьби з такими проблемами система використовує рівні доступу та спеціальні електроні ключі. Навіть як що скопіювати дані із збереження контрольних сум для дешифратора то скопіювати ключ не вдався так як він використовує трішки іншу технологію..

Модель створення електронних замків для певних відділів та важливих приміщень чи кімнат – Використовуючи дану модель підприємство створює додаткові елементи захисту у вигляді значної кількості замків. Така система дозволяє підвищити рівень безпеки адже навіть проникнувжи на підприємство “гостям” буде значно складніше потрапити в приміщення де зберігається інформація.

Модель керування комп’ютерною технікою працівників – Головна іде цієї моделі це відгородження рядових працівників від керування та налаштування системи. Системний адміністратор самостійно налаштує та встановить програмне забезпечення. Такий підхід не дозволяє навіть встановити якесь програмне забезпечення без участі спеціального працівника. Але як показує практика кількість систем які були заражені через використання піратського пз або програмного забезпечення з ненадійних джерел значно скоротилася .

Модель захисту від завідома шкідливих веб сайтів – Ні для кого не секрет що в глобальній мережі інтернет є безліч небезпечних веб сайтів. Дана модель збирає всі сайти в спеціальні бази даних та блокує спробу переходу за посиланням яке приведе на один із таких веб ресурсів.

Модель роботи лише на території підприємства – Така модель проводить моніторинг не лише працівників, а й місце знаходження і за допомогою спеціальних алгоритмів може визначити типову поведінку(місця з яких здійснювати вхід працівники його посадові обов'язки та доступу). Як що система побачить підозрілу поведінку то акаунт буде тимчасово заблокований.

Провівши аналіз діяльності модулю моніторингу працівників можна сказати наступне:

- Програмне забезпечення створене для збільшені захисту та покращення інформаційно безпеки підприємства
- Програмне забезпечення може здійснювати контроль та нагляд за працівниками.
- При використані працівники не можуть самостійно проводити маніпуляції із системою що в рази зменшує шанс зараження шкідливим програмним забезпеченням

Модуль має багато функцій та може забезпечувати як моніторинг працівників, захист інформації та контроль за працівниками, що перетворює його в універсальній інструмент контролю та моніторингу. Такий підхід дозволяє підприємству значною мірою провести оновлення та реструктуризацію в сфері безпеки та контролю. Дане програмне забезпечення може розвиватись в будь якому напрямку починаючи від зміни процесу моніторингу працівників до покращення систем контролю. А використання гнучких систем налаштування та адміністрування перетворює дане програмне забезпечення в перспективний інструмент який може бути інтегрований в основну інформаційну систему та перейняти частину функцій, або буде здійснювати додатковий захист працюючи поряд з основною інформаційною системо та проводячи резервне копіювання даних. Переглядати програми які запущені та

2.2 Огляд існуючих методології створення програмного забезпечення

Для початку створення програмного забезпечення потрібно визначити за допомогою якої методології буде створюватись підсистема моніторингу працівників. Всього є 9 основних методологій:

- Agile Modeling
- DSDM
- Extreme programming (XP)
- Feature driven development (FDD)
- OpenUP
- Scrum
- Lean software development
- Kanban software development
- Scrumban

Agile Modeling- це набір правил, принципів, які дозволяють швидко виконувати поставлені завдання за допомогою документів та створення моделів майбутнього програмного продукту.

DSDM Створений та базується на концепціях швидкого проектування та створення програм з постійною участю замовника та команди програмістів.

Extreme programming (XP) Даний підхід базується на перевірених методах розробки програмного забезпечення та завжди використовується парне програмування.

Feature driven development (FDD) Спеціальна методика для швидкої розробки. При такому підході невеликі проекти отримують термін лише дві неділі, а великі розбиваються на менші та також виконуються по дві неділі кожний.

OpenUP Метод розробки який в основі представляє розділення проекту на чотири частини:

- Початковий етап створення
- Специфікація

- Створення програмного забезпечення
- Передача готового продукту замовникові.

Такий підхід дозволяє команді розробників біль коректно використовувати ресурси та контролювати весь процес створення програмного продукту.

Scrum Підхід при якому розробники базують свою роботу на існуючих практиках кодування.

Lean software development Метод базується на елементах швидкої розробки та тестування програмного забезпечення. Такий підхід дозволяє команді проводити розробку та тестування програм одночасно.

Kanban software development Метод при якому навантаження розподіляється порівно, а головним принципом є виконання роботи в визначені терміни.

Scrumban є гібридом двох інших методик Scrum та Kanban software development. При такому підході кожний член команди можу сам обрати роль та частину роботи яку потрібно виконати.

Для виконання роботу був обраний Agile Modeling так як дана методологія базується на створені моделей та різного роду документацій, даний підхід дозволяє швидко виконати поставлені завдання.

2.3 Метод порівняльного аналізу

Метод порівняльного аналізу базується на порівнянні двох чи більше об’єктів(програмного забезпечення в рамках даної роботи) виявлені та пошуку сильних та слабких сторін, характеристик та різних властивостей програмного забезпечення. Після чого проводиться детальний аналіз та порівняння які базуються основі раніше зібраних даних. Даний метод використовується різних закономірностей та можливостей роботи програм які можуть надати переваги, або створити різного роду вразливості. Метод використовується науковими працівника та вченими і може бути використаний в різних сферах діяльності.

2.4 Постановка завдання створення програмного забезпечення

Стрімка еволюція технологій визначає майбутній розвиток системи безпеки. Сьогодні одним із пріоритетів розвитку будь-якої розвиненої країни та її стратегії є покращення якості систем безпеки і, в першу чергу, ефективне використання їх для забезпечення доступу до інформації лише тим особам, які мають на це право. Використання системи ідентифікації персоналу дозволить підвищити рівень безпеки та надійності зберігання інформації.

Програмне забезпечення буде розроблятись за допомогою MS Visual studio 2019 C# та MS QSL server. Для зручності користування буде розроблено інтерфейс користувача та різні під пункти де можна буде проводити роботу з даними, або переглядати інформацію

Система моніторингу працівників має автоматизувати контроль доступу персоналу та відвідувачів і відсіяти неавторизованих гостей, які намагаються отримати доступ до інформації, або потрапити на територію компанії. Додаток повинен визначати хто намагається отримати доступ, або потрапити на територію підприємства, шляхом отримання і аналізу даних. Також система повина моніторити час перебування на підприємстві що може спростити роботу бухгалтерії, так як будуть точні дані годин роботи.

Крім того за допомогою спеціальної підсистеми слід передбачити керування електронними замками, в середні підприємства, для здійснення більш точного контролю переміщення працівників, захист деяких кімнат від доступу, а визначенням працівників, які намагаються потрапити на заборонену територію. Крім того, програма має моніторити спроби авторизації та доступ до інформації.

Програмне забезпечення буде працювати наступним чином:

- При вході на підприємство працівник буде проходити авторизацію за допомогою спеціального ключа-перепустки.

- Система запише дані та активує доступи до внутрішніх систем

- Кожна важлива кімната, приміщення та для пересування між різними частинами підприємства та для входу у відділи потрібно буде пройти повторну ідентифікацію.

- Якщо система відмовить декілька раз підряд, то буде створене спеціальне повідомлення з інформацією про працівника та місце куди він намагався потрапити.

- Програмне забезпечення зможе допомагати в контролі доступу до мережі інтернет для певних девайсів.

- Після виходу з підприємства система має зафіксувати час

- Система автоматично зберігатиме час додаткової роботи.

Аналіз даних – Процес отримання даних з перепуски та дешиврування даних з генерацією електронних ключів.

Замість повного відстеження роботи працівників, контролюється робота мережі — маршрутизаторів, серверів, брандмауерів — з метою усунення доступу до небезпечних веб ресурсів.

Враховуючи вище сказане виникають завдання:

- Проводити ідентифікацію працівників;
- Проводити дешифрування даних
- Забезпечувати захист користувачів
- Забезпечувати активний захист від вірусних загроз.
- Забезпечити редагування даних.
- Забезпечити прості механізми додавання або видалення даних.
- Забезпечити захист від веб загроз шляхом блокування різних сайтів.
- Створення механізмів контролю за працівниками.
- Копіювати та зберігати історію браузера з робочого персонального комп’ютера

- Перевіряти результат виконаних завдань
- Здійснювати моніторинг мережі(здійснювати моніторинг трафіку який був прийняти або відправлений).
- Фіксувати час перебування працівників на підприємств.
- Створити автоматизований журнал
- Створити інструмент для збереження резервної копії даних.
- Створити різні рівні доступу.
- Забезпечити можливість швидкого перегляду даних.

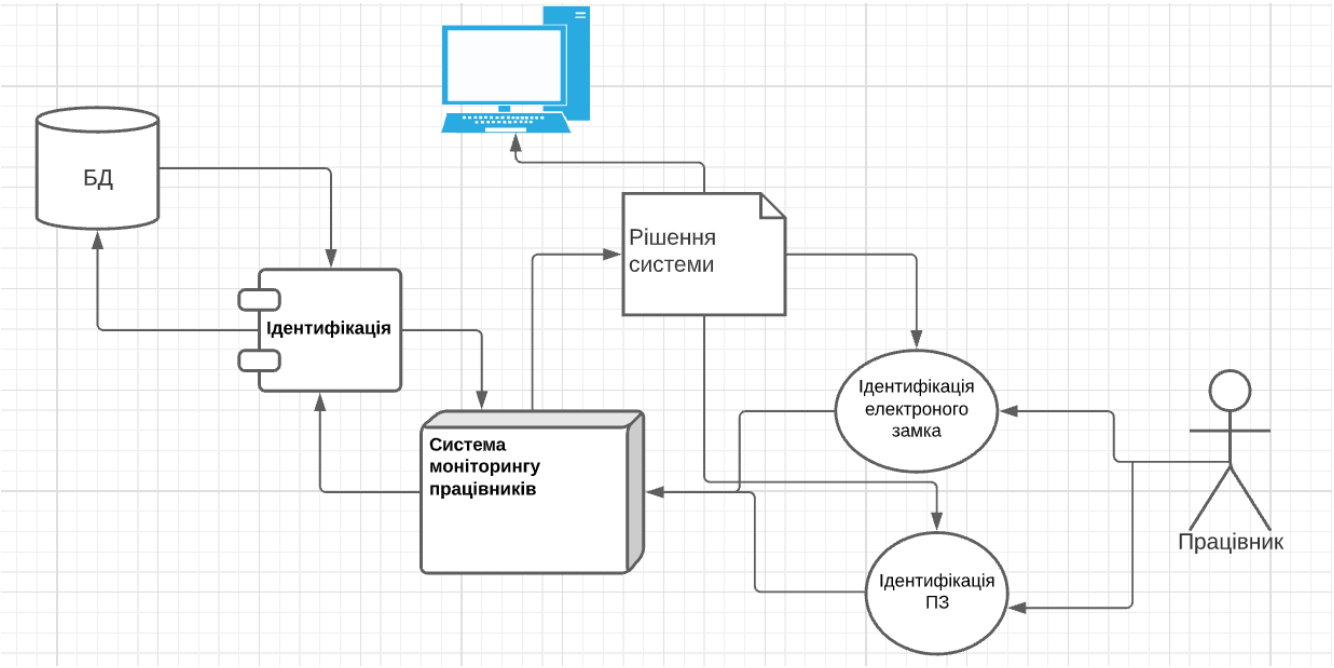


Рис 2 UML діаграма авторизації

Висновок 2

Будь яке сучасне підприємство потребує гідний рівень захисту даних та конфіденційної інформації як підприємства так і працівників.

В ході проведення дослідження був обраний порівняльний метод.

Такий підхід дозволяє порівняти готові програмні засобі та обрати найбільш оптимальний варіант.

Моніторинг працівників дозволить усунути такі основні проблеми :

– Низький рівень захисту даних;

– Неефективне керування працівниками;

– Збільшить рівень захисту окремих систем(персональних комп’ютерів);

Головна перевага даної системи в тому що будь яка спроба авторизації чи викрадення даних не зможе пройти повз систему. Головний недолік полягає в тому, що програмне забезпечення не зможу відразу виконувати всі функції на повну, а пройде певна кількість часу перед тим як система буде виконувати всі функції.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ПІДСИСТЕМИ МОНІТОРИНГУ ПРАЦІВНИКІВ ПРАТ ОБОЛОНЬ

3.1 Вибір середовища розробки

Для створення програмного забезпечення було розглянуто значну кількість варіантів, як мов програмування так і баз даних. Для обрання програмного забезпечення був використаний метод порівняння при якому було здійснено аналіз, вивчено можливості та інструменти для контролю та розробки.

Оптимальним варіантом стали Microsoft visual 2019 використав мову програмування C # та Microsoft sql server 2018 для забезпечення створення додатку.

3.2. Інформаційне забезпечення системи

Для забезпечення працездатності будь якої інформаційної системи чи програмного забезпечення яка працює з інформацією необхідно створити базу даних. Для створення бази даних використано програмне забезпечення Microsoft SQL server 2018(SQL сервер та SQL server manager для зручного керування). Програмний продукт від Microsoft дозволяє швидко створити базу динних, а також інтегрувати до додатку за допомогою вбудованих інстрментів Microsoft visual studio 2019.

