АНОТАЦІЯ

Тема магістерської роботи «Система контролю і управління доступом».

Актуальність магістерської роботи полягає в необхідності дослідження питань управління доступом у різні приміщення шкільного закладу та забезпечення безпеки навчального процесу.

Об'єкт дослідження – робота системи контролю доступу в шкільному закладі, принципи регулювання доступу, роботи служби охорони та адміністрації школи, методи контролю відвідуваності школи учнями, інформування вчителів та батьків учнів, а також підвищення рівню безпеки для учнів та працівників школи.

Мета роботи – створення системи управління доступом, яка дозволить попередити несанкціонований доступ до шкільних приміщень небажаним особам, також дозволятиме зберігати и переглянути потім інформацію про інциденти, буде інтегрована з іншими системами безпеки та миттєвого сповіщення. Також система має бути захищеною від проникнень та зламу, оскільки деякі дані будуть передаватись через глобальну мережу Інтернет.

Під захистом слід розуміти налаштування захищеного від зламу сервера з модулем SSL та придбання надійного SSL-сертифікату від відомого центру сертифікацій, це дозволить не боятися комп’ютерних шахраїв і того, що персональні дані працівників та учнів будуть викрадені або знищені.

Під інтеграцією зі сторонніми модулями мається на увазі існуючі та встановлені напівавтоматичні системи пожежного попередження та пожежогасіння, систему відеоспостереження, сервіс допомоги батькам, вчителям та учням Смарсі.

Для реалізації поставленої мети були вирішені наступні питання: проведено дослідження та аналіз існуючого підходу до роботи служби безпеки та адміністрації шкільного закладу, на основі реалізації попереднього проектування та у період переддипломної практики були зроблені висновки, на базі яких було змодельовано та створено нову систему з урахуванням підказок та побажань персоналу, учнів та їх батьків. Також додана інтеграція з системами пожежного попередження та пожежегасіння, відеоспостереження і с проектом інформування Смарсі.

Також проведено обґрунтування вибору апаратних, програмних засобів та програмного середовища для розробки системи. Практична цінність

магістерської роботи полягає в тому, що розроблена система може бути використана для реального використання у шкільних та інших освітніх закладах, а також на деяких підприємствах, тому що дозволяє досить легко змінювати налаштування, додавати нові модулі або інтегруватись з іншими програмними продуктами.

Ключові слова: СКУД, СИСТЕМА КОНТРОЛЮ УПРАВЛІННЯМ ДОСТУПУ, КОНТРОЛЕР,ІДЕНТИФІКАТОР, ЗІИТУВАЧ, ШЛАГБАУМ, ТУРНІКЕТ, ІНТЕРФЕЙСНІ МОДУЛІ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

Магістерська робота містить 93 сторінки, 43 рисунки, 14 таблиць, 24 посилання.

SUMMARY

Theme of master's work is "Access Control and Management System".

The urgency of the master's work is the need to research the issues of access control in different premises of the school and ensure the safety of the educational process.

The object of the study is the operation of the access control system at the school, the principles of access regulation, the work of the school's security and administration, methods of controlling school attendance by students, informing teachers and parents of students, as well as improving the level of safety for students and school staff.

The purpose of the work is to create an access control system that will prevent unauthorized access to the school premises to unwanted persons, will also allow to store and then view incident information, will be integrated with other security and instant alert systems. The system should also be protected from intrusion and hacking, as some data will be transmitted over the global Internet.

Under security, you need to understand that a secure SSL server is configured and that you have a secure SSL certificate from a reputable certification authority, that you will not be afraid of computer scams and that the personal data of employees and students will be stolen or destroyed.

Integration with third-party modules means existing and installed semi-automatic fire-prevention and fire-extinguishing systems, a video surveillance system, a service for the parents, teachers and students of Smarsi.

To achieve this goal, the following issues were solved: research and analysis of the existing approach to the work of the security service and the administration of the school were conducted, based on the preliminary design and during the undergraduate practice, conclusions were drawn, on the basis of which a new system of taking into account the prompts and wishes of staff, students and their parents. Integration with fire-fighting and fire-extinguishing systems, video surveillance and with the Smarsi information project has also been added.

A justification of the choice of hardware, software and software environment for system development was also provided. The practical value of a master's thesis is that the developed system can be used for real use in school and other educational establishments, as well as in some enterprises, because it makes it quite easy to change settings, add new modules or integrate with other software products.

Keywords: SKUD, ACCESS CONTROL SYSTEM, CONTROLLER, ID, SENSOR, SWITCH, TOURNAMENT, INTERFACE MODULE, SOFTWARE.

The master's thesis contains 93 pages, 43 drawings, 14 tables, 24 references

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНТ ТА ТЕРМІНІВ

АРМ – автоматизоване робоче місце

БД – база даних

ІС – інформаційна система

КБД – корпоративна база даних

КУД – контроль і управління доступом

ПБД – персональна база даних

ПІН – персональний ідентифікаційний номер

СКД – системи контролю доступу

СКУД – система контролю і управління доступом

СРЧ – системи реального часу

СУБД – система управління базою даних

ADO – ActiveX Data Objects

API – Application Programming Interfaces

CASE – Computer Aided System Engineering

FK – foreign key (зовнішній ключ)

IDE – Integrated Development Environment, об'єднане середовище розробки

MFC – Microsoft Foundation Class library – базова бібліотека класів

PK – primary key (первинний ключ)

PL – presentation logic (презентаційна логіка)

SOA – Service Oriented Architecture

UML – Unified Modeling Language

WWW – World Wide Web

ВСТУП

Школа – це маленьке життя, яку свого часу проживає кожен дорослий. Це один з основних етапів нашого життя. Все в світі починається з малого, все народжується з малого, а потім виростає: маленький паросток стає великим деревом, струмочок вливається в річку, слова переростають в пропозиції і великі романи, з кількох нот складаються великі мелодії. Ось так і ми: починаємо пізнавати життя в школі. А потім, у дорослому житті, спираємося на свій розум і ті знання, які отримали в школі. Таким чином, загальна освіта просто необхідна.

Безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз.

Безпека школи, як і будь-якого іншого закладу освіти – це умови збереження життя і здоров'я учнів, вихованців і працівників, а також матеріальних цінностей освітнього закладу від можливих нещасних випадків, пожеж, аварій та інших надзвичайних ситуацій. Вона включає всі види безпеки, що містяться в Законі «Про технічне регулювання» і складається з багатьох напрямків, а також являє собою цілісну систему, частини якої працюють взаємопов'язано, забезпечуючи безпеку учнів і співробітників під час освітнього процесу.

Україна приєдналася до Декларації про безпеку шкіл (Safe Schools Declaration) і стала сотою країною, що підтримала положення цього документа. Відповідний лист з підтвердженням участі України підписала Міністр освіти і науки Ганна Новосад. Декларація містить низку зобов'язань для попередження і реагування на напади та використання закладів освіти у військових цілях у період збройного конфлікту.

За чотири роки з часу відкриття Декларації у багатьох країнах-підписантах відбулися зміни щодо політики держави стосовно освіти у час збройного конфлікту, і їхній досвід може бути цінним для України.

Важливим аспектом приєднання до Декларації є відновлення освітньої інфраструктури, забезпечення психологічної реабілітації учнів, батьків і вчителів, сприяння проведенню тренінгів з безпеки та охорони здоров'я тощо [1][1)].

Керівництво школи має своєчасно здійснювати комплексне забезпечення безпеки учнів. Адже на школі лежить відповідальність за захист і збереження здоров'я дітей. Саме тому в освітній організації повинна строго дотримуватися техніка безпеки, організовуватися тренування по евакуації з працівниками та учнями, забезпечуватися навчання заходам безпеки, проводитися профілактика нещасних випадків. У школі повинні розроблятися маршрути по евакуації, інструкції та брошури по боротьбі з тероризмом і екстремізмом, проводитися регулярні огляди території, огорож, спортивних майданчиків. В рамках захисту перед терористичною загрозою – проводити заходи щодо недопущення на територію школи сторонніх осіб, вести постійний облік відвідують її громадян [2][2)].

Одна зі складових безпеки в школі – це система контролю управлінням доступу (СКУД). Це сукупність технічних засобів і організаційних заходів, що дозволяють контролювати доступ до об'єктів СКУД і відстежують переміщення людей по території, що охороняється. В даний час, СКУД визнані одним з найбільш ефективних методів вирішення задач комплексної безпеки для об'єктів.

[1)] [1] МОН України: Україна приєдналась до Декларації про безпеку шкіл. URL: https://mon.gov.ua/ua/news/ukrayina-priyednalasya-do-deklaraciyi-pro-bezpeku-shkil-mi-stali-100-oyu-krayinoyu (дата звернення 22.11.2019).

[2)] [2] Довідник заступника директора школи. Безпека у школі. URL: https://www.menobr.ru/rubric/17-bezopasnost-v-shkole (дата звернення 13.08.2019).

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Склад системи контролю і управлінням доступу

Система контролю і управління доступом (СКУД) зазвичай складається з серверів СКУД (в залежності від навантаження та розгалуженості контрольованої мережі, в цій ролі може як старовинний ноутбук, так і найсучасніший, найпотужніший кластер серверів – і керують підключеними до них контролерами СКУД. Контролер (контрольна панель) – це спеціалізований високонадійний комп'ютер. У ньому зберігається інформація про конфігурацію, режими роботи системи, список людей, які мають право доступу до ресурсу, а також їх привілеї доступу до цього ресурсу. У простих випадках мінімальний варіант контролера може бути вбудований в зчитувач, турнікет, замок або інший виконавчий пристрій (рис. 1.1).

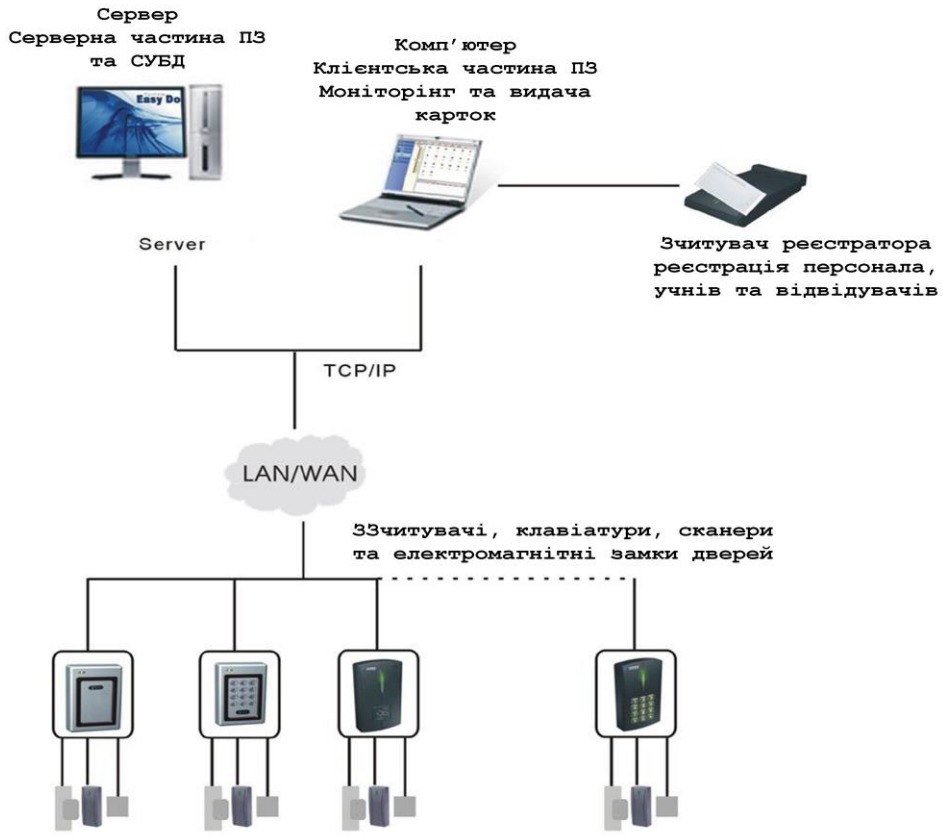

Рисунок 1.1 – Склад СКУД

Блокуючі пристрої (БлП) – це пристрої, що забезпечують фізичне перешкоджання доступу і обладнані виконавчими пристроями для управління їх станом (турнікети, прохідні кабіни, двері і ворота, обладнані виконавчими пристроями СКУД).

Зчитувальний пристрій, зчитувач – це пристрій, призначений для зчитування (введення) ідентифікаційних ознак. Цю інформацію він передає контролеру, який і приймає рішення про допуск людини до ресурсу. Можна налаштувати контролер так, що він буде запитувати підтвердження прийнятого рішення у комп'ютера. Для підвищення надійності ідентифікації крім зчитувачів до контролера може підключатися клавіатура для набору персонального ідентифікаційного номера (ПІН-коду).

Ще одним важливим поняттям СКУД є ідентифікатор користувача – унікальна ознака суб'єкта або об'єкта доступу. В якості ідентифікатора може використовуватися код, біометрична ознака, або речовинний код. Ідентифікатор, що використовує речовинний код – предмет, в який (на який) за допомогою спеціальної технології занесений ідентифікаційна ознака у вигляді кодової інформації (карти, електронні ключі, брелоки та ін. пристрої).

Інший тип пристроїв, які можна підключити до контролера – це охоронні панелі. Це також спеціалізований контролер, який відстежує стан охоронних датчиків (датчики на дверях, вікнах, об'ємні датчики та інші). Якщо стан будь-якого датчика змінюється, то інформація про це тут же надходить в основний контролер.

Виконавчі пристрої – це пристрої або механізми, що забезпечують приведення у відкритий або закритий стан БлП (електромеханічні, електромагнітні замки, електромагнітні засувки, механізми приводу шлюзів, воріт, турнікетів і інші подібні пристрої). В них може бути набір реле, за допомогою яких вони здійснюють управління виконавчими пристроями: електромехані-

чними замками, турнікетами, ліфтами, автоматичними воротами та іншими (рис. 1.2) [3][1)].

Рисунок 1.2 – Різноманітність засобів обмеження доступу

1.2 Головні можливості системи контролю та управління доступом

Можна перелічити нижче основні можливості, які надає установка СКУД на об'єкті, що охороняється.

Контроль і управління доступом – це основна функція системи, за її допомогою проводиться поділ прав доступу учнів, співробітників та візитерів в певні приміщення, а також відмова в доступі небажаним особам. Крім того, можливе дистанційне керування блокувальними пристроями (замки, турнікети і пр.). СКУД дозволяє заборонити прохід для співробітників у святкові та вихідні дні, а також після закінчення учбового або робочого часу.

[1)] [3] Система контролю і управління доступом – Вікіпедія. URL: https://uk.wikipedia.org/wiki/Система_контролю_управління_доступом (дата звернення 13.08.2019).

Збір і надання статистики. СКУД збирає інформацію про осіб, які пройшли через певні точки контролю доступу. По кожному співробітнику можливе отримання такої інформації: час входу та виходу, спроби доступу до заборонених для нього приміщення і зони, а також спроби проходу в недозволений час. Також можливо відстежити переміщення співробітника по території із зазначенням місця і часу. Таким чином, всі виявлені порушення трудової дисципліни можуть бути занесені до особової справи співробітника, а керівництво порушника повідомлено в робочому порядку. Крім того, виходячи з інформації, про останній точці проходу, СКУД дозволяє визначити місцезнаходження співробітника в будь-який момент часу.

Доступ у контрольовані зони тільки за особистим ідентифікатором. При проході за допомогою ідентифікаційної карти на екрані монітора в пункті охорони може відображатися вся інформація по співробітникові і його фотографія, що виключає можливість проходу за чужою карткою. Також на рівні правил реакції СКУД можна забезпечити захист від передачі ідентифікатора іншій особі і блокувати повторний вхід на територію об'єкта з тієї ж самої карті доступу [4][1)].

Облік робочого часу. За допомогою розробленої системи обліку робочого часу, реєструється час приходу до школи працівників та учнів і час їх виходу. В результаті надається можливість визначити сумарний час перебування співробітника або учня у школі, а на самому початку дня, наприклад, о 8:30 система обліку робочого часу, вбудована в СКУД, може формувати груповий звіт про учнів, які не пройшли через контрольну точку входу на територію. Це дозволяє в масовому порядку виявляти тих, хто запізнився або не з'явилися і може зняти навантаження про контроль з вчителів та класних керівників. Аналогічний звіт можна отримати і в кінці робочого дня на пункті виходу з території.

[1)] [4] ДСТУ 4000-2000 Системи тривожної сигналізації. Охоронні теле(відео) системи і системи контролювання доступу. [Чинний від 1.07.2001]. К.: Держстандарт України, 2000. 20 с.

Автономність роботи системи. СКУД оснащується системою безперебійного живлення, що дозволяє не переривати роботу в разі відключення електрики в будівлі. Також система контролю доступом завдяки функціоналу контролера має можливість продовжувати роботу, наприклад, при виході керуючого комп'ютера з ладу.