Для ідентифікації та моніторингу працівників створено таблицю “ідентифікація” з полями:

-Код рівня доступу

-ID працівника

-ID перепуски

-Серійний номер обладнання

Для отримання та перевірки особистих даних створено таблицю “працівники” з полями:

-ID працівника

-ПІБ

-Посада

-Код договору

-Дата початку дії договору

Для перевірки рівня доступу створено таблицю “перепустка” з полями:

- ID перепустки
- Рівень доступу

Для контролем за персональними пристроями ідентифікації створено таблицю “обладнання” з полями:

- Серійний номер обладнання
- Тип обладнання

Для забезпечення веб захисту створено таблицю “Веб захист” з полями:

- Серійний номер обладнання
- Заблоковане посилання

Для забезпечення захисту від вірусних загроз створено таблицю “Захист від ПЗ” з полями:

- Ідентифікатор модулю захисту
- Цифровий підпис
- DRM
- Серійний номер обладнання

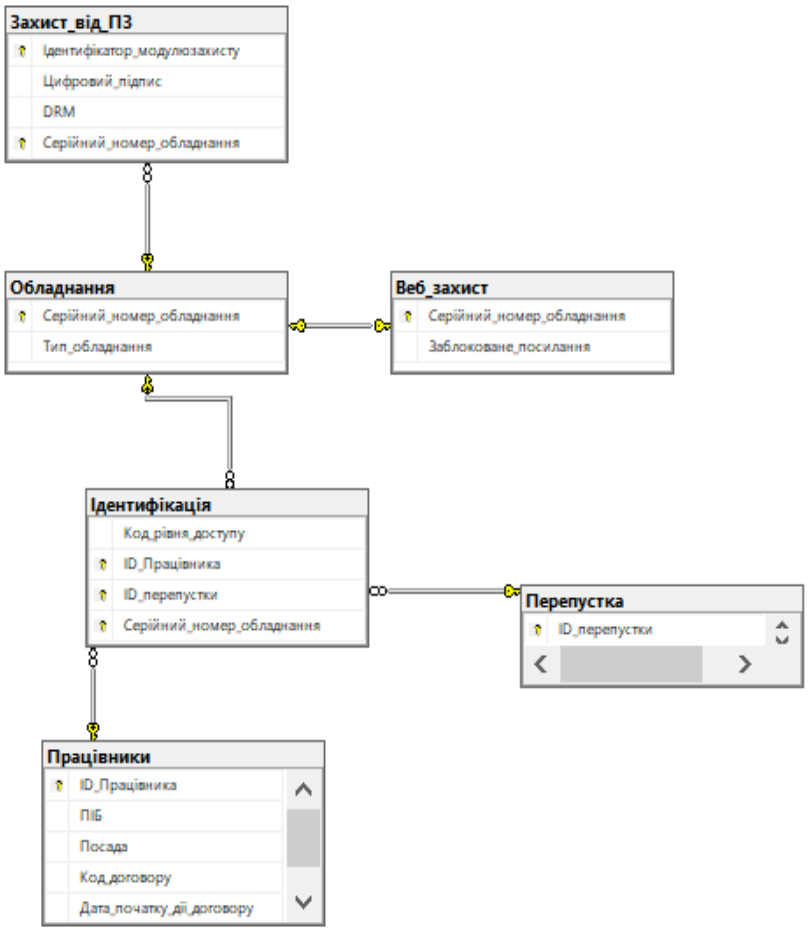


Рис 3 База даних

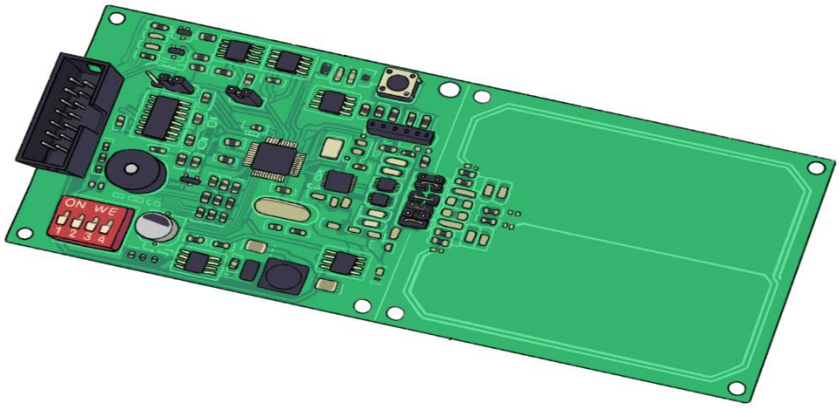
3.3Апаратне забезпечення

Для реалізації апаратної частини використано наступне обладнання:

-Зчитувач smart card

-Безконтактний пропуск(smart card)

-NFC чіп



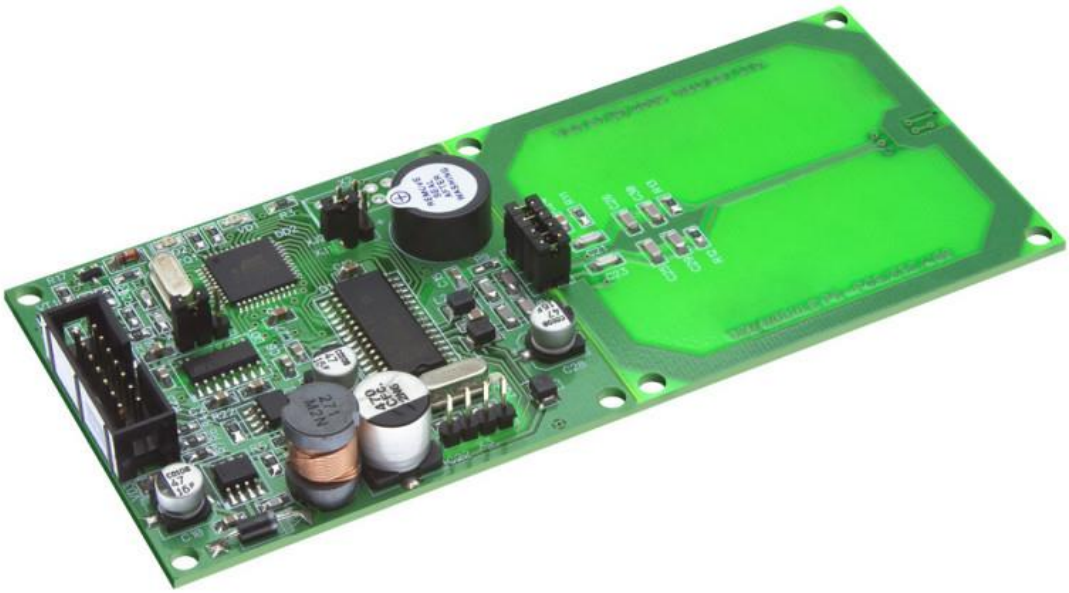
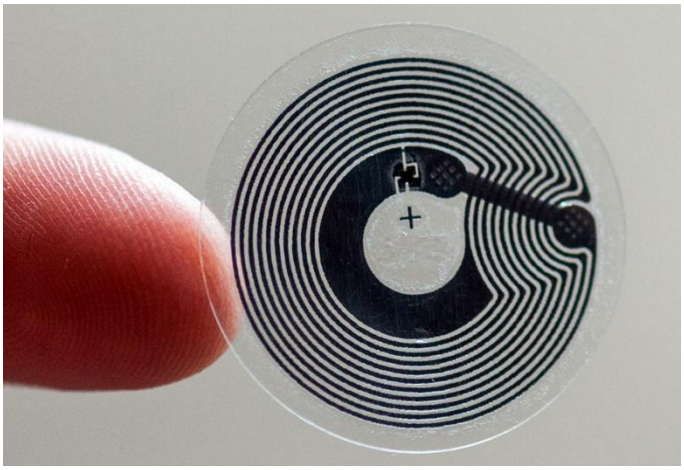


Рис 4-5 зчитувачі smart card

Рис 6 перепустка smart card



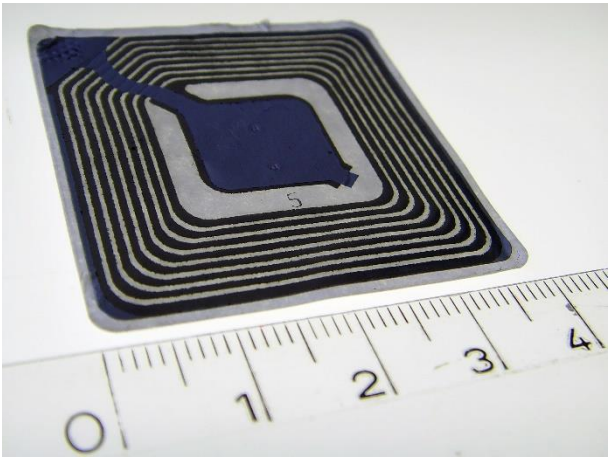


Рис 7-8 Приклади nfc чіпів

Для отримання роботи двох NFC чіпів до електронної перепустки додається додатковий чіп який реагує лише на оригінальні системи для зчитування. Таким чином ми отримуємо перепустку з одним постій активним чіпом та одним напів активним. Додатковий чіп використовується для отримання спеціального електронного ключа і може бути задіяний лише в “рідних” апаратних інструментах для зачитування даних.

3.4. Методи вирішення задач

Створення інтерфейс користувача для зручної роботи з програмним продуктом

Для створення середовища користувача був обраний Microsoft visual studio 2019 та платформа Windows.form дана платформа дозволяє швидко виконати поставлені завдання, створити графічний інтерфейс простим та зрозумілим.

Для роботи з базою даних visual studio дозволяє створити зявзок та проводити роботу з даними в середині створеного програмного продукту і звертатись за допомогою до Microsoft SQL server лише в екстрених випадках.

3.4.1. Авторизація працівника

Моніторинг працівників та забезпечення інформаційної безпеки на підприємстві є тісно сплетені і забезпечення якісного моніторингу та контролю за працівниками рівноцінно збільшенню інформаційної безпеки. Адже найбільшою небезпекою для будь яких систем є самі працівники.

Майбутня система повинна містити в своїх елементах авторизацію. Адже лише працівники служби безпеки та керівники деяких відділів можуть мати доступ до інформації.

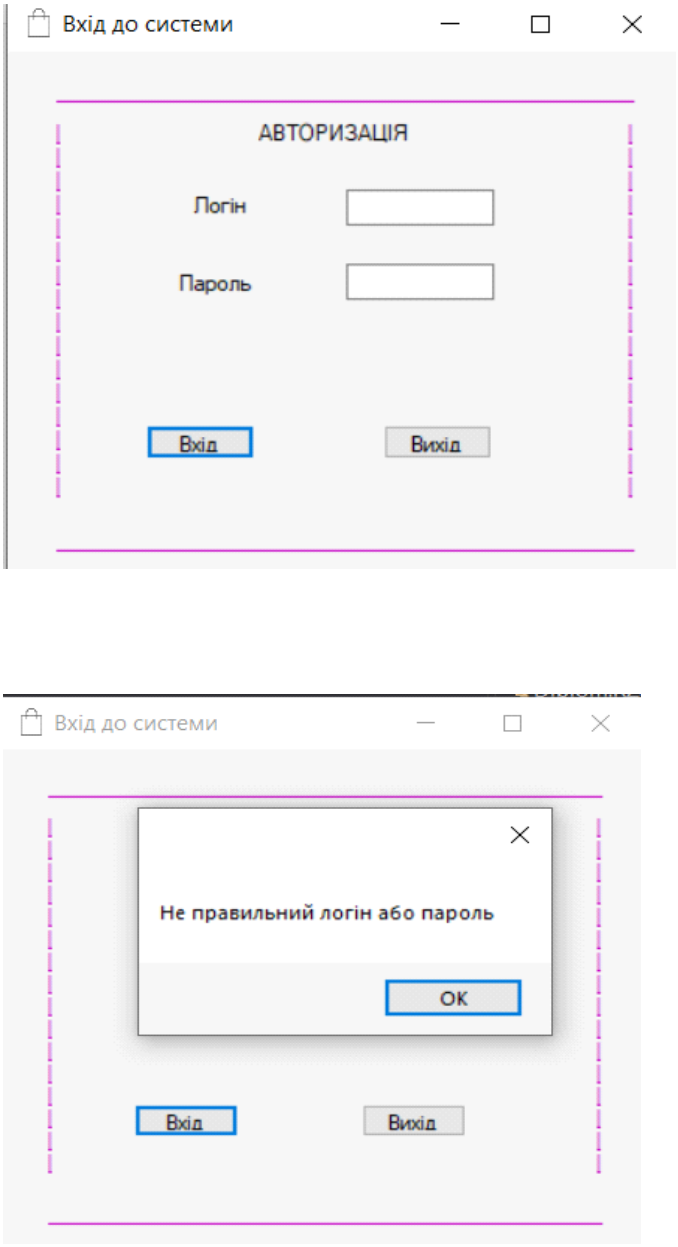


Рис 9-10 форма авторизації

В системі моніторингу працівників присутня авторизація за допомогою логіну та паролю. Додатковим захистом є шифрування даних яке вимагає постійного підключення до мережі компанії для роботи програмного забезпечення. Такий підхід дозволяє бути впевненим, що такого рівні захисту буде достатньо для базового захисту. Крім того при постійних спробах авторизації із невірними даними програмне забезпечення заблокує мак адрес пристрою та повідомить до служби безпеки.

Для захисту даних від неавторизованого доступу створена та впроваджена процедура авторизації та використано напрацювання з відділу інформаційної безпеки. Авторизація дозволить перевірити хто намагається отримати доступ до програмного продукту. Для забезпечення інформаційної безпеки програмне забезпечення буде відхилювати будь які спроби увійти або запити які прийшли із зовнішнього рівня мережі. Отже для того щоб працювати з модулем моніторингу працівників персональний комп'ютерний пристрій має бути підключений до корпоративної мережі.

Для успішної авторизації мають бути виконані дві умови:

- Введення вірного логіну та паролю

- Підключення до програмного забезпечення за допомогою корпоративної мережі

3.4.2. Інформаційна безпека

Для забезпечення веб захисту створено спеціальну базу даних де зберігаються всі небезпечні веб посилання. При спробі перейти на веб ресурс спершу йде порівняння з БД а вже потім система дозволяє, або забороняє перехід та використання.

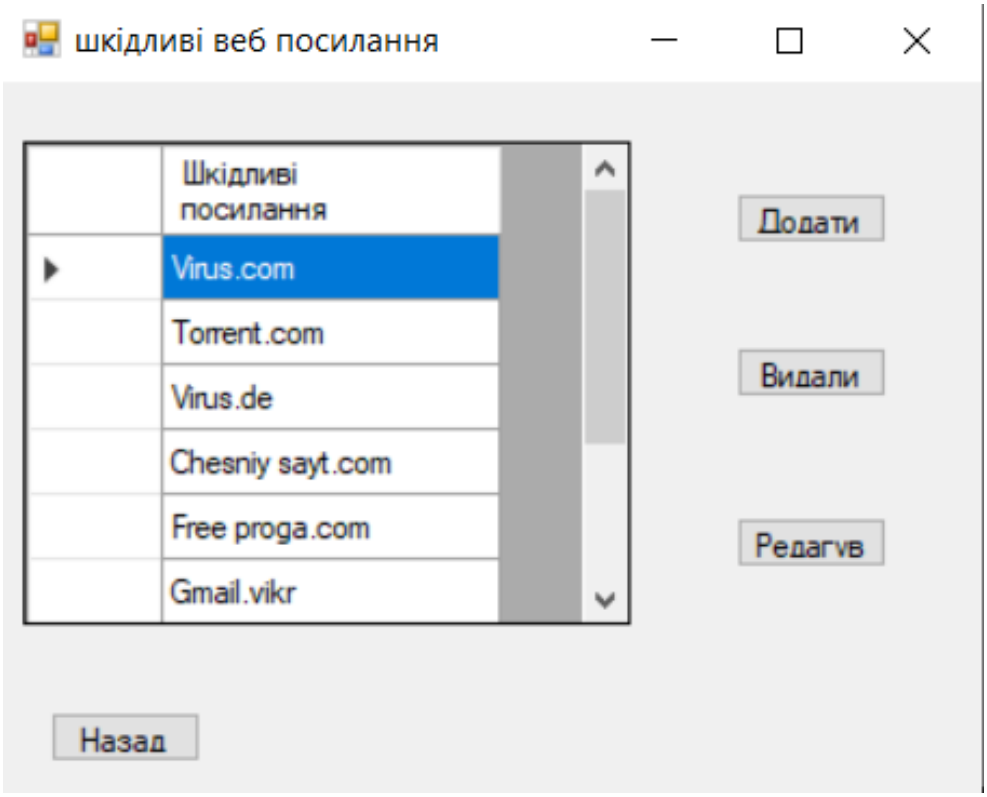


Рис 11 База даних із шкідливими посиланнями

Для забезпечення захисту пристроїв використається система яка перевіряє цифровий підпис програмного забезпечення і при його наявності дозволяє проводити інсталяцію, при відсутності забороняє.

3.4.3. Звітна інформація

Звітна інформація формується за допомогою майстра звітів та інструментів report

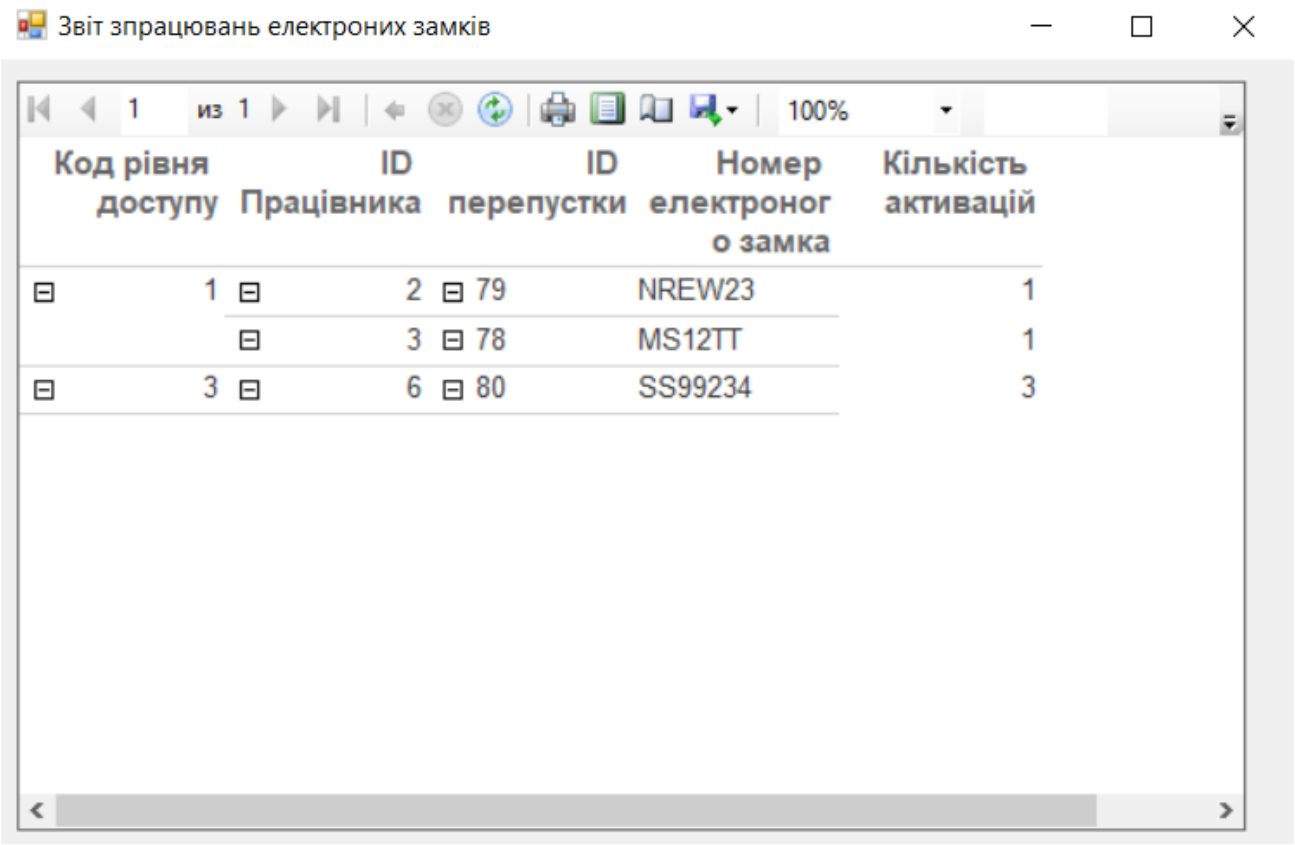


Рис 12 звіти спрацювання електронних замків

3.4.4. Головне меню

Головне меню виконане в мінімалістичному стилі. Мінімалізм дозволяє виконати роботу без великої кількості елементів, які будуть нагромаджувати інтерфейс програмного забезпечення і відволікати працівників, або створювати складнощі для працівників які виконують свої службові обов’язки.

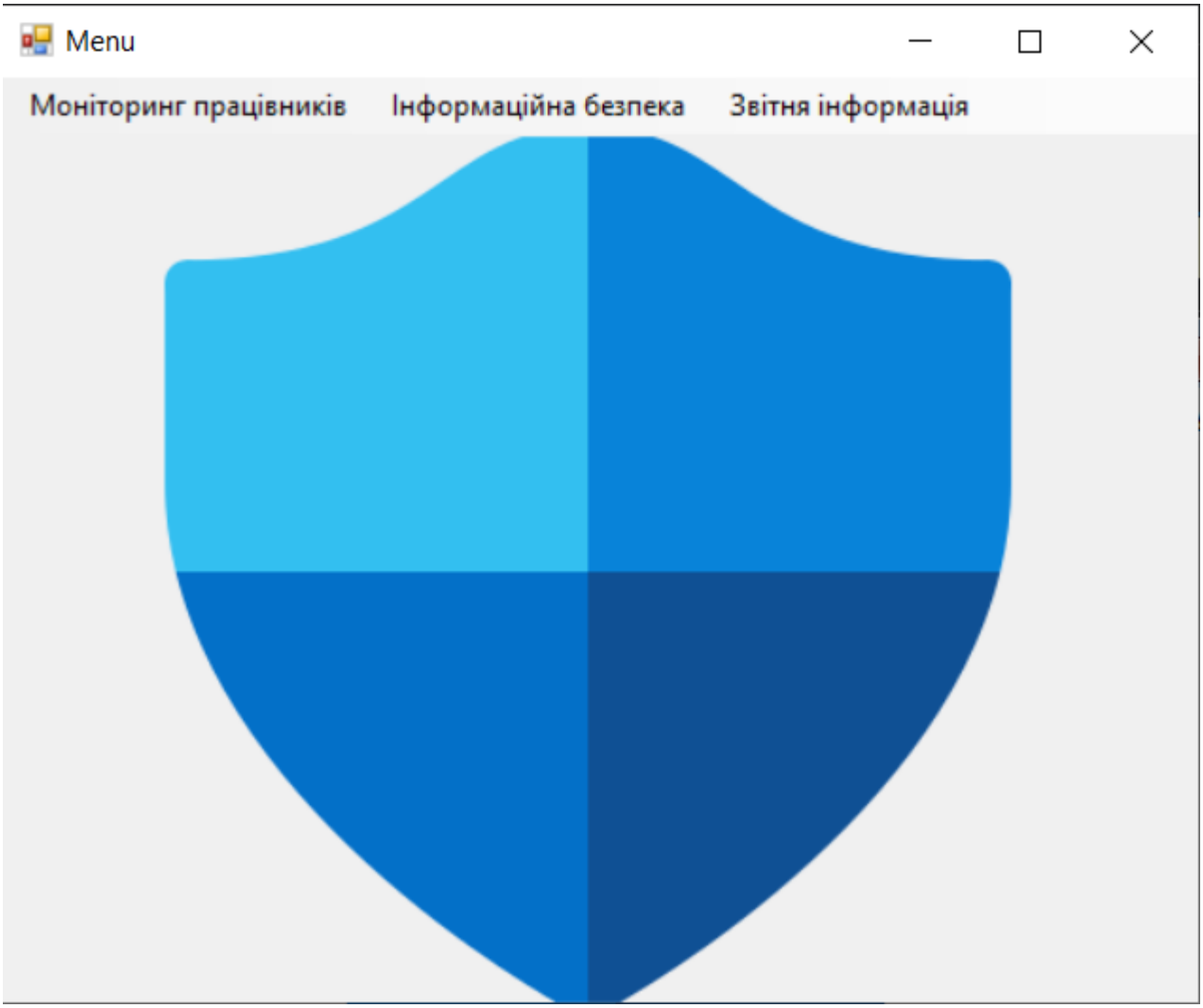


Рис 13 Головне меню програмного забезпечення підсистеми моніторингу працівників.

Для проведення ідентифікації працівників використовуються унікальні електроні замки в різких кімнатах де потрібна підвищена безпека та на пропускних пунктах. Спеціальне обладнання зчитує дані з перепустки, проводить дешифрування. Після чого передає дані до системи, яка проводить дешифрування даних та витягує спеціальний код з якого генерується електронний ключ. Завдяки такому підходу значно підвищується рівень безпеки так, як навіть після копіювання даних з перепустки та створення фальшивої перепустки для проникнення на територію підприємства система дізнається про спробу неавторизованого доступу через спеціальне шифрування яке в своєму коді містить унікальні елементи в чіпі

для ідентифікації. Крім того система підтягує особисті дані працівника для покращення процесу ідентифікації та контролю переміщення.

Якщо працівник пройде успішну авторизацію то система про це повідомить. У вікні програми поля Код рівня доступу, ID працівника, ID перепустки та електронний ключ будуть ідентичні. Крім того поля ПІБ, посада, код договору та дата початку дії договору покажуть інформацію про працівника.

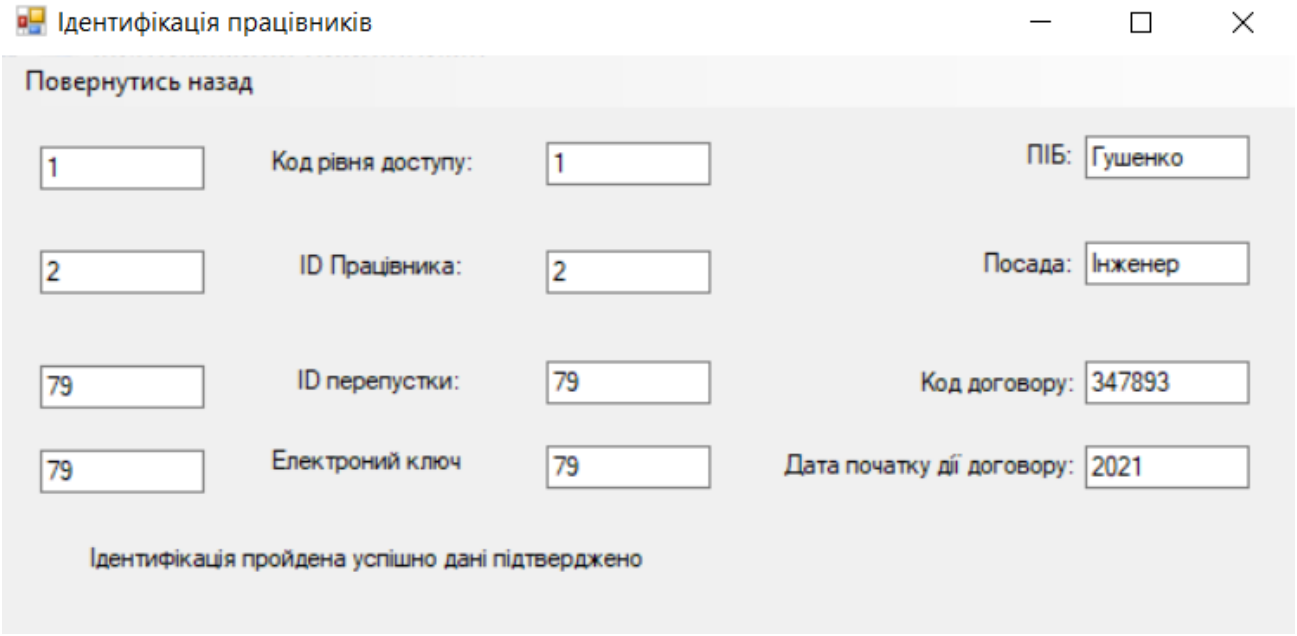


Рис. 14 приклад успішної ідентифікації

Як що працівник не пройде авторизацію, або хтось скопіює дані перепустки та спробує пройти на підприємство, або відкрити захищену кімнату.

Поля Код рівня доступу, ID працівника, ID перепустки з одної сторони будуть заповнені, а поле електронній ключ буде некоректно замовлене через те що система не можу зчитати унікальній код чіпу. А інформація про працівника буде відсутня.

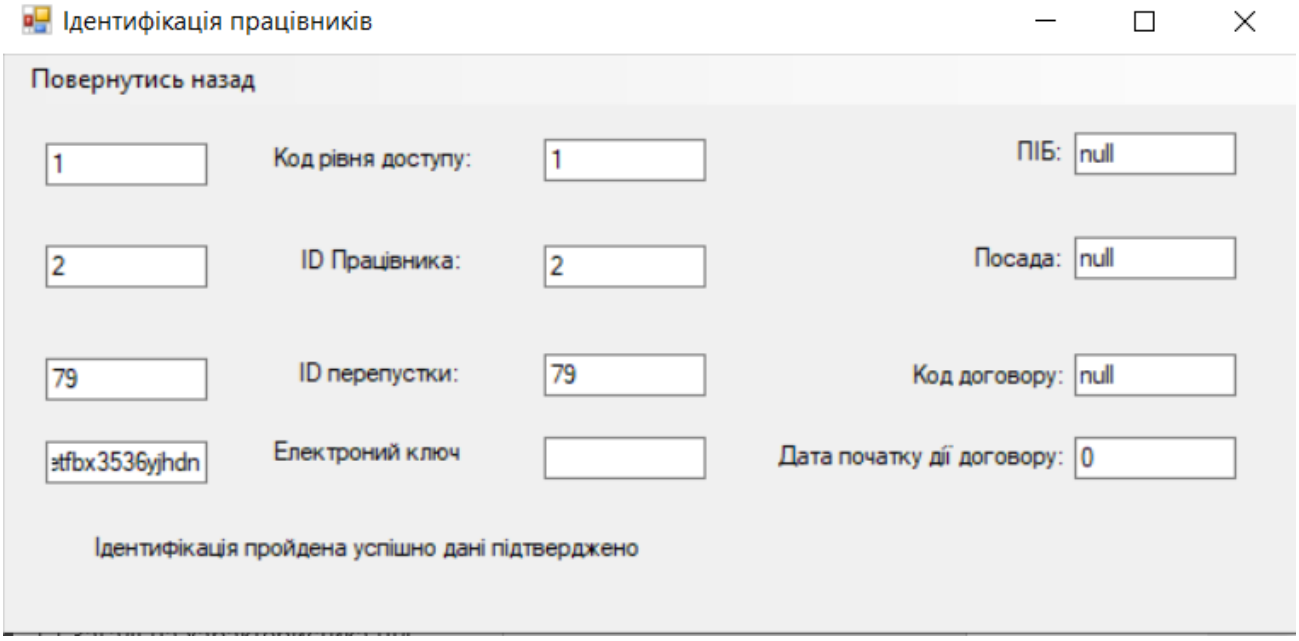


Рис. 15 Приклад не коректної ідентифікації

3.3.5. Забезпечення Web захисту

Для забезпечення веб захисту використовується спеціальний модуль. Головним завдання модуля є відслідковування всіх посилань за якими намагаються перейти працівники та їх блокування. Всі заблоковані посилання записуються в базу даних. При спробі перейти за посилання спершу проводиться перевірка чи присутнє таке посилання в спеціальній БД.

Якщо посилання відсутнє, то система дозволяє користувачеві перейти до веб ресурсу.

Якщо веб посилання присутнє в спеціальній базі даних, то перехід за веб посиланням буде заблокованим, а запис про блокування переходу за вірусним, або підозрілим посиланням буде додане в базу даних у вигляді серійного номеру обладнання, заблокованого посилання, ID працівника, ПІБ та посада.