Охорона об'єкта в реальному часі. СКУД надає можливість ставити певні приміщення на охорону і знімати їх з охорони. Крім того, в реальному часі можна отримувати відомості про всілякі позаштатних і тривожних ситуаціях через спеціальні сповіщення відповідальних осіб. Крім цього в базі даних системи реєструються всі тривожні події і події, що дає можливість доступу до цієї інформації в подальшому при необхідності. Завдяки наявним у СКУД засобів, співробітник охорони зі свого робочого місця за допомогою комп'ютера має можливість не тільки керувати дверима і турнікетами, а й подавати сигнали тривоги. У комп'ютер СКУД у співробітника охорони можуть бути занесені поверхові плани будівлі зі схемою розташування контролерів обмеження доступу.

Віддалене управління системою через локальну мережу або мережу Інтернет або навіть з мобільного телефону. Якщо при установці підключити СКУД до мережі Інтернет, то у адміністрації школи, або керівника служби охорони, з'являється можливість вести віддалене управління і контроль за роботою системи, також можна цю інформацію надавати диспетчеру служби охорони. Також можна сказати і про можливість управління СКД зі свого мобільного телефону, правда це більше відноситься до GSM систем контролю доступу.

Інтеграція СКУД і СКД з іншими системами безпеки і охорони. Системи контролю і управління доступом можна поєднати і вбудувати з іншими системами безпеки, наприклад системою відеоспостереження, охоронною та пожежною сигналізацією. Контроль доступом разом з відеоспостереженням забезпечують майже повний контроль над охоронюваними приміщеннями. При виникненні позаштатної ситуації така система в найкоротші терміни до-

зволить виявити і заблокувати порушника. При інтеграції СКУД і охоронної сигналізації є можливість налаштувати спільну реакцію системи на несанкціоноване проникнення в те чи інше приміщення. Наприклад, можна включити сирену на пункті охорони, тривожну лампу або ж і зовсім заблокувати всі двері в необхідної частини будівлі. Інтеграція СКУД з системою пожежної сигналізації дозволяє автоматично розблокувати двері, турнікети і прохідні в разі пожежі, щоб не треба було бігати по задимлених коридорах та шукати когось, в кого є ключ від пожежного виходу. Всі ці заходи значно спрощують евакуацію персоналу в такий важкий період [5][1)].

1.3 Класифікація систем контролю і управлінням доступу

Системи контролю і управління доступом класифікують за:

а) способом управління системою контролю доступу:

1) автономні;
2) централізовані (мережеві);
3) універсальні;

б) кількістю контрольованих точок доступу:

1) малої місткості (менше 16 точок);
2) середньої ємності (не менше 16 і не більше 64 точок);
3) великої місткості (64 точки і більше);

в) функціональними характеристиками:

1) СКУД з обмеженими функціями;
2) СКУД з розширеними функціями;
3) багатофункціональні СКУД;

г) видом об'єктів контролю, які здійснюють:

1) контроль доступу фізичних об'єктів;
2) контроль доступу до інформації;

[1)] [5] Інтеграція СКУД з іншими системами. URL: https://smartsec.com.ua/uk/ integraciya-skud-z-inshimi-sistemamy/ (дата звернення 02.09.2019).

д) рівнем захищеності системи від несанкціонованого доступу до інформації:

1) нормального;
2) підвищеного;
3) високого [6][1)].

Узагальнена схема класифікації СКУД представлена на рис. 1.3.

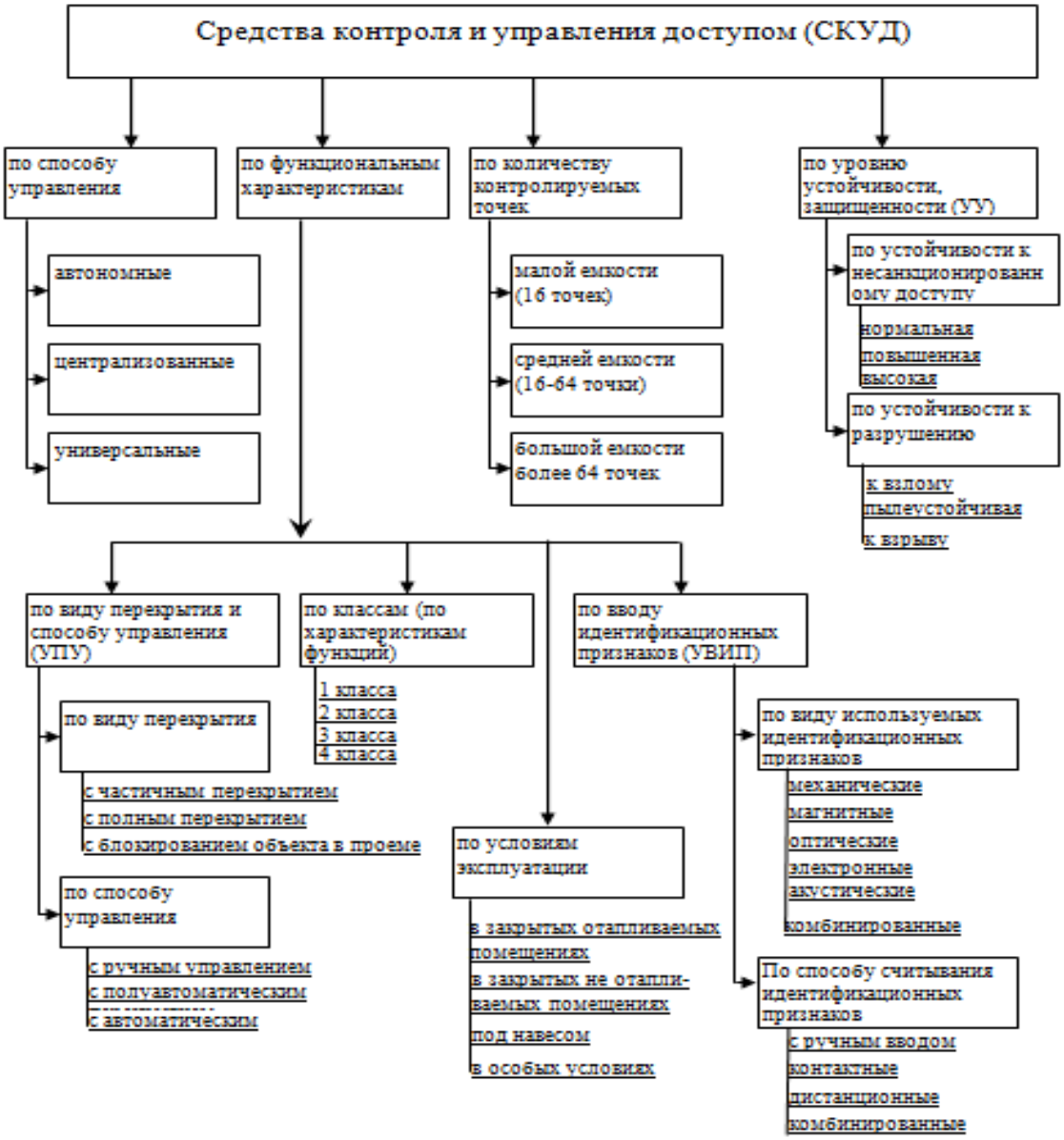

Рисунок 1.3 – Класифікація СКУД

[1)] [6] Про Системи управління доступом. URL: http://www.gamma.kz/gt/ sud.html (дата звернення 02.09.2019).

Автономні СКУД служать для управління однією або кількома точками доступу, без передачі інформації на центральний пульт і без контролю з боку оператора і без використання комп'ютера, що управляє. Зазвичай вони не мають зчитувача на «вихід» і для відкривання дверей зсередини приміщення використовується звичайна електрична кнопка виходу. Контролер автономної системи повинен мати функцію програмування – занесення кодів ідентифікаторів в пам'ять. Для цього в більшості моделей застосовується спрощений спосіб програмування на основі використання «майстер-ключа». «Майстер-ключ» це ідентифікатор, при зчитуванні якого контролер переходить в режим запису кодів ідентифікаторів в пам'ять. Усі наступні лічені ідентифікатори заносяться в пам'ять системи і стають чинними. Сучасні автономні СКУД мають можливість зберігати в пам'яті до декількох сотень кодів ідентифікаторів [7][1)].

Переваги автономних систем: їх невисока вартість, легкість програмування системи, відсутність великої кількості кабельних з'єднань, оперативність і порівняльна простота монтажу та зручність використання для невеликих об'єктів.

До недоліків можна віднести незручність процесу програмування в разі кількості дверей від трьох і більше, і користувачів більше ніж п'ятдесят, відсутність можливості оперативного впливу на процес проходу, обробки протоколу подій і отримання вибіркових звітів по заданих критеріях, великі труднощі адміністрування системи (наприклад, видалення / заміни в пам'яті системи загублених / скомпрометованих ключів), відсутність можливості інтеграції з охоронними системами та відеоспостереженням та багато інших.