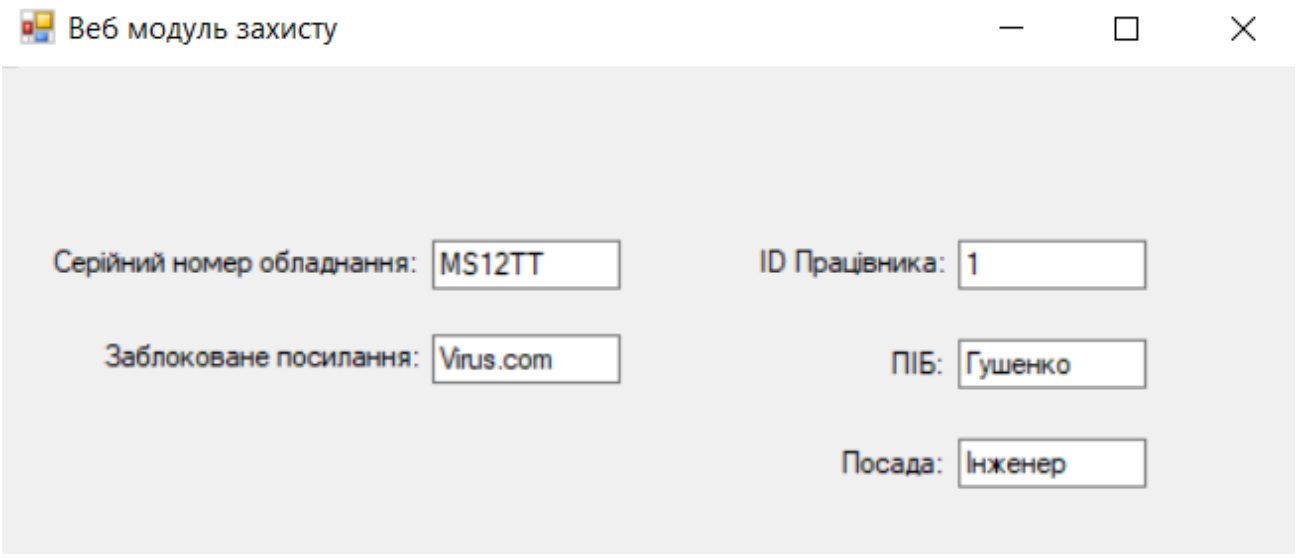


Рис. 16 Реєстрація інформації при спробі перейти за забороненим посиланням.

3.4.6. Захист від стороннього забезпечення

Захист від стороннього забезпечення відіграє важливу роль в інформаційній безпеці будь якого підприємства. Адже значна кількість втрати інформації завдячує саме встановлені програмного забезпечення з сумнівних джерел та без цифрових підписів.

Цифровий підпис це унікальна мітка(підпис) яку ставлять власники, або розробники на своє програмне для його ідентифікації.

Будь яке програмне забезпечення отримане з сумнівних або невідомих джерел може містити шкідливий код. За допомогою якого зловмисники зможуть скопіювати, пошкодити або отримати контроль частини системи. Даний може призвести до втрати конфіденційно даних. Систма захисту створена для саме для забезпечення інформаційної безпеки та зменшення шансу викрадення даних шляхом потрапляння шкідливого програмного забезпечення.

Як що система не знайде цифровий підпис то буде створено запис в базі даних де буде інформація про ідентифікатор модулю захисту, інформація про цифровий підпис(для виключення випадкового спрацювання), дані захисту програмного забезпечення(DRM) та інформація про працівника.

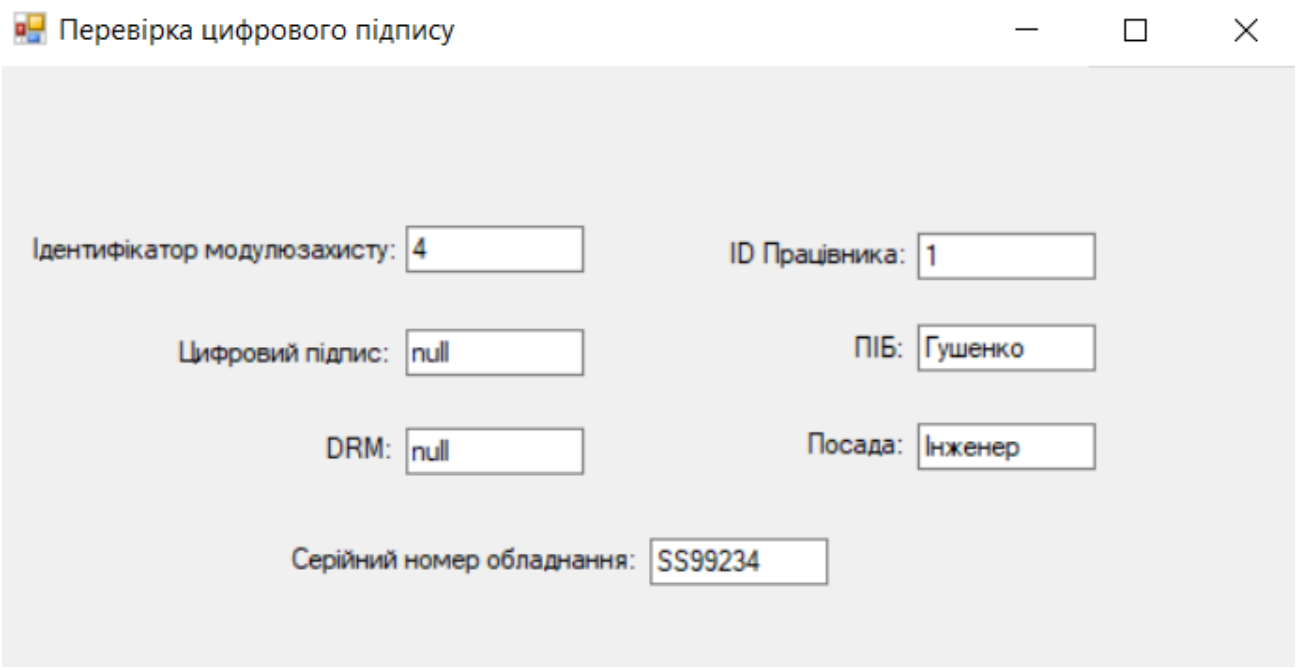


Рис. 17 Реєстрація інформації при спробі перейти за забороненим посиланням

3.5. Релевантність розробки

Для розрахунку релевантності потрібно розрахувати скільки підприємство витратить на готові рішення захисту, або зможе заощадити використовуючи власне програмне забезпечення.

Використання сторонніх систем захисту та моніторингу працівників потребує значних капіталом вкладень та несе ряд обмежень для підприємства:

- Всі дані можуть бути скопійовані на сервера власника
- Приватне акціонерне товариство Оболонь не є власником та не може змінювати, або якимось чином змінити програмний продукт на програмному рівні.
- Доступ до контрою за програмним забезпеченнями мають представники розробників, що може поставити під сумнів безпеку конфіденційної інформації та підірвати Інформаційну безпеку підприємства.
- Програмне забезпечення поставляється з закритим кодом, а отже компанія не може бути впевнена в тому, що система не відправляє якісь дані розробникам.

- У випадку проблем підприємство стає залежим від швидкості реакції партнера.
- Програмне забезпечення не може бути інтегроване в сервіси компанії.

Тип програмного забезпечення: керування персоналом та інформацією.

Рівень використання нових елементів в написані програмного забезпечення.

Перевірка та визначення складності написання нових алгоритмів роботи: Алгоритми матимуть можливість розв'язувати стандартів завдання

Типи ніформації наведені в таблиці 3.4.1.

Таблиця 3.4.1. Визначення типу інформації

Тип інформації	Позначення	Кількість наборів даних
Кількість видів змінної інформації	ЗІ	M = 3 (1 вх, 2 вих)
Кількість видів нормативно-довідкової інформації	НДІ	N = 3
Кількість банків (баз) даних	БД	P = 2
Обробка в Real time	РЧ	Так
Забезпечення телекомунікаційної обробки даних та керування об'єктами які знаходяться віддалено	ТОУ	Ні

Витрати часу для розробки та створення ескізного проекту ескізного проекту T_1 і технічного завдання T_2 наведено в таблиці 3.4.2.

Таблиця 3.4.2.Визначення витрат часу

Тип системи	Стадія розробки системи	
	Ескізний проект, T_1	Технічне завдання, T_2
Керування виробничою інформацією.	45	16

Визначаються витрати часу на стадії «технічний проект», «робочий проект» і «впровадження».

Базове значення витрат часу для стадії «технічний проект»:

$$T_{Бз} = 47$$

Коефіцієнти k_1, k_2, k_3 для стадії «технічний проект» наведені в таблиці 2.6.3. Також нижче в таблиці 3.1.4 наведено коефіцієнт використання нових ідей в проекті k_0 для кожної з стадій систем розробки.

Таблиця 3.4.3. Коефіцієнти k_1, k_2, k_3 для стадії «технічний проект»

Тип використаної інформації	Ступінь новизни
	Г
k_1 (ЗІ)	0,5
k_2 (НДІ)	0,43
k_3 (БД)	1,24

Таблиця 3.4.4. Коефіцієнт ступеню використання нових ідей в проекті, k_o

Стадія розробки системи	Вид обробки	Ступінь новизни
		Г
Технічний проект	РЧ	1,10
Робочий проект	РЧ	1,150
Впровадження	РЧ	1,06

Коефіцієнт трудовитрат на стадії «технічного проекту»:

$$k_{\text{п}} = \frac{k_1 * m + k_2 * n + k_3 * p}{m + n + p} = \frac{0{,}5 * 5 + 0{,}43 * 4 + 1{,}25 * 2}{3 + 4 + 2} = \frac{6{,}72}{9} = 0{,}74$$

Визначення витрат часу для стадії «технічний проект» (T_3):

$$\text{Т}_{\text{з}} = \text{Т}_{\text{Бз}} * k_{\text{п}} * k_{\text{о}} = 47 * 0{,}61 * 1{,}1 = 31{,}537$$

Базове значення витрат часу для стадії «робочий проект»:

$$\text{Т}_{\text{Б4}} = 75$$

Коефіцієнти k_1, k_2, k_3 для стадії «робочий проект» наведені в таблиці 2.6.5.

Таблиця 3.4.3. Коефіцієнти k_1, k_2, k_3 для стадія «робочий проект».

Тип інформації яка була використана	Група складності алгоритму	Ступінь використання нових ідей
		Г
k_1 (ЗІ)	3	0.48
k_2 (НДІ)	3	0.29
k_3 (БД)	3	0.24

Коефіцієнт трудовитрат на стадії «робочий проект»:

$$k_{\text{п}} = \frac{k_1 * m + k_2 * n + k_3 * p}{m + n + p} = \frac{0{,}48 * 5 + 0{,}29 * 4 + 0{,}24 * 2}{3 + 4 + 2} = \frac{4{,}04}{9} = 0{,}448$$

Коефіцієнт складності контролювання вхідних та вихідних даних:

$$k_c = 1.00\ (l2; 22)$$

Визначення витрат часу для стадії «робочий проект» (T_4):

$$\text{Т}_4 = \text{Т}_{\text{Б4}} * k_{\text{п}} * k_{\text{о}} * k_c = 75 * 0{,}367 * 1{,}15 * 1 = 31{,}654$$

Базове значення витрат часу для стадії «впровадження»:

$$\text{Т}_{\text{Б5}} = 21$$

Визначення витрат часу для стадії «впровадження» (Т_5):

$$\mathrm{Т}_5 = \mathrm{Т}_{Б5} * k_{\text{п}} * k_{\text{о}} * k_c = 21 * 0{,}367 * 1{,}05 * 1 = 8{,}092$$

Визначення загальних витрат часу на розробку системи*:*

$$T_\varepsilon = T_1 + T_2 + T_3 + T_4 + T_5 = 45 + 16 + 31{,}537 + 31{,}654 + 8{,}092 = 132{,}283$$

Визначення чисельності виконавців. Для дипломного проекту (випускової роботи) кількість робочих годин складає 530 із 7-годинним робочим днем, тому на розробку проекту виділено Ф, днів:

$$\Ф = \frac{530}{7} = 75$$

Кількість місяців на розробку, М:

$$\mathrm{М} = \frac{\Ф}{25} = \frac{75}{25} = 3$$

Чисельність виконавців:

$$\mathrm{Ч} = \frac{T_\varepsilon}{\Ф} = \frac{132{,}283}{75} = 1{,}764 \approx 2$$

Місячна оплата праці програміста:

$$\mathrm{ЗП}_{\mathrm{ПР}} = 19460$$

Оплата праці виконавців:

$$V_1' = \mathrm{Ч} * \mathrm{М} * \mathrm{ЗП}_{\mathrm{ПР}} = 2 * 3 * 19460 = 116760$$

Витрати, що були направлені на розробку програмного забезпечення для ПК. Витрати на придбання доставку та установку ПК

Розрахунок річного фонду часу роботи ПК. Дійсний річний фонд часу ПК:

$$Т_{ПК} = Т_{ОП} - (6 * 8 + 5 * 12) = 2000 - (6 * 8 + 5 * 12) = 1892$$

Величина фонду часу ПК:

$$Т'_{ПК} = Т_{ПК} * \frac{R}{Т_{ОП}} = 1892 * \frac{450}{2000} = 425.7$$

Приблизна вартість персонального комп'ютора:

- $Ц_Р$ – ринкова вартість ПК (8000).
- $k_{УН}$ – коефіцієнт, який враховує витрати для приведення ПК в робочий стан (0.12).

$Ц_{ПК} = Ц_Р * (1 + k_{УН}) = 8000 * (1 + 0.12) = 8960$

Заробітна плата для персоналу яки обслуговує пристрої (якщо роботи виконуються не на власному ПК):

$$З_{ОП} = 12000$$

Амортизаційні відрахування:

$$З_{АМ} = \frac{Ц_{ПК}}{Н_А} = \frac{8960}{5} = 1792$$

$Н_А$ – норма амортизаційних відрахувань, яка для ПК дорівнює 5

Витрати на електроенергію, споживану ПК:

- Потужність ПК, $Р_{ПК}$=0,4 кВт.
- Фонд корисного часу роботи ПК, $Т_{ПК}$= 425.7 год.
- Вартість 1 кВт електроенергії для підприємств, $Ц_{ЕЛ}$=1,68 грн/кВт.
- Коефіцієнт інтенсивного використання ПК, *А* = 0,9.

$$З_{ЕЛ} = Р_{ПК} * Т_{ПК} * Ц_{ЕЛ} * А = 0,4 * 425,7 * 1,68 * 0,9 = 257,4634$$

Витрати на поточний ремонт і технічне обслуговування ПК визначаються як 6% від балансової вартості ПК (*Ц*$_{ПК}$), $З_Р$:

$$З_Р = Ц_{ПК} * 0,06 = 8960 * 0,06 = 537,6$$

Непрямі витрати, пов'язані з експлуатацією ПК, визначаються як 5% від балансової вартості ПК (*Ц*$_{ПК}$), $З_{МАТ}$:

$$З_{МАТ} = Ц_{ПК} * 0,05 = 8960 * 0,05 = 448$$

Поточні витрати на експлуатацію, V_1'':

$$V_1'' = З_{ОП} + З_{АМ} + З_{ЕЛ} + З_Р + З_{МАТ} = 12000 + 1792 + 257,4634 + 537,6 + 448 = 15035,06$$

Загальні витрати на розробку програмного забезпечення комп'ютерної системи:

$$V_1 = V_1' + V_1'' = 116760 + 15035,06 = 131795,06$$

Витрати на придбання і установку ПК:

$$V_2 = Ц_{ПК} = 8960$$

Витрати для підготовку спеціального преміщення

Дані витрати прямо залежать структури підприємства та приміщень які вже знаходяться на території. Для даного підприємства яке вже має приміщення яке повністю задовольняє вимого додаткові витрати будуть. V_3 = 0.

$$V_3 = 0$$

Витрати для проведення навчання працівників підприємства V_4, Сисктма розробляється з простим інтерфейсом та не потребує багато знань. А форми перевірки авторизації не дозволять внести зміни зо дозволяє провести прискорений курс навчання персоналу V_4 = 2000 грн.

$$V_4 = 2000$$

Порахована загальна вартість створення ескізного проекту та розробки модулю моніторингу персоналу.

Вартість створення та інтеграції модулю моніторингу працівників.:

$$V_\varepsilon = V_1 + V_2 + V_3 + V_4 = 131795{,}06 + 8960 + 0 + 2000 = 142755{,}06$$

Для розрахунку річного економічного ефекту слід розглянути норму втрати для налаштування комп'ютерних систем та загальну вартість розробки системи:

$$V_\text{P} = \frac{V_\varepsilon}{\text{H}_\text{A}} = \frac{142755{,}06}{5} = 28551{,}01$$

Річний прибуток від впровадження системи буде досягнуто за рахунок збільшення збереження коштів за рахунок зменшення кількості персоналу складе 146000 на рік

Основні джерела прибутку від впровадження комп`ютерної системи і порядок його підрахунку наведено в таблиці 3.4.1.

Таблиця 3.4.4. Основні джерела прибутку

№	Джерела прибутку	Річний прибуток, $П_Р$
1.	Збереження зменшення кількості персоналу	146000
2.	AS-IS – TO BE	-132804 ((2020 – 13087) *12)
∑=		14196

Коефіцієнт економічної ефективності розробки

$$\text{К}_\text{ЕФ} = \frac{\text{П}_\text{P}}{V_\text{P}} = \frac{14196}{28551{,}01} = 0{,}497215$$

Термін окупності розробки

$$Т_{ОК} = \frac{1}{К_{ЕФ}} = \frac{1}{0,497215} = 2,011201$$

Таким чином, термін окупності інформаційної системи буде 2 роки.

Власне програмне забезпечення моніторингу працівників дозволить проводити налаштування на програмному рівні, може бути повністю інтегровано в інформаційну інфраструктуру компанії та не допустить витоку даних через те що власником є підприємство

3.6. Інструкція користувача

Запустивши програмне забезпечення користувач потрапить до вікна авторизації де необхідно вказати логін та пароль для подальшої роботи з програмним продуктом

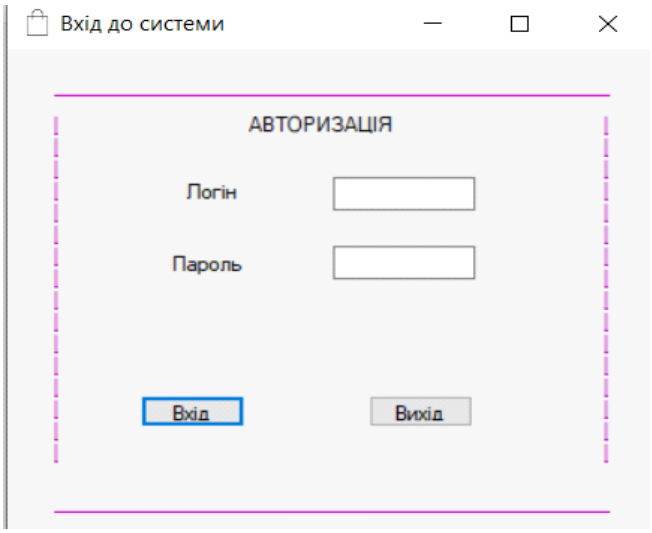


Рис 18 Форма авторизації

Після успішної авторизації користувач потрапляє до головного меню де можна додавати, видаляти, змінювати дані та здійснювати процес моніторингу персоналу

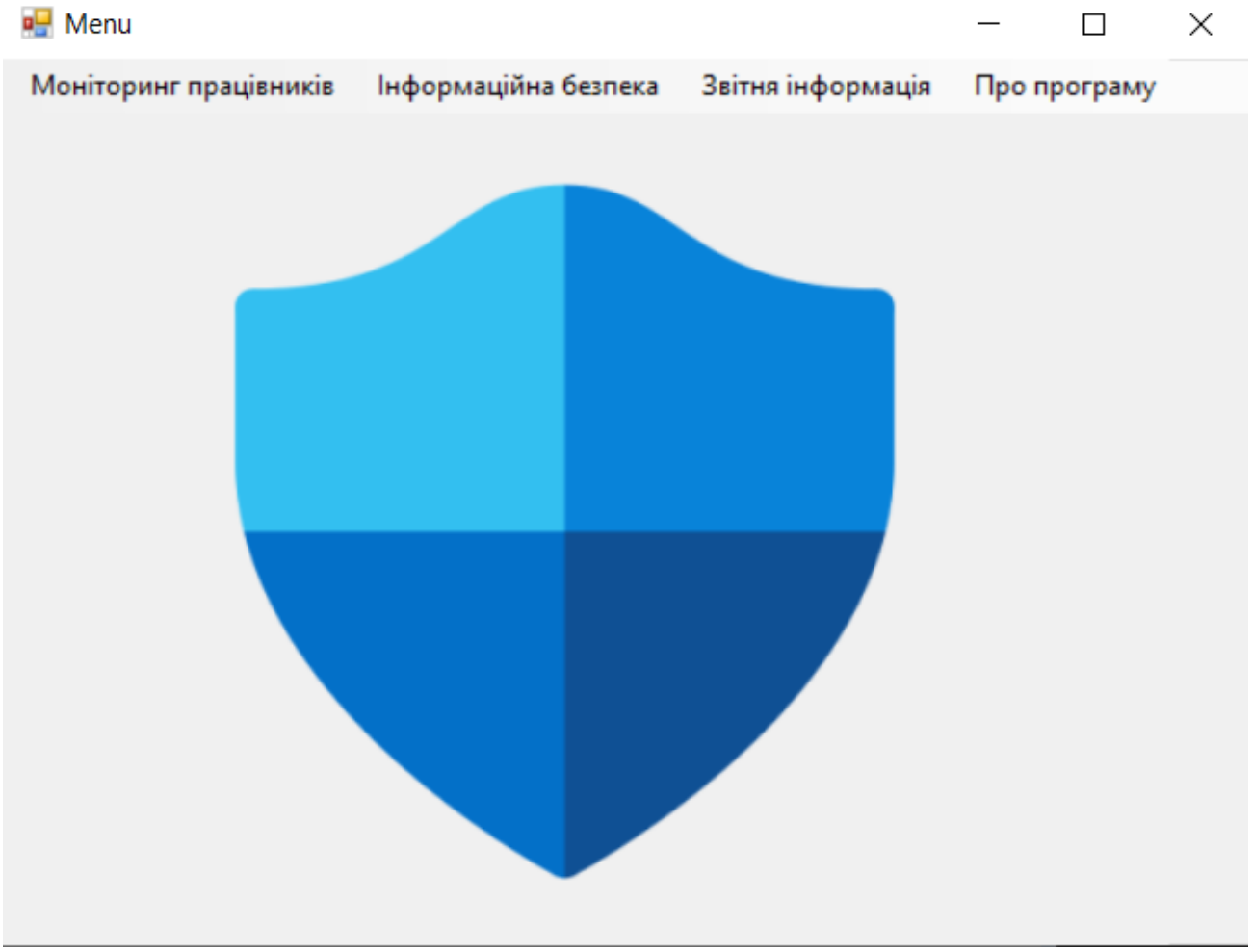
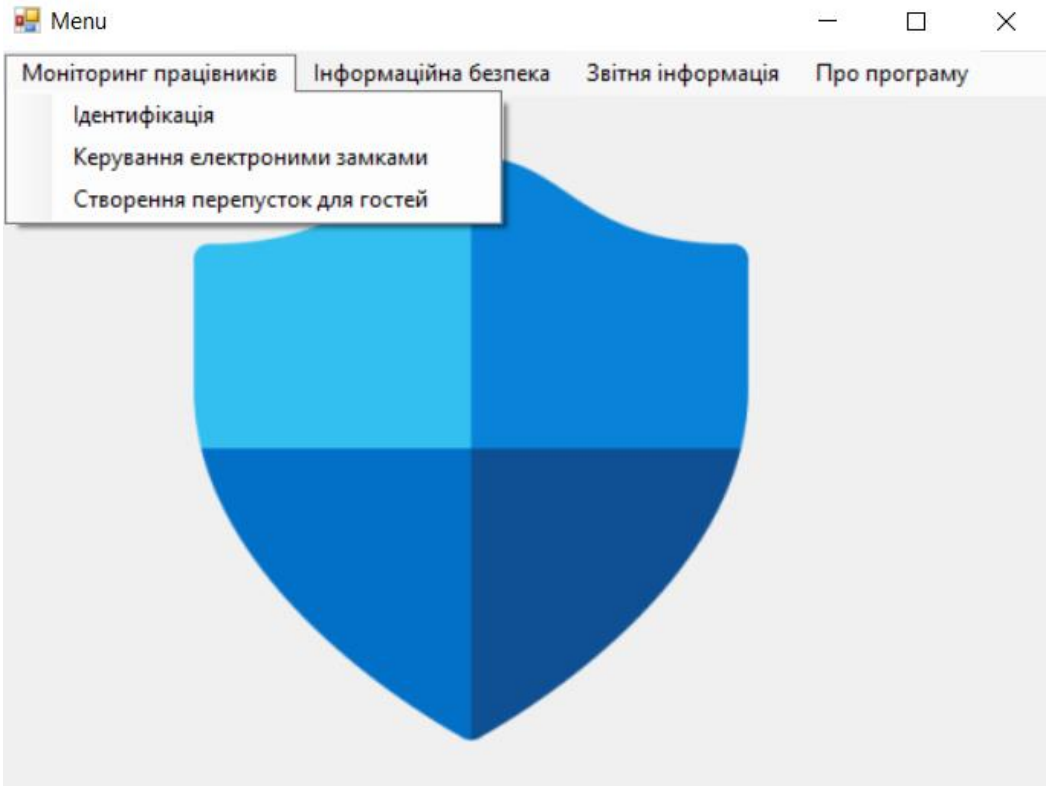


Рис 19 Головне меню

Кнопки навігації виконані за допомогою елемента Menu strip .

Після потрапляння до головного меню користувач може розгорнути підменю для отримання можливості здійснити перехід до необхідно елементів.



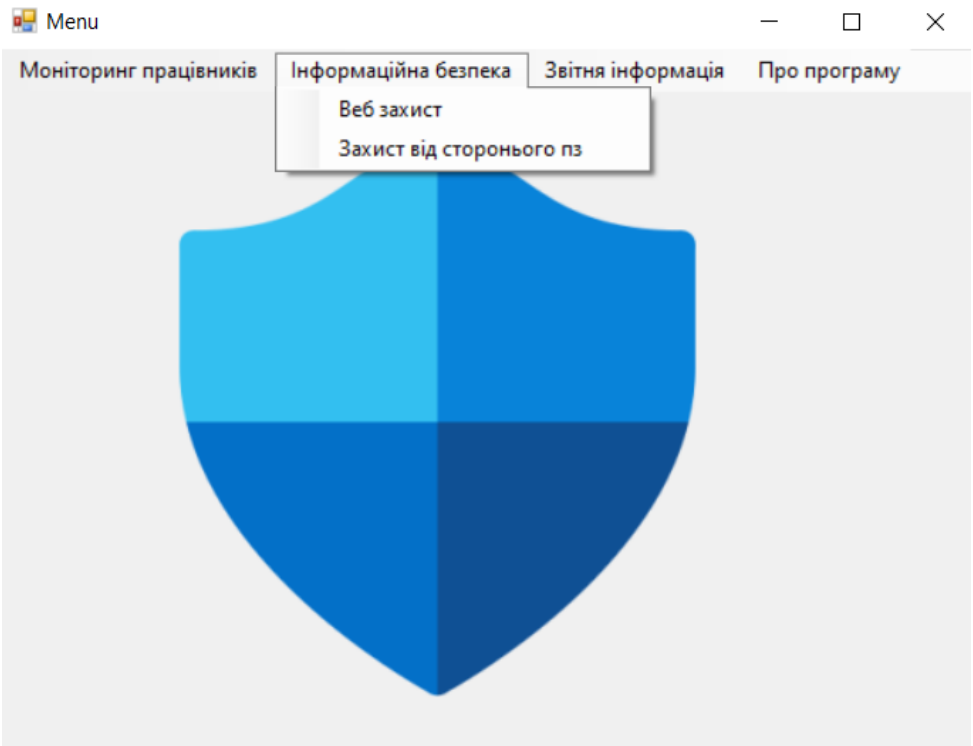
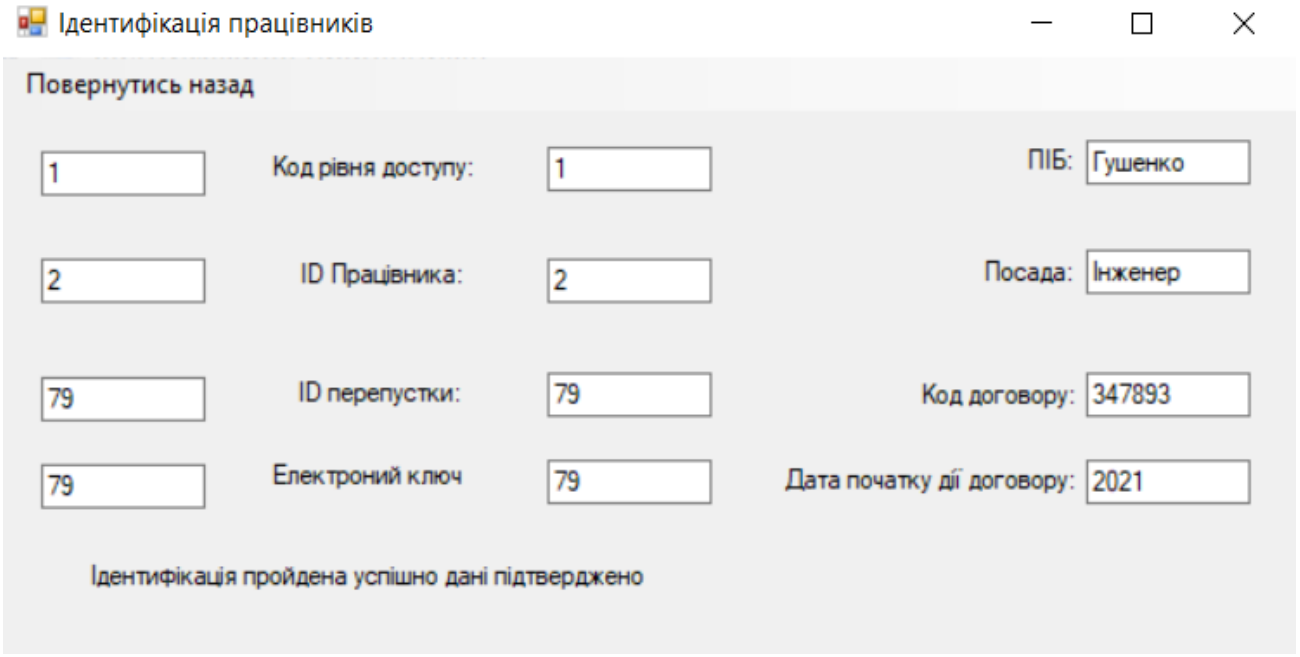


Рис 20-21 Розгорнуті підменю

Для здійснення моніторингу працівників необхідно перейти до пункту підменю “ідентифікація” де відкриється форма “Ідентифікація працівників”. На даній форма можна переглядати інформацію про працівника та перевіряти успішність чи відмову авторизації.