Мережеві, або централізовані СКУД служать для управління великою кількістю точок доступу з обміном інформацією з центральним сервером і контролем та управлінням системою з боку оператора.

[1)] [7] Волковіцький В.Д., Волхонський В.В. Системи контролю і управління доступом. М.: Екополіс і культура, 2007. 164 с.

Це величезний клас СКУД, головна особливість яких в тому, що вони мають можливість конфігурації апаратури і управління процесом доступу з терміналів оператора або працівника служби охорони. Різні мережеві СКУД мають свої індивідуальні особливості і розрізняються за:

– архітектурою;

– можливостями;

– масштабом (граничної кількості зчитувачів / точок проходу);

– кількістю керуючих комп'ютерів;

– типом застосовуваних зчитувачів;

– степені стійкості до зламу і електромагнітних впливів.

Більшість мережевих СКУД зберігають всі достоїнства автономних систем, основне з яких – робота без використання керуючого комп'ютера. Це означає, що при вимкненні сервера або пошкодженні лінії зв'язку система фактично перетворюється в автономну. Контролери даних систем, так само як і автономні контролери, мають власний буфер пам'яті кодів карт користувачів і подій, що відбуваються в системі.

1.4 Способи ідентифікації

Існує два різних напрямки в способах ідентифікації. Це ідентифікація з використанням електронних карт, і ідентифікація, яка використовує біометричні параметри людини. Зараз застосовуються нижчеперелічені типи карт, кожному з яких відповідає певний тип зчитувача [8][1)].

Магнітні картки (рис. 1.4) – зчитуються, при проведенні в певному напрямку і з певною швидкістю по щілини зчитувача. Магнітна смуга із записаною на ній інформацією нанесена на одну зі сторін пластикової картки. Сучасні магнітні смуги виготовлені з матеріалів, що вимагають сильних маг-

[1)] [8] Картки-ідентифікатори, для систем контролю доступу. URL: http://www.avtolik.ru/access/ systems/identifikotor.htm (дата звернення 17.08.2019).

нітних полів для запису інформації і, відповідно, для її знищення, тому можна не боятися випадкового розмагнічування.

Рисунок 1.4 – Магнітна картка та зчитувач

Однак магнітні картки досить чутливі до зовнішніх впливів іншого роду – забруднення, вологи, подряпин. Ще один недолік пов'язаний з необхідністю точного позиціонування в зчитувач. Середній термін служби магнітних карт становить близько року, потім магнітний шар стирається. Тому магнітні картки застосовують, як правило, в системах, де передбачена часта заміна карт, наприклад, в готелях або на автостоянках.

Безконтактні радіочастотні (PROXIMITY) карти (рис. 1.5) – найбільш перспективний на сьогоднішній день тип карт. Безконтактні картки діють на відстані і не вимагають чіткого позиціонування, що забезпечує їх стійку роботу і зручність використання, високу пропускну здатність. Для зчитування інформації з безконтактної картки її досить просто піднести до зчитувача. Зчитувач генерує електромагнітне випромінювання певної частоти і, при внесенні карти в зону дії зчитувача, це випромінювання через вбудовану в карті антену живить чіп карти.

Рисунок 1.5 – Типи безконтактних карток

Отримавши необхідну енергію для роботи, карта пересилає на зчитувач свій ідентифікаційний номер за допомогою електромагнітного імпульсу певної форми і частоти. При цьому картка може перебувати в кишені або в гаманці.

Карти Віганда (рис. 1.6) – названі по імені вченого (Wiegand), який відкрив сплав, що володіє прямокутною петлею гістерезису. Усередині карти розміщені відрізки дроту з цього сплаву, які при переміщенні повз голівки, що зчитує дозволяють зчитати інформацію.

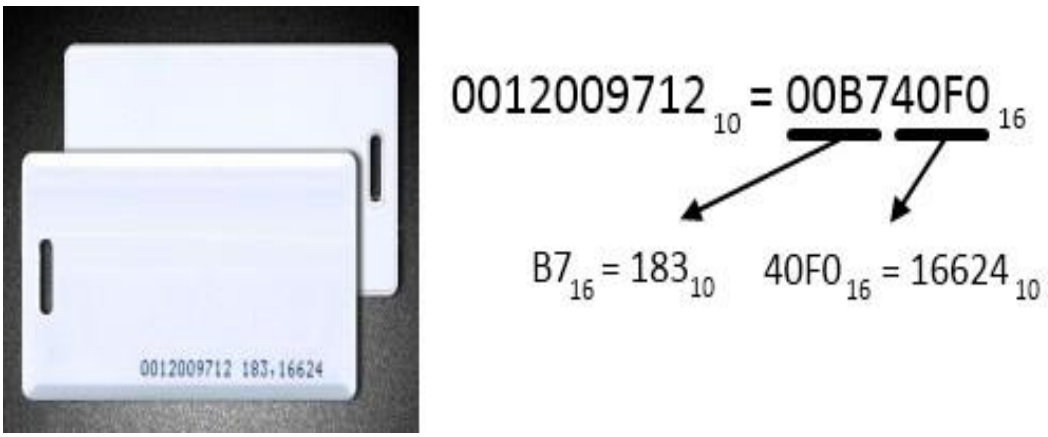

Рисунок 1.6 – Картка Віганда та розшифровка коду

Зазвичай на картці друкується 3 числа. Насправді, це одне і те ж число. Перше – 4-байтний код у десятирічному обчисленні. Друге і третє числа – два 2-байтних числа того ж самого коду.

Ці карти довговічніші, ніж магнітні, але і більш дорогі. Одним з недоліків є те, що код в карту занесений при виготовленні раз і назавжди.

Штрих-кодові карти (рис. 1.7) – на карту наноситься штриховий або його різновид – баркод (Bar code). Існує більш складний варіант, коли штрих-код закривається матеріалом, прозорим тільки в інфрачервоному світлі, зчитування відбувається в інфрачервоній області.

Рисунок 1.7 – Штрих-кодова картка

Розшифрування такого коду проводиться в двох вимірах (по горизонталі і по вертикалі). Двомірні коди поділяються на багаторівневі (stacked) і матричні (matrix). Багаторівневі штрих-коди з'явилися історично раніше, і являють собою поставлені один на одного кілька звичайних лінійних кодів. Матричні ж коди більш щільно упаковують інформаційні елементи по вертикалі.

Touch-memory (рис. 1.8) – металева таблетка, усередині якої розташований чіп ПЗП. При торканні таблетки зчитувача, з пам'яті таблетки в контролер пересилається унікальний код ідентифікатора. Досить дешеві і зручні.

Рисунок 1.8 – Touch-memory ключ

До біометричних способів ідентифікації (рис. 1.9) відносять кілька способів.

Рисунок 1.9 – Біометричні способи ідентифікації особи

Сканування відбитків пальців – є найзручнішим методом, а застосовувані при цьому пристрої – найдешевші. Перевагою є і надійність сканування відбитків пальців: несанкціонований доступ можливий приблизно в одному випадку з мільйона, а відмова в доступі уповноваженому користувачу вини-

кає приблизно в 3% випадків і пов'язаний в основному з неправильним доглядом за сканером або пошкодженням поверхні (наприклад, поріз або опік пальця). Майже половина сучасних смартфонів мають вбудовані сканери відбитків пальців, технологія вдосконалюється та стає більш дешевою.

У способі ідентифікації за геометрією долоні і кисті рук скануються не лінії, як у відбитків пальців, а геометрія руки: форма долоні або кисті, довжина пальців і т. д. В принципі, по надійності цей метод практично не поступається попередньому, але подібні системи займають набагато більше місця, що ускладнює їх використання на звичайному комп'ютері, та й коштують вони набагато дорожче.

Досить рідко поки що використовується сканування очей. При цьому розрізняють два типи: сканування райдужної оболонки і сканування сітківки ока. Перший метод більш простий і зручний, але і менш надійний. Другий є найнадійнішим, проте найдорожчим.

Вже зараз майже всі флагманські смартфони мають систему ідентифікації обличчя за допомогою інфрачервоних сканерів або фронтальних камер. Ця технологія теж все біль вдосконалюється та доволі надійна. Але поки що є певні недоліки, наприклад, якщо власник такого смартфону або ноутбуку буде дуже нетверезим, пристрій його не впізнає – дуже змінюється міміка.

Ідентифікація за голосом – перевагою метода є зручність використання. Але він має низьку надійність, так як для того, щоб голос людини значно змінився, достатньо застудитися.