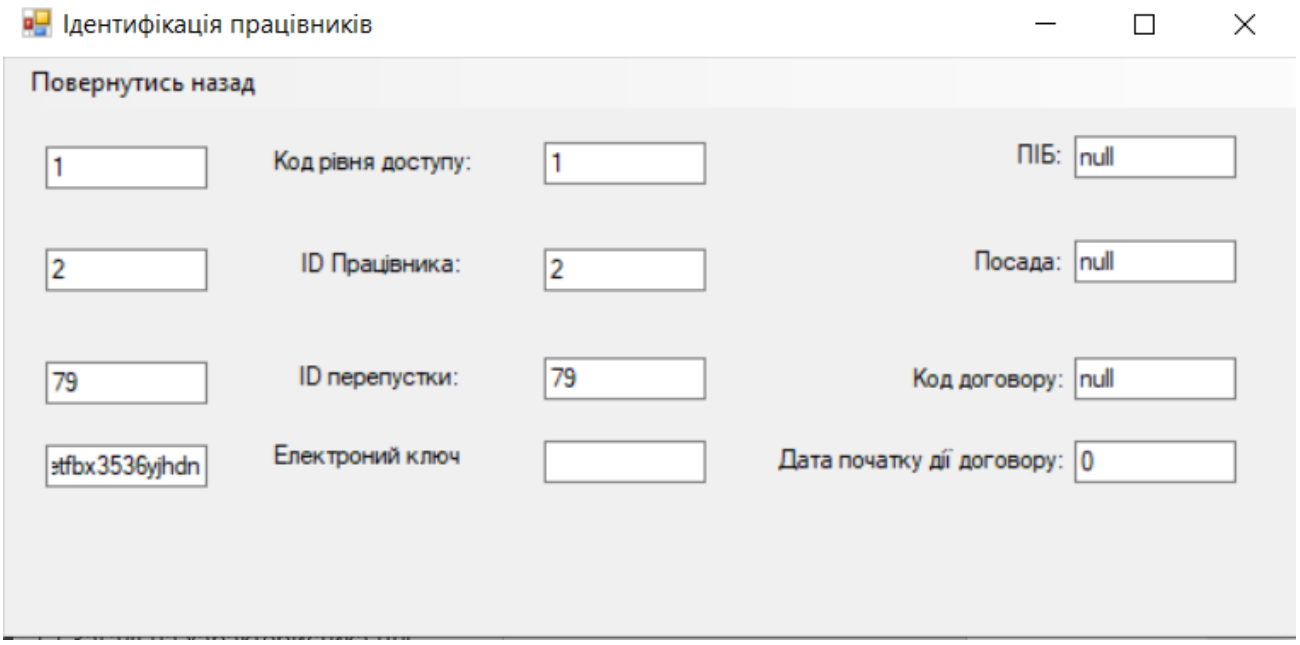


Рис 22-23 форма для ідентифікації працівників

При спроби перейти за будь яким посиланням відбувається процес перевірки посилання з шкідливими посилання в базі даних, а до програми буде здійснено запис до бази даних де буде вказано інформацію. Про працівника, номер пристрою та шкідливе веб посилання.

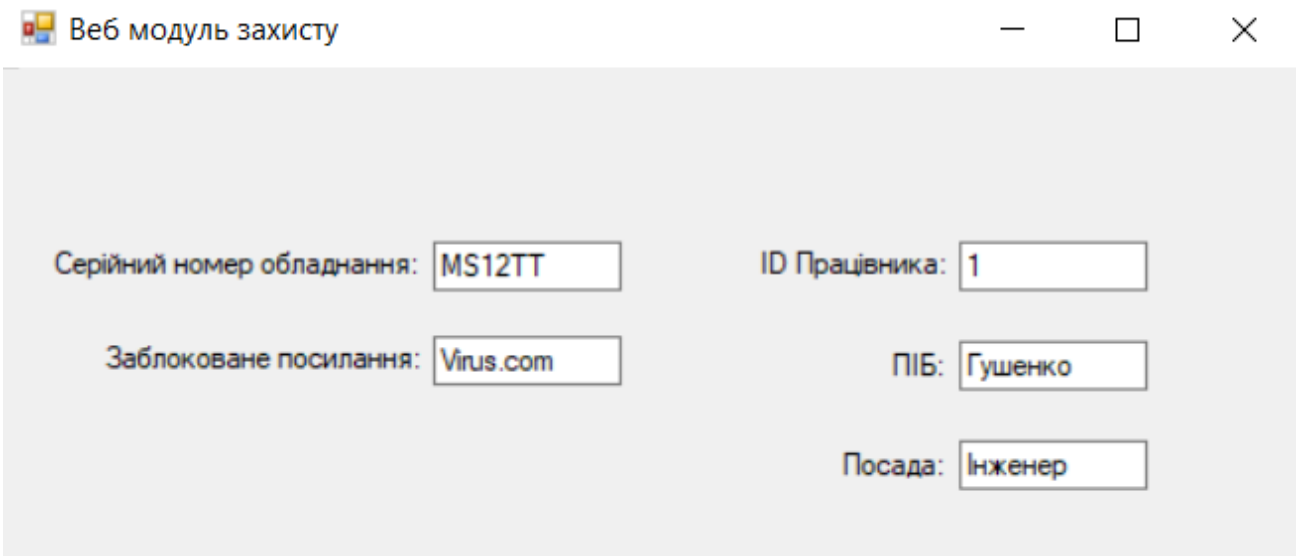


Рис 24 форма інформації про веб захист

При встановлені програмного забезпечення здійснюється перевірка цифрового підпису. Як що підпису немає встановлення не може бути розпочате, а інформація про спробу встановлення буде записано до бази даних.

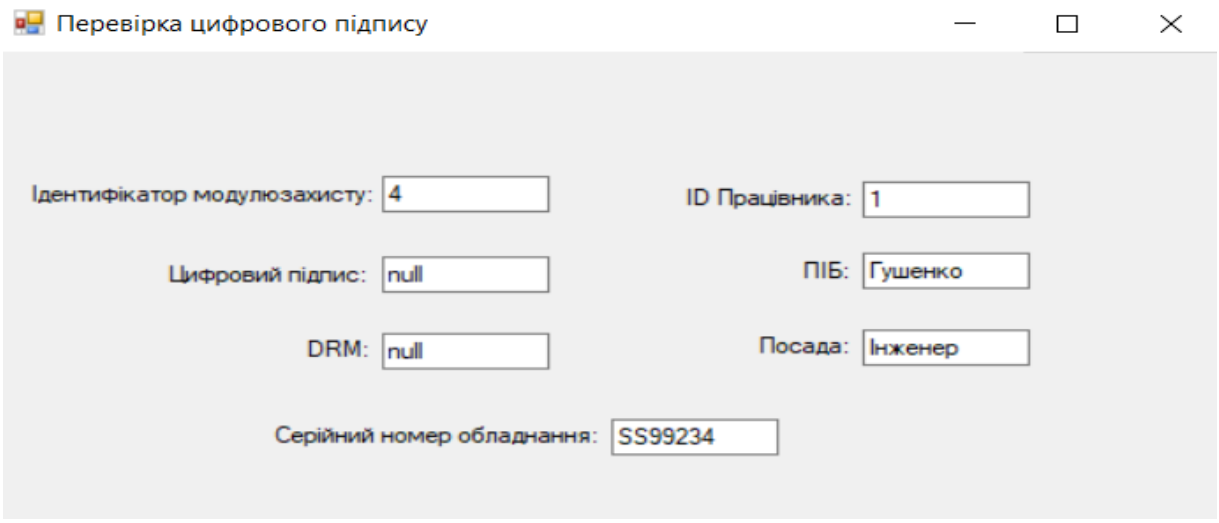


Рис 25 форма перевірки цифрового підпису

Звіти спрацювань електронних замків дозволяють моніторити пересування працівників, а також дізнатись кількість спрацювань.

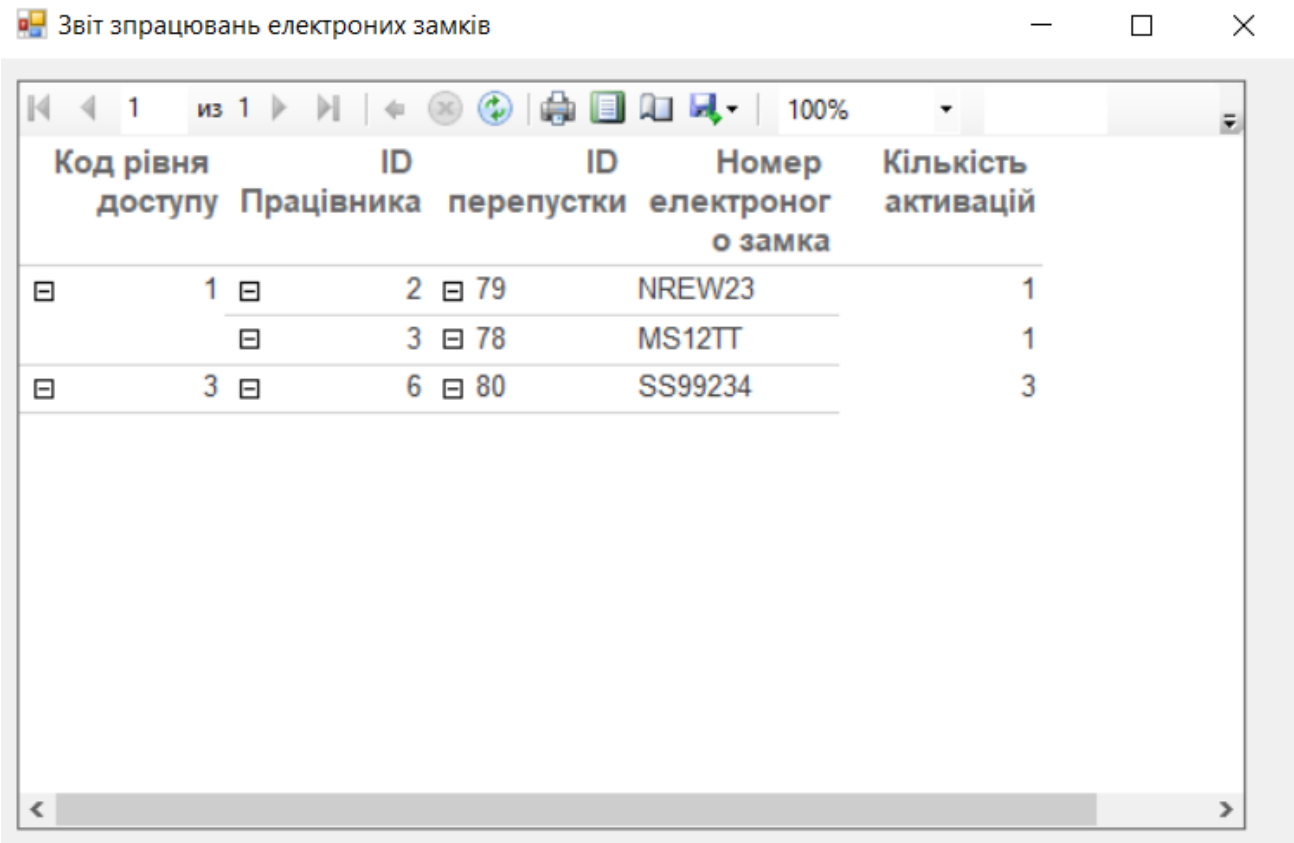


Рис 21 форма звітної інформації

Висновок 3

В сучасному світі є багато середовищ, мов програмування та інструментів для створення і роботи з інформацією(базою даних). Правильний вибір дозволяє значно пришвидшити виконання поставлених завдань. Середовище MS visual studio має інструменти синхронізації з базою даних MS SQL server, що дозволяє покращити та пришвидшити виконання поставлених завдань.

Описано методи вирішення завдань, проведено розрахунок релевантності та створено інструкцію користувача.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ НА ПІДПРИЄМСТВІ

ПрАТ Оболонь займається створенням та реалізацією різного роду напоїв..

В структурі підприємства здіяно приблизно 5680 працівників для успішного функціонування.

Підприємство завжди орієнтуєтеся на сучасні тенденції покращення рівня безпеки. Згідно нормативної документації на підприємстві раз в квартал проводять семінари де навчають персонал. Діяльність підприємства вимагає найвищого ступеню гігієни робочих приміщень Спеціальні служби разом з працівниками підприємства раз на рік проводять перевірку стану приміщень, дотримання санітарних норм та працездатності всіх систем захисту від пожежі.

4.1 Шумоізоляція

Для забезпечення комфортних умов роботи та захисту працівників від шумів та гучних звуків. Було проведено модернізацію приміщень та здіснено обшивання стін спеціальними матеріалами, які володіють першокласними властивостями для приглушення шумів та протидії пожежам. Зниженя рівня шуму майже до нуля можливе за рахунок використання спеціальних термостійких матеріалів із внутрішньої та зовнішніх частин. А наявність спеціальної стійкої сітки для протидії пожежам затримає розповсюдження полум’я в декілька раз. Що дозволить виграти необхідний час на евакуацію, або

протидію пожежі.

Сучасне обладнання генерує в рази менше шумів ніж їх старші аналоги. Але навіть теперішній рівень є досить великим. Через що значна кількість копаній та підприємств використовує спеціальні шумо поглинаючі матеріали.

4.2 Освітлення

Будь який офіс чи приміщення потребує достатньої кількості світла для комфортної роботи працівників.

В першу чергу слід звернути на рівень природнього світла. Як що його недостатньо то потрібно використовувати штучне для забезпечення комфортною умов роботи та збереження здоров’я працівників . Для забезпечення комфортних умов з мінімальними витратами можна використати комбіновану систему освітлення. Такий підхід дозволить використати природнє та штучне освітлення на максимум та дозволять зекономити. Для більшості робочих кабінетів комбінованої системи буде достатньо. А для приміщень де рівень освітленості має бути значно вищий підприємство закупило та встановило спеціальні енергоефективні джерела світла, які зможуть забезпечити необхідний рівень штучного світла.

Для забезпечення достатнього рівня штучного світла підприємство використовує лише перевірені та якісні джерела.

4.3 Техніка безпеки та електробезпека

Для забезпечення гідного рівня електро безпеки працівники підприємства постійно проходять спеціальні курси де здають екзамени та отримують посвідчення.

Після здачі екзаменів та отримання посвідчення вроводяться спеціальні семінари де представляються основи електро безпеки. Такий підхід дозволяє в декілька раз підняти рівень електро безпеки на підприємтві

РОЗДІЛ 5. ЦИВІЛЬНИЙ ЗАХИСТ

Створення спеціального плану для евакуації в разі екстрених ситуації

Вступ

Згідно вимог всі громадські приміщення де перебувають люди потребують створення спеціальної схеми евакуації при виникненні надзвичайних ситуацій(землетрус, пожежа). Даний документ є індивідуальним для кожного приміщення та створюється окремо.

Головною метою плану евакуації при надзвичайних ситуація: є дуже простою вона допомагає зорієнтуватись працівникам під час непередбачуваних та екстрених ситуація для безпечної евакуації із зони небезпеки; план евакуації вказує на можливі виходи(двері, вікна) та на спеціальне обладнання яке може допомогти в екстриних ситуаціях, а також на засоби індивідуального захисту для працівників.

Привітне акціонерне товариство Оболонь складається з комплексу офісних та виробничих приміщень з великою кількістю людей. Саме тому створення плану евакуації є дуже важливим етапом в забезпечені безпеки на підприємстві та допоможе зберегти життя та здоров’я персоналу у випадку надзвичайних ситуацій.

5.1 Проведення оцінки ризиків для персоналу в разі виникнення пожежі

Головню цілю дипломної роботи є використання створення підсистеми моніторинг у працівників та збільшення якості інформаційної безпеки на

підприємстві. Головними об’єктами з якими буде працювати програмне забезпечення це персонал приватного акціонерного товариства Оболонь . Підприємство знаходиться на закритій території та складається з багатьох офісних та виробничих приміщень, які утворюють комплекс. Весь комплекс з’єднаний між собою. Діяльність підприємства базується на використані різного роду техніки. А отже шанс впливу негативних та небезпечних факторів є досить високою.

Достатній рівень безпеки гарантований за умов, як що:

$$Q_{\text{в}} \le Q_{\text{в}}^{\text{н}},$$

де $Q_{\text{в}}^{\text{н}}$ — нормований індивідуальний ризик, $Q_{\text{в}}^{\text{н}} = 10^{-6}$ рік$^{-1}$;

$Q_{\text{в}}$ — розрахунковий індивідуальний ризик.

Час евакуації людей з території на якій є небезпечна ситуація починається з розрахунку руху одного або декілька потоків чи груп людей через спеціальні виходи.

Час необхідний для повної евакуації персоналу t_p може бути визначений, як сума часу для подолання певних ділянок t_i:

$$t_p = t_1 + t_2 + t_3 + ,...- + t_i,$$

де t_1— час руху людського потоку на першій (вихідній) ділянці, хв.;

t_1, t_2, t_3 ,..., t_i — час руху людського потоку на кожній з наступних ділянок шляху, хв.

Проведення оцінки соціального ризику можна трактувати як імовірність загибелі десятьох та більше працівників в наслідок надзвичайної ситуації.

5.2 План евакуації відділу ведення звітності

На Рис. 26 План евакуації з відділення в загальний хол та на вихід.

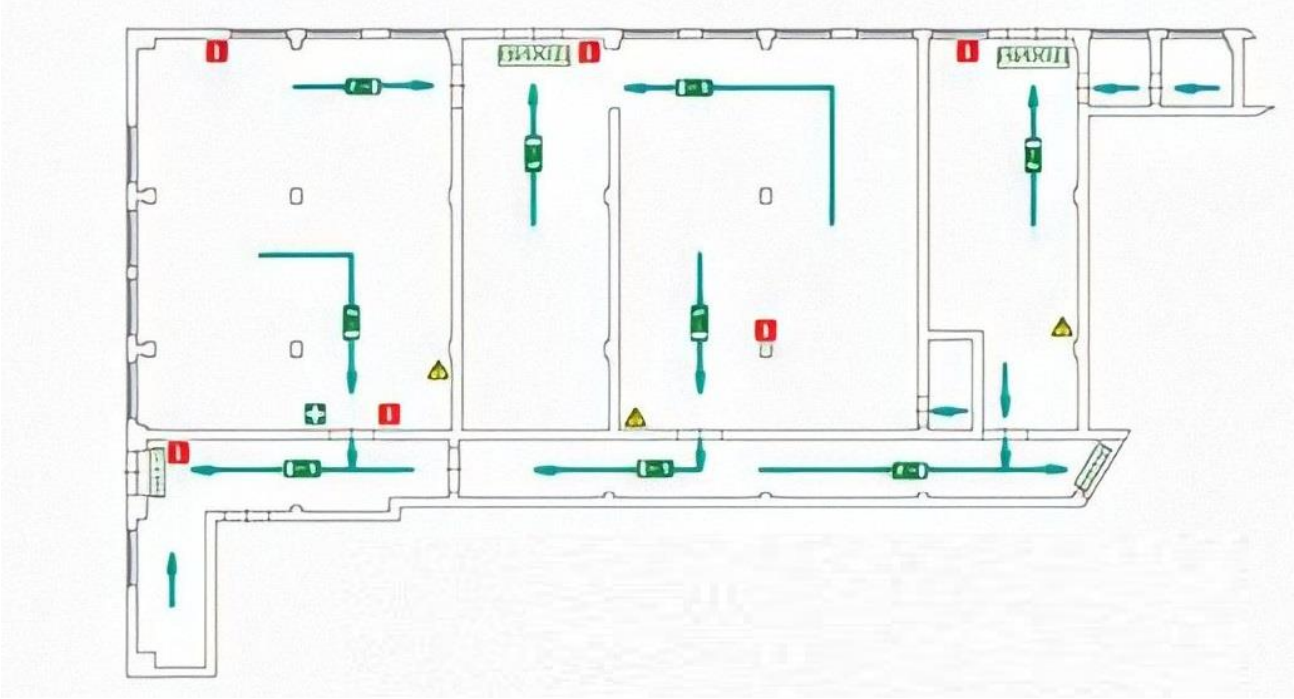


Рис. 26 План евакуації

Кабінети офісного центру розташовані в одноповерховій будівлі, загальна площа приміщень 180 м^2, висота стелі 3,2м.

Евакуація здійснюється у напрямку головного евакуаційного виходу, джерело пожежі знаходиться в дальньому кабінеті.

Площа загоряння: 6 м^2.

Щільність людського потоку на першій ділянці евакуаційного шляху:

$$D_1 = \frac{N_1 f}{l_1 \delta_1} = \frac{20 * 0{,}1}{25 * 4} = 0{,}02 \text{м}^{-2}$$

Час руху людського потоку по першій ділянці:

$$t_1 = \frac{l_1}{V_1} = \frac{25}{100} = 0{,}25 \text{хв.}$$

Інтенсивність руху людського потоку по першій ділянці:

q_1=0,1 м/хв.

Щільність людського потоку на другій ділянці евакуаційного шляху:

$$D_1 = \frac{N_1 f}{l_1 \delta_1} = \frac{15 * 0{,}07}{20 * 4} = 0{,}013 м^{-2}$$

Інтенсивність руху людського потоку по другій ділянці:

$$q_2 = \frac{2 q_1 \delta_1}{\delta_2} = \frac{2 * 0{,}1 * 4}{4} = 0{,}2 м/хв.$$

Час руху людського потоку по другій ділянці, так як $q_2 = 0{,}2 < q_{max} = 16{,}5$:

$$t_2 = \frac{l_2}{V_2} = \frac{20}{100} = 0{,}2 хв.$$

Розрахунковий час евакуації

$$t_р = t_1 + t_2 = 0{,}25 + 0{,}2 = 0{,}45 \text{ хв.}$$

Геометричні характеристики приміщення:

h = 1,7 м; V= 0,7 * 180 = 126,2 м^3

А — розмірний параметр, що враховує питому масову швидкість вигоряння горючого матеріалу і площу пожежі, кг/с^n:

$$A = \frac{0{,}67\psi_F}{\sqrt{\tau_{ст}}} = 0{,}67\frac{0{,}01\cdot 6}{\sqrt{1000}}420 = 0{,}267 \text{ ; при } n = 1{,}5.$$

Визначаємо $t_{кр}$ при $\alpha = 0{,}3$ і $E = 40$ лк, $B = \frac{353 C_p V}{(1-\varphi)\eta Q} = 311.3$ кг

$$Z = \frac{h}{H} * \exp\left(1{,}4 * \frac{h}{H}\right) = \frac{1{,}7}{3{,}2} * \exp\left(1{,}4 * \frac{1{,}7}{3{,}2}\right) = 0{,}28; \; l_{пр} = 20 \text{ м};$$

по підвищеній температурі:

$$t_{кр}^{т} = \left\{\frac{311.3}{0{,}267} * \ln\left[1 + \frac{70-20}{(273+20)*0{,}28}\right]\right\}^{1/1{,}5} = 58{,}2\text{с};$$

по втраті видимості:

$$t_{кр}^{вв} = \left\{\frac{311.3}{0{,}267} * \ln\left[\,1 - \frac{126{,}2 * \ln(1{,}05 * 0{,}2 * 40)}{20 * 311.3 * 243 * 0{,}28}\,\right]^{-1}\right\}^{1/1{,}5} = 63{,}4\text{с};$$

по зниженому вмісту кисню:

$$t_{кр}^{в} = \left\{\frac{311.3}{0{,}267} * \ln\left[\,1 - \frac{0.044}{(((B * 0.101)/126{,}2) + 0.27) * 0.28}\,\right]^{-1}\right\}^{1/1{,}5} = 61\text{с};$$

$$t_{кр} = \min\left\{t_{кр}^{вв}, t_{кр}^{в}, t_{кр}^{тг}\right\} = \min(58.2, 63.4, 61) = 58 \text{ с}.$$

Необхідний час евакуації людей з приміщення підприємства:

$t_{нб} = 0{,}8 t_{кр} = 0{,}8 * 58 = 46{,}4$ с $= 0{,}78$ хв.

Із порівняння $t_р$ з $t_{нб}$ отримуємо:

$$t_р = 0,45 < t_{нб} = 0,78.$$

$$P_{еш} = \begin{cases} \dfrac{\tau_{бл} - t_р}{\tau_{пе}}, & якщо\ t_р \langle \tau_{бл} \langle t_р + \tau_{пе} \\ 0,999, & якщо\ t_р + \tau_{пе} \le \tau_{бл} \\ 0, & якщо\ t_р \ge \tau_{бл} \end{cases}$$

де $\tau_{бл}$ — час від початку пожежі до блокування шляхів евакуації, хв.;

$t_р$ — розрахунковий час евакуації людей, хв.,;

$\tau_{пе}$ — інтервал часу від виникнення пожежі до початку евакуації людей, хв.

Імовірність евакуації по евакуаційним шляхам:

$$P_{е.ш} = \frac{\tau_{бл} - t_р}{\tau_{пе}} = 0,18.$$

Імовірність евакуації:

$P_е = 1 - (1 - (1 - P_{е.ш}) (1 - P_{п.з}) = 1 - (1 - (1 - 0,18) (1 - 0) = 0,82.$

Розрахунковий індивідуальний ризик:

$$Q_в = Q_п P_{пр} (1 - P_е) (1 - P_{п.з}) = 0,2 * 10^{-3}\ 1\ (1 - 0,82) (1 - 0) = 9,4 * 10^{-7};$$

$$Q_в = 9,4 * 10^{-7} < Q_в^н = 10^{-6}.$$

Оцінка соціального ризику на ділянці

$$Q_{10} = \begin{cases} 0, \text{ якщо } t_{\text{р}} \le \tau_{\text{бл}}; \\ 0, \text{ якщо } t_{\text{р}} \ge \tau_{\text{бл}} \text{ і } \text{М} < 10; \\ \dfrac{\text{М} - 9}{\text{М}}, \text{ якщо } t_{\text{р}} \ge \tau_{\text{бл}} \text{і } \text{М} \ge 10, \end{cases}$$

Так як $t_{\text{р}} < \tau_{\text{бл}}$ приймаємо $Q_{10} = 0$, тобто імовірність загибелі в наслідок пожежі 10 і більше людей на ділянці, що досліджується дорівнює 0.

ВИСНОВОК

В ході виконання дипломної роботи було проведено дослідження проблеми проведення моніторингу працівників. Проведено аналіз загальної характеристики підприємства та відділу технічної підтримки. Ознайомлено з функціями та завданнями відділу, загрозою втрати інформації.

Проведено аналіз програмних засобів систем моніторингу працівників. Створено порівняльну таблицю для кращого розуміння сильних та слабких сторін всіх програмних засобів.

В ході проведено аналіз методології створення програмних продуктів та обрання методології яка дозволяє швидко та якісно виконати поставлене завдання. Обрано середовище та мову для розробки програмного засобу, а також обрано базу даних, яка буде відповідати за зберігання та роботу з інформацією. Підраховано релевантність розробки нового програмного продукту та термін окупності.

Представлено інструкцію користувача для ознайомлення з можливостями роботи нового програмного продукту.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Документація відділу кадрів ПрАТ «Оболонь».

2. Мюллер Джон Поль, Семпф Билл (2019) C# для чайников 608с

3. Джеймс Р. Грофф. Пол Н. Вайнберг. Эндрю Дж. Оппел (2019) SQL: полное руководство. 3-е издание 90с

4. Євгенія Яковенко, Ігор Журавель, Іван Горбатий, Андрій Бондарєв (2019) Інформаційна безпека 580с

5. Аллен Дж. Тейлор (2020) SQL для чайников 544с

6. Эндрю Троелсен, Филипп Джепик (2019) Язык программирования C# 7 и платформы .NET и .NET Core, 8-е издание, том 1 672 с

7. Юлія Лісовська (2018) Інформаційна безпека України 172 с

8. Когут Ю.І.(2021) Корпоративна безпека 460 с

9. Ден кенеді (2019) Безжальний менеджмент. Управління людьми та прибутком

10. Климов Александр Петрович (2012) советы програмистам 544с

11. John Sharp(2005) Microsoft® Visual C#® 2005 Step by Step 429с

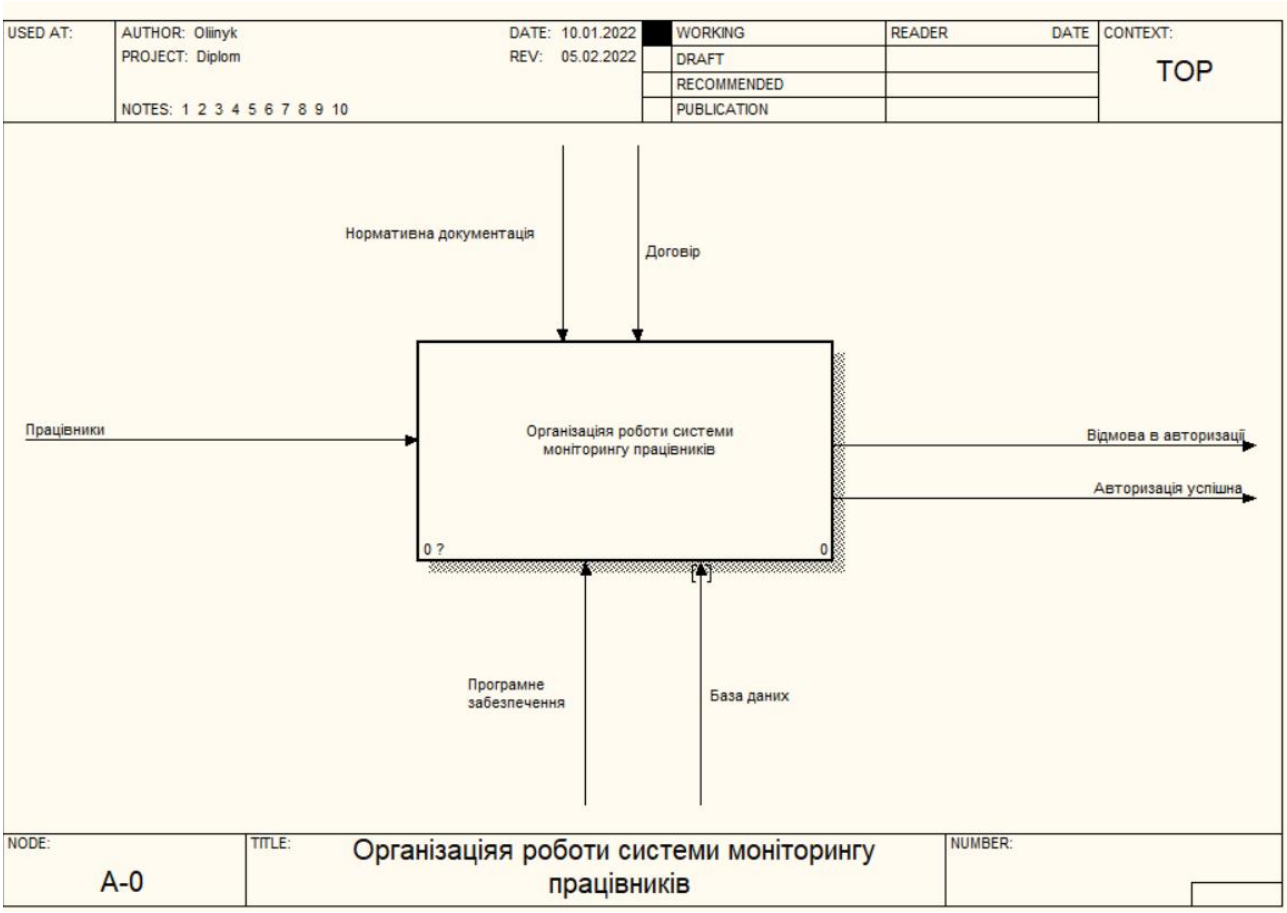
12. Брюс Джонсон (2015) Professional Visual Studio 2015 с 468