Підпис – людина розписується на спеціальному пристрої типу графічного планшета. Комп'ютер порівнює отриману написану інформацію з тієї, яка зберігається в його базі, і в залежності від результатів порівняння надає доступ або відмовляє в ньому. Саму підпис легко підробити, але сучасні зчитувачі вимірюють ще і характеристики руху руки при листі, що підвищує надійність методу.

Геометрія особи, клавіатурний почерк – ці методи цього часу не дуже добре розроблені, реально діючих систем, наскільки відомо, на цей час не існує.

1.5 Принципи роботи систем контролю доступу

В основі роботи систем контролю і управління доступом закладений принцип порівняння тих чи інших ідентифікаційних ознак, що належать конкретній фізичній особі або об'єкту, з даними, закладеними в систему [9][1)].

Кожен із співробітників (вчителів, учнів, батьків, відвідувачів) отримує карту доступу або брелок, що містить індивідуальний код, який присвоюється при видачі карти доступу в бюро пропусків. В якості коду можуть використовуватися також біометричні дані людини. При проході на територію, що охороняється або в приміщення, що охороняється, проводиться зчитування даних з носія коду через зчитувачі, встановлені біля дверей. Інформація про відвідувача передається в систему, де проводиться аналіз та дається сигнал, адекватно реагує на ситуацію, що склалася: «Прохід дозволено»,« Прохід заборонено», «Повторний прохід по одній карті», виведення сигналу «Тривога» на пульт охоронця при порушенні охоронюваної території без відповідних прав і т.і.

При необхідності втручання охорони в ситуацію, що склалася на екрані комп'ютера поста охорони виводиться тривожний сигнал і інструкція, яка визначає дії персоналу в даній ситуації. Причому, система тут же може відреагувати на тривожну ситуацію, заблокувавши замки в приміщення, що охороняється і шляхи проходу за точками доступу.

Для аналізу подій, що відбулися є можливість перегляду і роздруківки протоколу подій за певний період часу. Для виключення зловживань в вико-

---

[1)] [9] Давлетханов М. Увага, чужий, 2003. URL: http://daily.sec.ru/dailypblshow.cfm?rid=5&pid=6637&pos=1&stp=50 (дата звернення 09.09.2019).

ристанні карт і посилення прохідного режиму в особливо важливі зони є ряд функцій, що дозволяють:

– виключити подвійний прохід в зону по одній карті (розрізняють можливості блокування повторного проходу на певний час – для систем, які не є обладнані зчитувачами на виході і заборона на вхід в несуміжні зони для повних систем контролю доступу);

– дозволити доступ тільки по 2-м картками (увійти можуть тільки двоє людей, зустрівшись разом і що володіють відповідними повноваженнями);

– обмежити кількість осіб в приміщенні і зоні (при перевищенні встановленого порогового значення контролер не пропустить в зону чергового людини);

– встановити режим «вхід під примусом» (непомітно для оточуючих охороні подається сигнал тривоги);

– охоронцеві дається право на самостійне прийняття рішення про дозвіл на прохід відвідувача (при зчитуванні карти на монітор охоронця виводиться фотографія власника, яка звіряє з зображенням, що видаються відеокамерою);

– встановити режим лічильника на використання карти (кількість читань карти на конкретному зчитувачі обмежується);

– встановити прихований контроль в приміщенні (подати сигнал тривоги на пульт охорони при проникненні в приміщення, що підлягає і відсутності відповідних прав, причому для зловмисника факт виявлення залишається невідомим).

1.6 Постановка завдання

Метою розробки даної дипломної роботи є створення інформаційної системи обліку контролю доступу для шкільного закладу. Ця система повинна поєднувати в собі комплекс заходів, здійснюваних керівництвом навчального закладу самостійно або спільно із запрошеними співробітниками охо-

ронних структур, пов'язаних з організацією доступу на об'єкт, що охороняється, пересуванням фізичних осіб, транспортних засобів на об'єкті, що охороняється, в нашому випадку школі.

Основне завдання – управління доступом на задану територію (кого пускати, в який час і на яку територію), включаючи також:

– обмеження доступу на задану територію;
– ідентифікацію особи, яка має доступ на задану територію;
– поєднання з системами пожежної тривоги та відеоспостереження;
– ведення журналу подій – входу-виходу, успішна або неуспішна, несанкціонована, тривога;
– збереження журналу подій при відмові або зникненні електричного живлення;
– ручне або напівавтоматичне сповіщення людей та відкриття блокуючих пристроїв для швидкої евакуації.

Крім того, слід врахувати ще деякі вимоги:

– зчитувач повинен бути відділений від контролера, щоб ланцюги, по яких проводиться відкриття замку, були недоступні;
– переважно використовувати обладнання в антивандальному виконанні з урахуванням кліматичних вимог;
– система повинна мати мінімальну кількість обладнання;
– система повинна легко масштабуватись;
– система повинна легко інтегруватися з іншими системами;
– система повинна мати резервне джерело живлення на випадок зникнення електричної мережі або умисного її відключення.

Вимоги до методу ідентифікації:

– низька вартість радіочастотного зчитувача;
– звичність і зрозумілість самої процедури і правил ідентифікації для персоналу, учнів та відвідувачів.

Установка СКУД дозволить забезпечити більш високий рівень безпеки у школі. Системи контролю і управління доступом (СКУД, СКД) є ефектив-

ним рішенням для обмеження доступу в приміщення небажаних осіб, зручного і легкого надання фізичного доступу і адміністративного моніторингу подій проходів дозволеними особами.

2 МОДЕЛЮВАННЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

2.1 Характеристика об’єкту автоматизації

Двоповерхова будівля Первомайської загальноосвітньої школи I-III ступенів №5 у м. Первомайськ Миколаївської області (рис. 2.1).

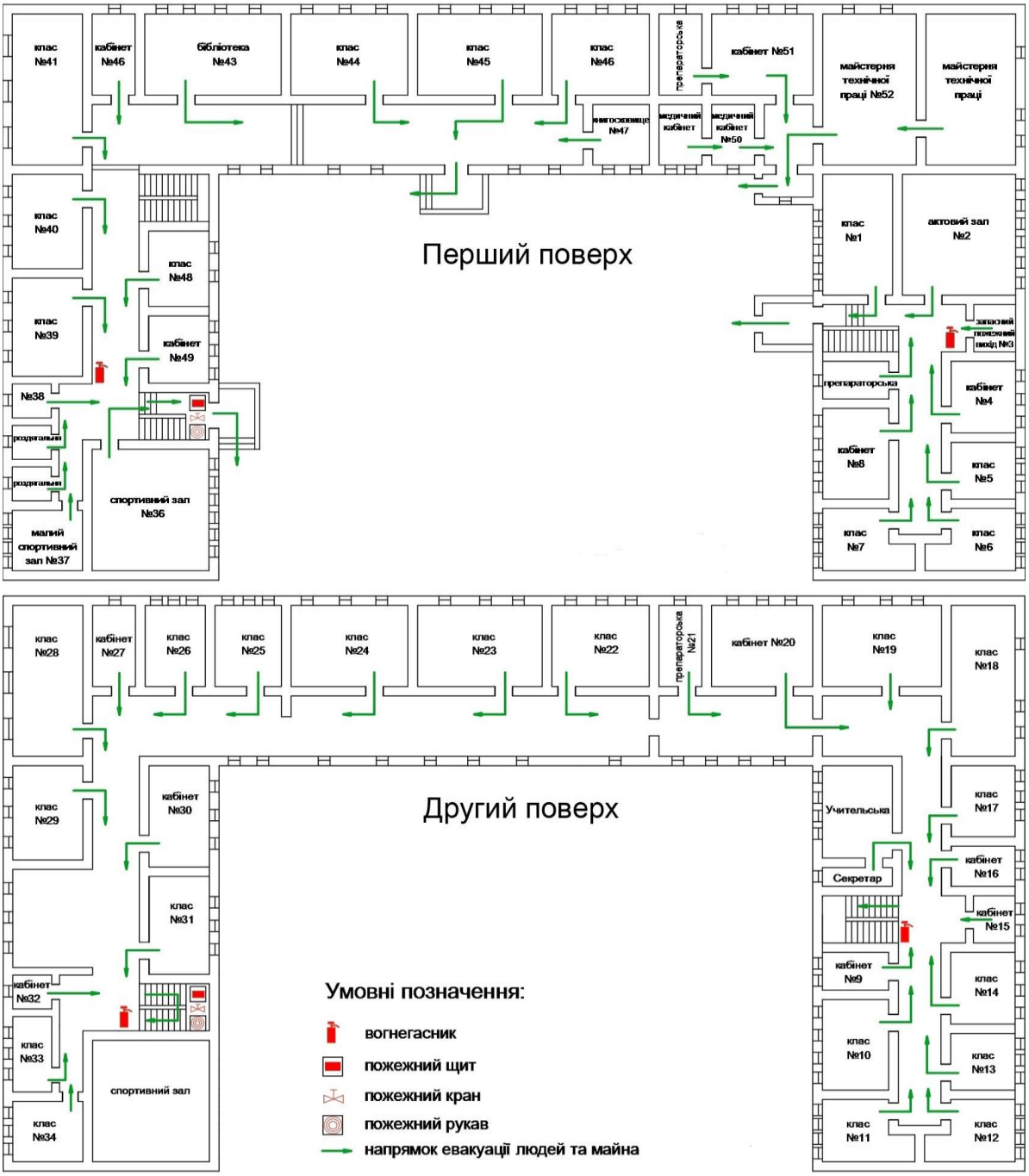

Рисунок 2.1 – План школи зі схемою евакуації

На даний момент пропускна система реалізована частково за розробкою мого диплома бакалавра – низка автономних контролерів без додаткового живлення, сервер на базі операційної системи Linux Centos 7.0, контролери зчитувачів та електромеханічних замків Z-5R NET, безконтактні зчитувачі RFID-карток (браслетів, брелоків) Iron Logic Matrix-II, електромагнітні замки МЕТАКОМ ML -250 для блокування дверей та безконтактний USB зчитувач-програматор RFID-карток Z-2 USB EM & HID PROX II & Mifare для програмування RFID-карток, під'єднаний до робочого комп'ютера завідувача з учбової частини, який виконує обов'язки адміністратора системи, а також турнікети Oxgard Praktika T-01.

Поточна архітектура виглядає таким чином (рис. 2.2):

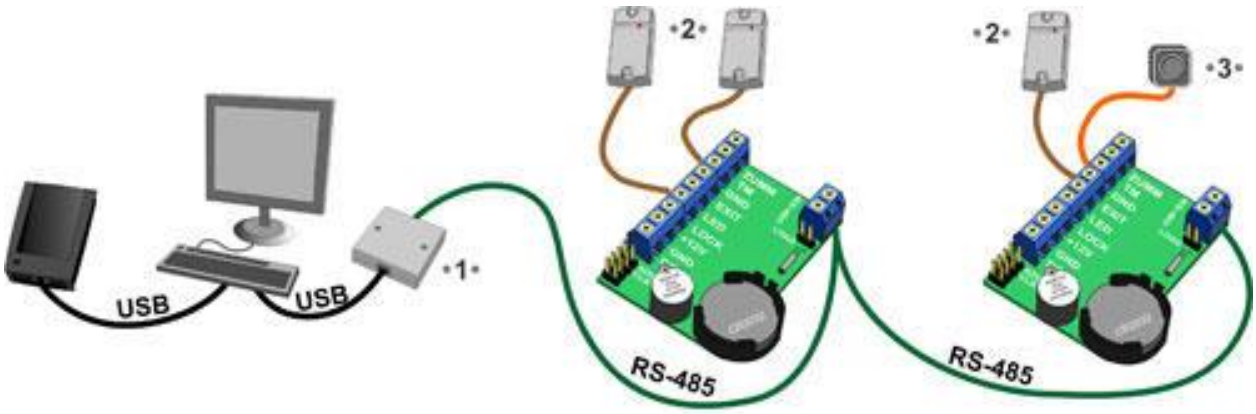

Рисунок 2.2 – Апаратна архітектура побудови СКУД

Вибір апаратного забезпечення було зроблено на основі швидкого аналізу існуючих систем організації безпеки, можливості спільної роботи апаратних засобів та доступних цін. Майже всі елементи масово виробляються в Китайській Народній Республіці на великих заводах під пильним наглядом інженерів та контролерів якості, чому набули великої популярності та витримали випробування часом.

На жаль, недостатнє фінансування не дозволило повністю реалізувати систему, але згодом це змінюється.

Кожному учню, співробітнику або відвідувачу видається ідентифікатор (електронний ключ) – пластикову картку, яка містить в собі індивідуальний код. Ці «електронні ключі» видаються в результаті реєстрації перелічених осіб за допомогою засобів системи. Фото при наявності і відомості про власника «електронного ключа» заносяться в персональну «електронну картку». Персональна «електронна картка» власника і код його «електронного ключа» зв'язуються один з одним і заносяться в спеціально організовану комп'ютерну базу даних. Зараз зчитувач встановлено на турнікеті біля вхідної двері. Вони зчитують з карток їх код та інформацію про права доступу власника карти і передають цю інформацію в контролер системи.

У системі кожному коду поставлена у відповідність інформація про права власника картки. На основі зіставлення цієї інформації та ситуації, при якій була пред'явлена картка, система приймає рішення: контролер відкриває або блокує турнікет.

Всі факти пред'явлення карток і пов'язані з ними дії (проходи, тривоги і т.д.) будуть фіксуватися в контролері і зберігатися в комп'ютері. Інформація про події, викликаних пред'явленням карток, може бути використана в подальшому для отримання звітів по обліку робочого часу, порушень дисципліни та ін.

2.2 Огляд існуючих систем

Ринок СКУД в Україні на даний момент досить великий і дуже різноманітний, і при цьому постійно розширюється: на ньому представлені як вітчизняні, так і зарубіжні виробники. Причому, це як раз той випадок, коли не соромно за вітчизняних виробників: їхня продукція, на думку фахівців, як мінімум не поступається, а за багатьма параметрами навіть перевершує іноземну. Але, на жаль, відрізняється більшою вартістю та меншим асортиментом. У кожного виробника свій напрямок діяльності по функціоналу обладнання та програмного забезпечення. Хтось пропонує великі, складні системи,

що підтримують інтеграцію з пожежними системами, системами відеоспостереження, і т.д., а хтось має спрямованість на невеликі будівлі і приміщення з невеликим числом «карткотримачів».

В кінці 2018р. було проведене телефонне опитування організацій, що займаються продажами і установками систем безпеки, перш за все систем контролю і управління доступом в Україні. У дослідженні взяли участь представники майже 300 компаній, що працюють на ринку технічних систем безпеки. В якості опитуваних виступили фахівці цих організацій – керівники підприємств, інженери, менеджери, які беруть безпосередню участь у продажу систем контролю доступу [11][1)].

У процесі дослідження респондентам пропонувалося відповісти, СКУД яких марок їм відомі. При відповіді на дане питання більшість респондентів (70%) в якості відомої їм торгової марки СКУД назвали Parsec, потім були названі Legos (62%), Perco (60%), Болід (56%). Інших виробників можна спостерігати на рисунку 2.3.

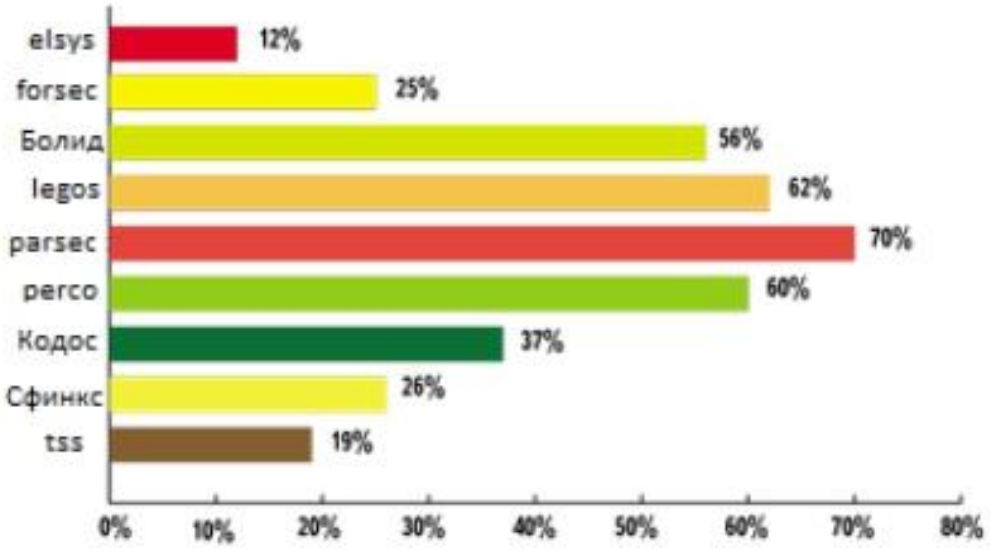

Рисунок 2.3 – Популярність СКУД в Україні

[1)] [11] Ринок СКУД. URL: http://sio.su/ (дата звернення 12.09.2019).