13. https://conf.ztu.edu.ua/wp-content/uploads/2017/09/234.pdf

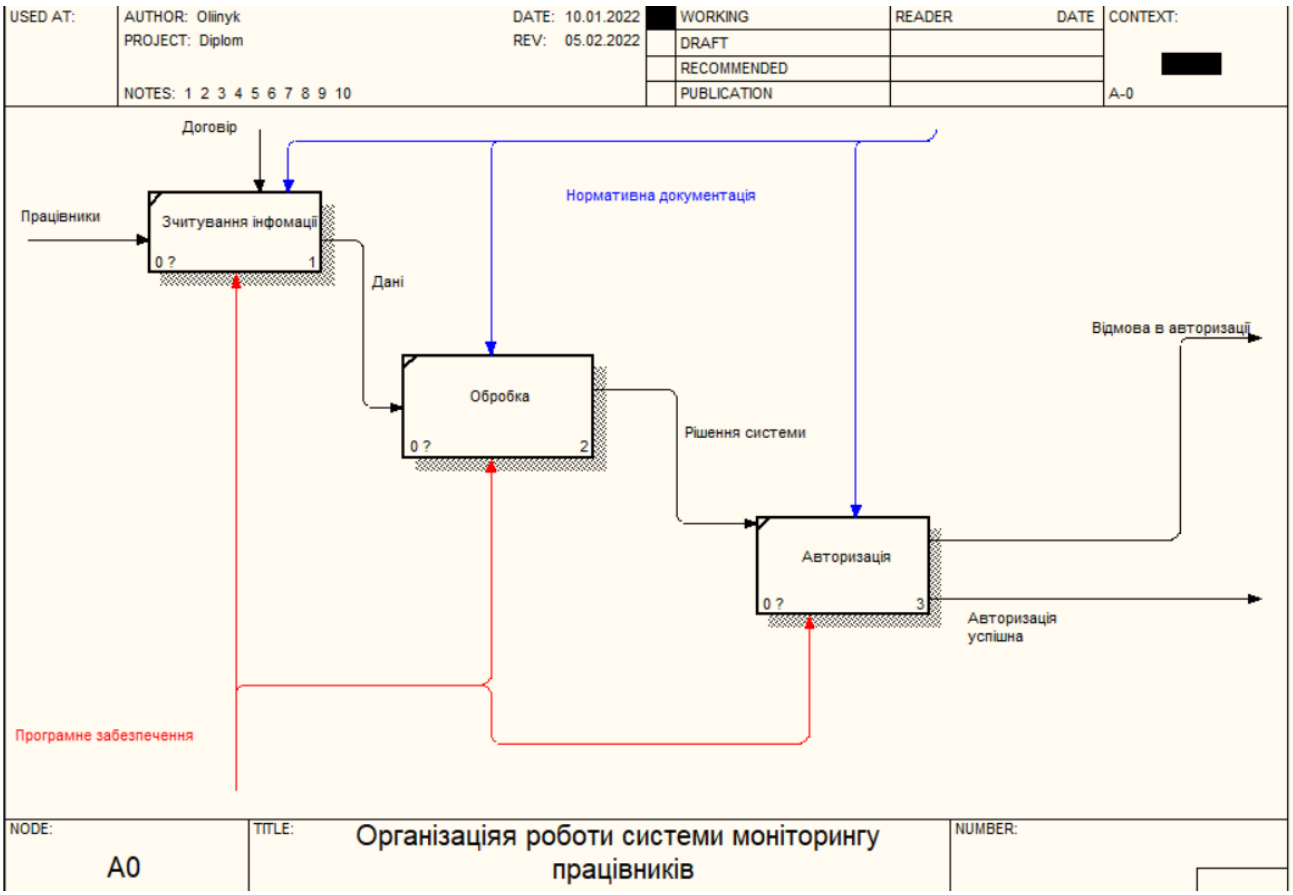
14. https://codernet.ru/books/c_plus/yazyk_programmirovaniya_c_lekcii_i_uprazhneniya/

15. Бен Форта(2012) SQL in 10 Minutes, Sams teach yourself 376 с

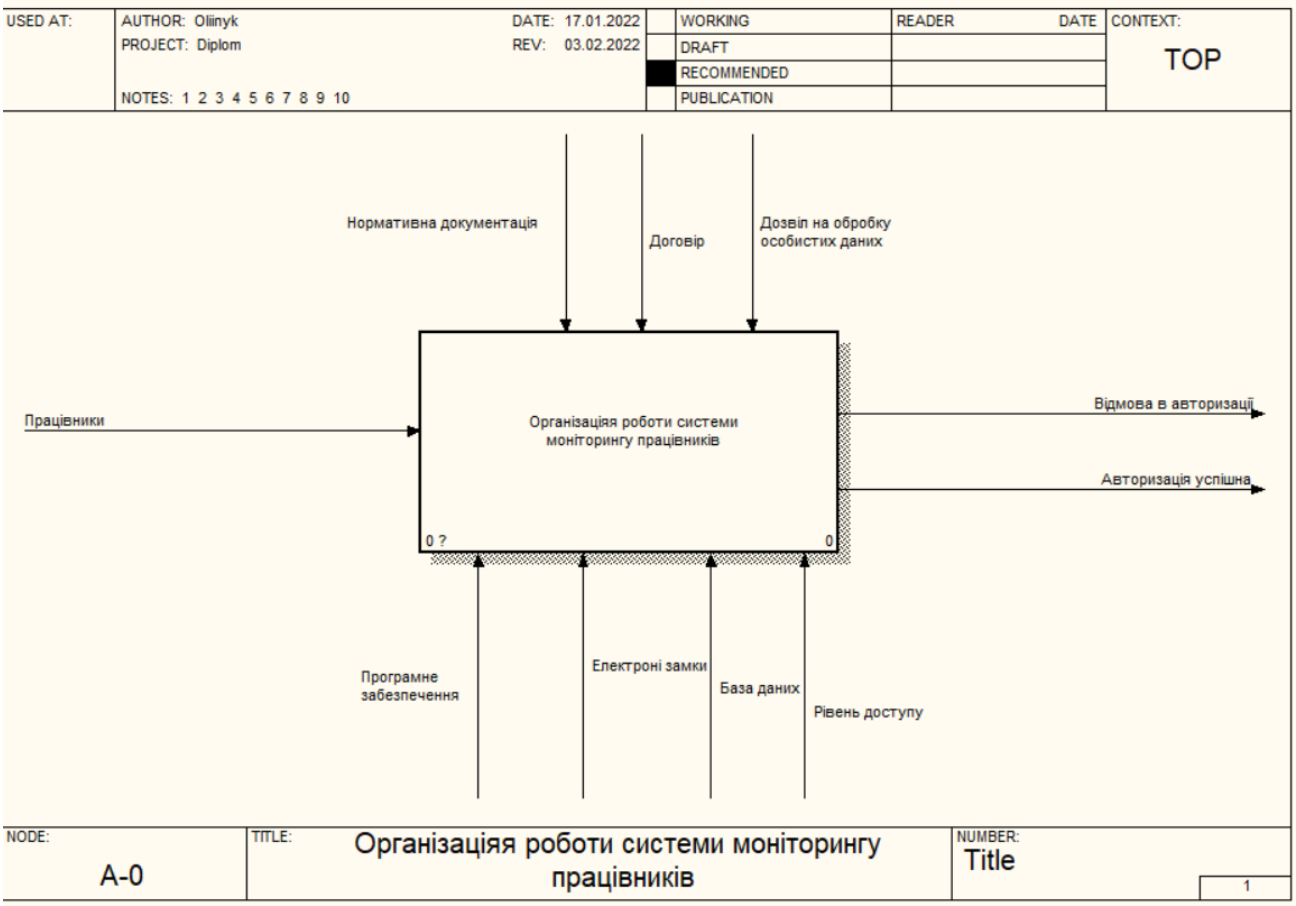
ДОДАТКИ



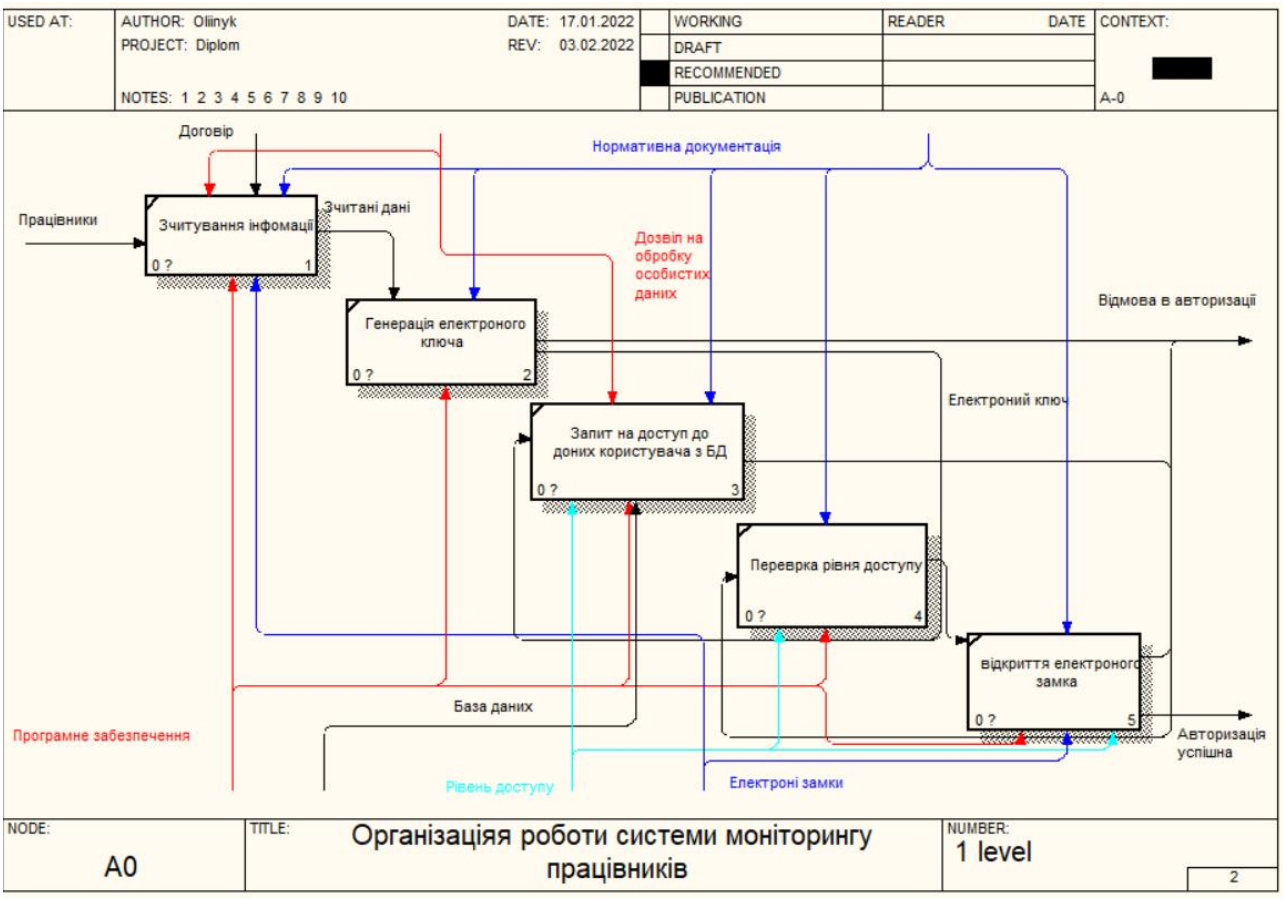
Додаток 1 Верхній рівень декомпозиції системи моніторингу персоналу



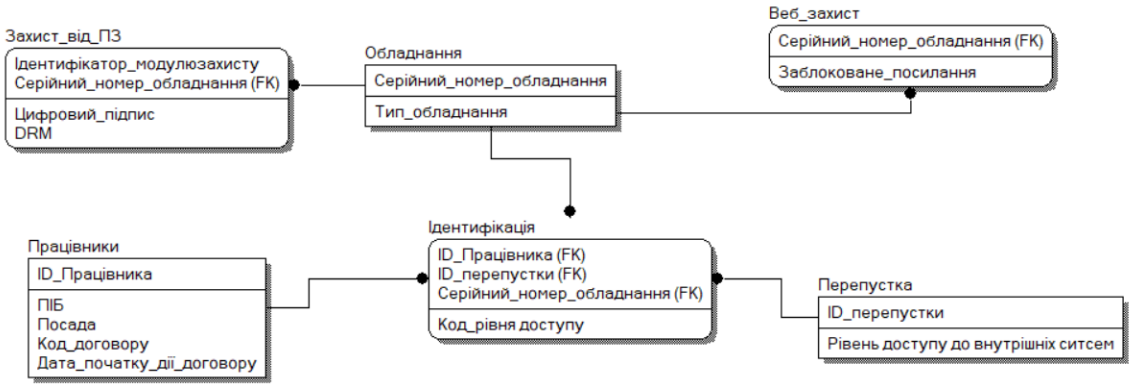
Додаток 2 декомпозиція 1 рівня як є



Додаток 3 Робота підсистеми для моніторингу працівників



Додаток 4 декомпозиція роботи підсистеми моніторингу працівників



Додаток 5 Схема бази даних в ERwin