Всі перелічені СКУД задовольняють вимогам по забезпеченню безпеки для багатьох підприємств, вони є універсальними і багатофункціональними. Зупинимося на них детальніше:

СКУД від ЗАТ Компанія «Легос». Компанія створена фахівцями-розробниками електронних систем і компонентів в 2007 році. Основний бізнес компанії – виробництво і продаж керуючого обладнання та програмного забезпечення для систем автоматизації, контролю та безпеки будівель і споруд. СКУД Legos за способом управління відноситься до типу універсальних і включає в себе функції як автономних, так і мережевих систем, що працюють з центральним пристроєм управління (комп'ютер) під контролем оператора та перехідних в автономний режим при виникненні відмов у мережевому обладнанні, в центральному пристрої або обриві зв'язку.

Можливості СКУД Legos:

- автоматичний контроль доступу (кількість точок проходу не обмежена);
- захист від доступу сторонніх осіб і небажаних відвідувачів;
- розгалуження доступу персоналу на об'єкти за часом і статусом;
- автоматизація оформлення та обліку перепусток, тимчасових карт;
- облік робочого часу;
- взаємодія з системами пожежегасіння і офісної автоматикою;
- інтеграція з системами відеоспостереження (Інспектор, Інтелект , Phobos, Трал, Dallmeier);
- автономне функціонування будь-якої точки проходу при відключенні комп'ютера, харчування;
- глобальна інтеграція на програмному рівні в інформаційну структуру підприємства імпорт / експорт даних в бухгалтерські та ERP-системи, системи інформаційної безпеки і т.д. [12][1)].

[1)] [12] Офіційний сайт Legos. URL: http://legos.ru/ (дата звернення 24.08.2019).

Науково-впроваджувальне підприємство "Болід" працює на ринку систем безпеки з 1991 року. Головний офіс компанії знаходиться в Московській області, місті Королеві. Основні напрямки діяльності – розробка і виробництво технічних засобів охорони, контролю доступу, відеоспостереження, систем автоматизації.

Програмне забезпечення (ПЗ) Legos призначене для налаштування, управління та моніторингу систем безпеки, автоматики і життєзабезпечення будівель, контролю персоналу. Інтерфейс ПО віконний і показаний на рисунку 2.4:

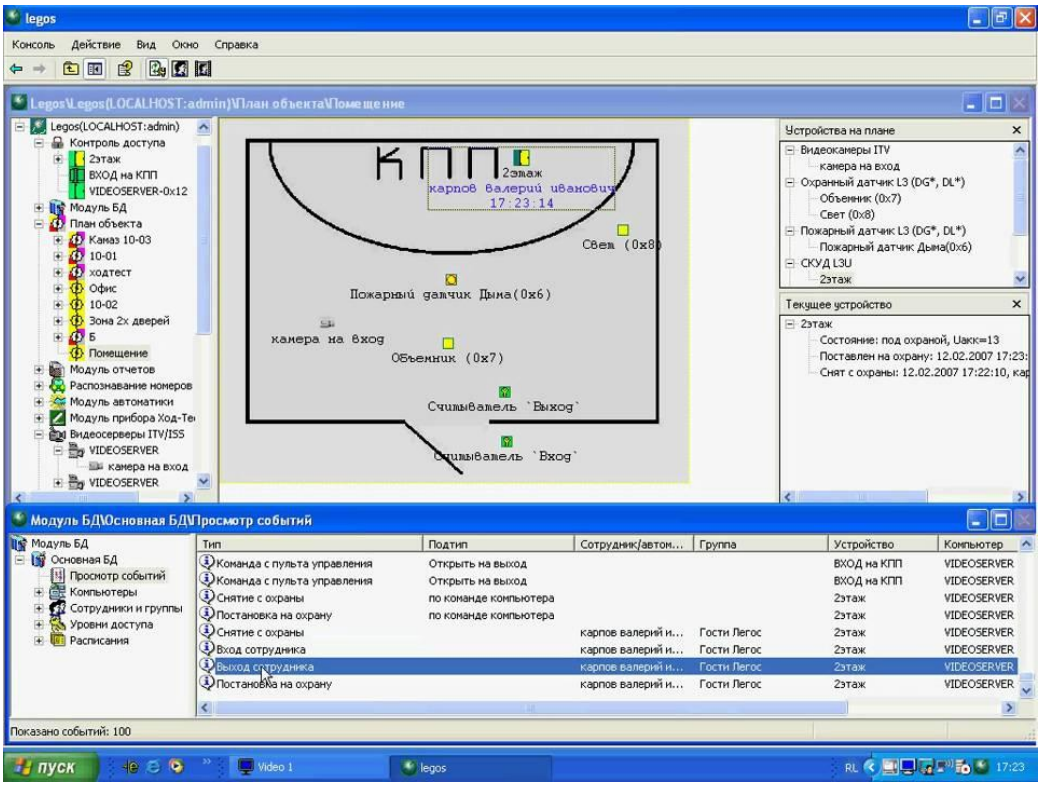

Рисунок 2.4 – Вікно ПЗ СКУД Легос

Дане ПЗ ліцензується за числом користувачів. Ліцензія «Класік» містить до 500 карток, ліцензія «Люкс» – до 3000. Але коштує цей комплекс досить дорого, крім того – прив’язаний до одного сімейства операційних систем.

СКУД Parsec призначена для забезпечення контролю доступу на самих різних об'єктах – від невеликого підприємства до цілого комплексу будівель. Крім цього система підтримує функції охоронної або охоронно-пожежної сигналізації. Parsec (ПС) – один з найвідоміших брендів в СНД в області систем контролю і управління доступом, який отримав високу оцінку як на вітчизняному ринку, так і за його межами. Виробництво обладнання та супутнього програмного забезпечення під торговою маркою Parsec почалося в 1997 році. За роки розвитку компанії система контролю доступу Parsec виконала нелегкий шлях, від найпростіших автономної системи, до складної, високотехнологічної мережевий [13][1)]. ПЗ також має віконний інтерфейс, програма встановлюється на комп’ютер оператора (рис. 2.5).

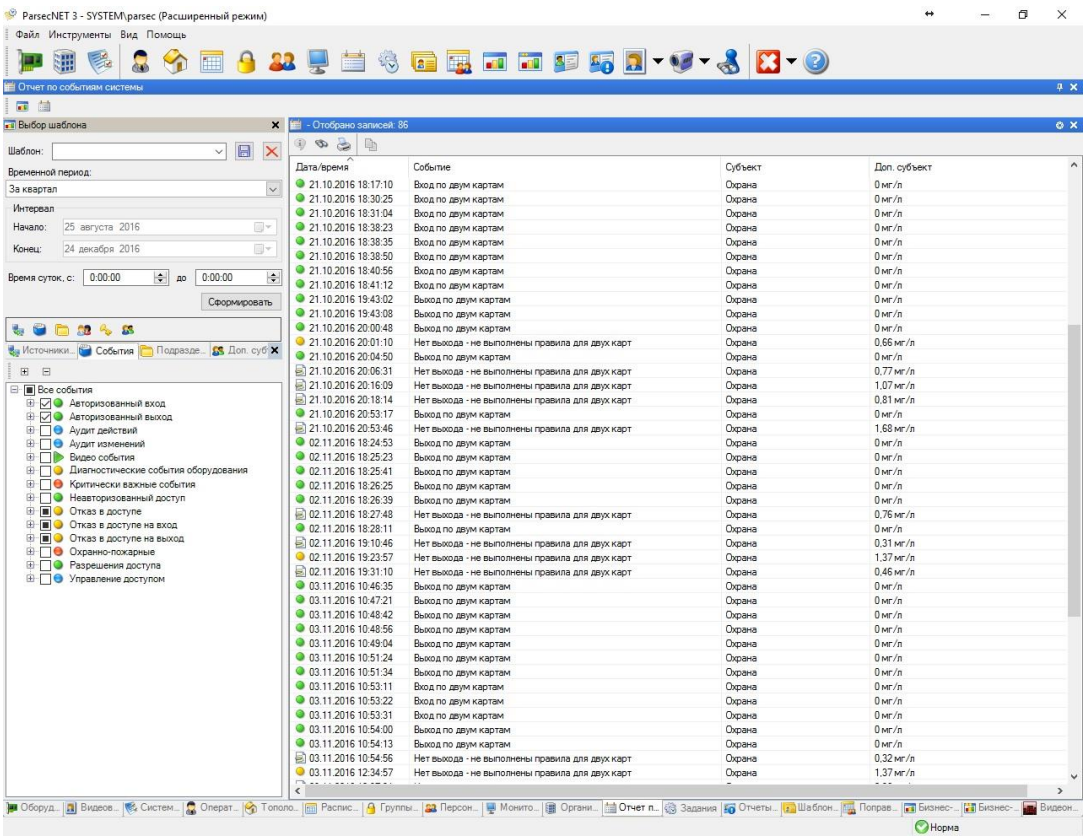

Рисунок 2.5 – Інтерфейс ПЗ СКУД Парсек

[1)] [13] Офіційний сайт Parsec. URL: http://www.parsec.ru/ (дата звернення 24.08.2019).

Інтерфейс може бути повнофункціональним, або на ПК може працювати тільки нотифікаційна консоль, яка повідомляє користувача про обрані події. При цьому всі служби системи, що забезпечують інформаційний обмін і використання цього обладнання, не залежать від призначеного для користувача інтерфейсу. Програмне забезпечення поставляється в одній з трьох конфігурацій:

– полегшена (light) версія системи має простий інтерфейс і мінімальні можливості для організації системи доступу в невеликому офісі;

– стандартна (standard) версія дозволяє будувати системи середнього масштабу, до неї можна замовляти різні конфігурації для отримання оптимального за ціною рішення;

– професійна (professional) версія дозволяє створювати складні багатотериторійні комплекси з організацією віртуальних підсистем. У ній вже включені практично всі додаткові модулі, які в стандартній версії ліцензуються окремо.

Третій лідер у списку СКУД – PERCo представляє собою широкий асортимент рішень – від локальних (на одні двері) до мережевих систем, розрахованих на велику кількість приміщень і прохідних з множинними точками проходу. Вибір конкретної СКД залежить від завдань, які стоять перед підприємством або установою. Програмне забезпечення PERCo-S-20 здійснює настройку і управління обладнанням, моніторинг його параметрів, систематизацію та архівування всієї інформації системи. Воно також здійснює підтримку обміну даними між контролерами і комп'ютером моніторингу, управління доступом і моніторинг пунктів проходу, роботу з базами даних і реєстрацію власників ідентифікаторів, дозволяють здійснювати візуальну ідентифікацію власників «електронних перепусток» на прохідній і для формування різних звітів [14][1)].

Інтерфейс знову віконний і представлений на рисунку 2.6.

[1)] [14] Официальный сайт PERCo. URL: http://www.perco.ru/ (дата звернення 26.08.2019).

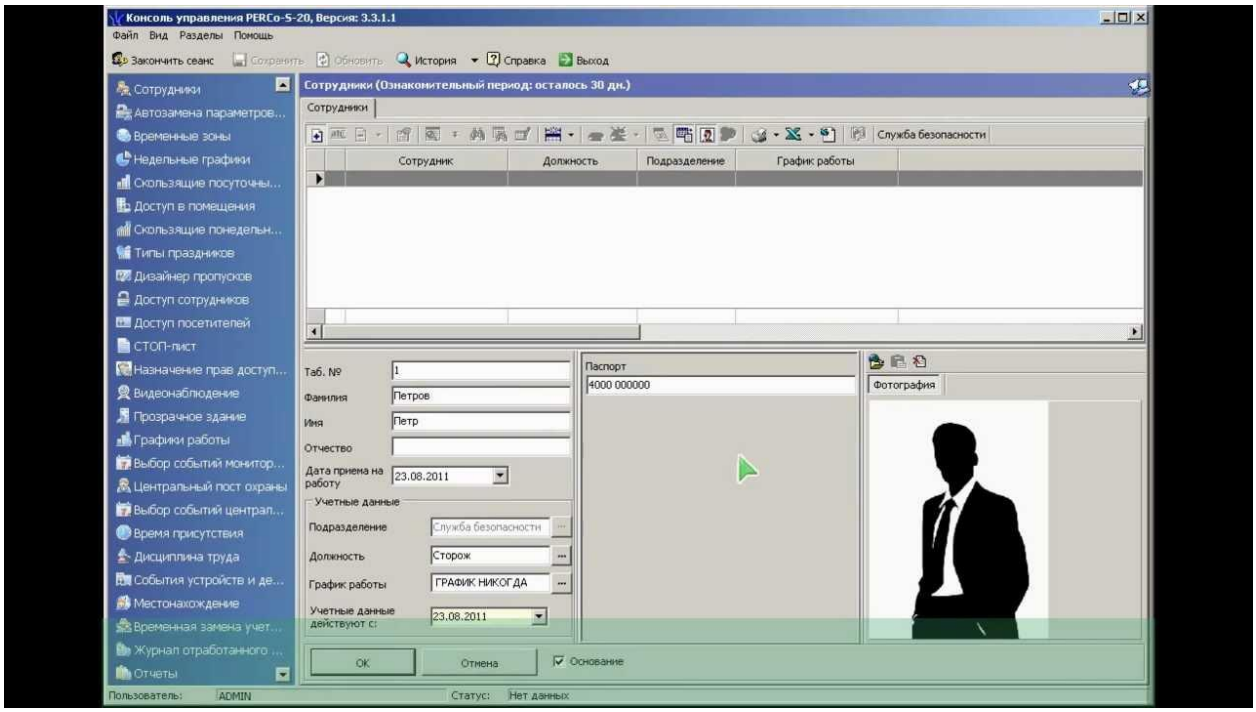

Рисунок 2.6 – Інтерфейс ПЗ СКУД PERCO

Нажаль, ПЗ має ті ж самі недоліки. Коли йдеться про вибір оптимальної системи контролю та управління доступом, необхідно брати до уваги, наскільки серйозні вимоги до безпеки пред'являються до об'єкта, де ви хочете помістити СКУД.

При виборі системи контролю та управління доступом слід враховувати не тільки ціну СКУД, а й надійність, безпеку, гнучкість, можливість індивідуальної доопрацювання як обладнання, так і програмного забезпечення і його подальшу експлуатацію [15][1)].

Аналіз технічних характеристик різних виробників СКУД ні до чого не привів, так як будь-яка технічна задача (з області СКУД), яке вирішується однією з систем, точно також може бути вирішена із застосуванням обладнання іншого виробника, тому при порівнянні СКУД доцільно використовувати ще одну змістовну характеристику – вартість системи конкретного виробника, а також аналіз програмного забезпечення цих СКУД.

1) [15] Сравнение СКУД. URL: http://biometricsecurity.ru/ (дата звернення 29.08.2019).

Було проведено коротке порівняння вартості і функціоналу та результати були зведені в таблицю 1:

Таблиця 1.

Назва ПЗ / Властивості ПЗ	Legos Люкс	ParcecNET Soft-08	PERCo-S-20
ОС, які підтримуються	Для сервера не нижче Microsoft Windows 2000 Adv. Server	Для сервера не нижче Microsoft Windows 2003 Server	Для сервера не нижче Microsoft Windows 2003 Server
Кількість користувачів	Не більш 3000	Не більш 4000	Не більш 50000
Кількість контролерів	Не більш 64	Не більш 8	Без обмежень
Інтеграція пожежної та охоронної сигналізації	+	+	+
Интеграция систем цифрового відеоспостереження	+	+	+
Наявність Web-интерфейсу	+	-	+
Кількість віддалених робочих місць	1	0	3
Можливість використання додаткових віддалених робочих місць	+	+	+
Модульність	+	+	+
Наявність всіх основних модулів в пакеті ПЗ	+	-	-
Користувацький интерфейс	Граф., віконн.	Граф., віконн.	Граф., віконн.

Відчутною перевагою ПО Legos є той факт, що всі основні модулі вже входять в пакет програмного забезпечення і не доводиться платити додаткові гроші, купуючи їх окремо. Завершальним етапом слід визначення вартості систем конкретних виробників і твір ранжирування можливих варіантів. У таблиці 2 представлені вихідні дані для розрахунку вартості систем контролю і управління доступом з лідерів ринку.

Таблиця 2. Вартість СКУД для двох точок проходу (турнікетів)

Назва	Ціна	Кількість	Сума
СКУД Parsec			
Контролер Parsec NC-5000	11389	2	22778
Зчитувач PR-P09	7963	4	31852
ПК-інтерфейс Parsec NI-A01-USB	3338	2	6676
ПЗ базове PNWin-08	6667	1	6667
Програмний модуль обліку робочого часу з генератором звітів PNWin-AR	8272	1	8272
Програмний модуль підготовки, ведення бази даних та другу пластикових карток PNWin-AR	13982	1	13982
Усього:			90227
Усього у перерахунку один пункт проходу			45114
СКУД Legos			
Контролер L5T04	11889	2	23778
Зчитувач PLR3	3193	4	12772
Конвертер CLE	4175	1	4175
ПЗ Люкс (32/3000)	18944	1	18944
Усього:			59669
Усього у перерахунку один пункт проходу			29835
СКУД PERCo			
Контролер PERCo-CT/L04	10730	2	21460
Зчитувач IR-07	3180	4	12720
Базове ПЗ, "Бюро перепусток", "Управління доступом», «Персонал», «Моніторинг», «Дисциплінарні звіти», «ОРС»	22790	1	22790
Програмний модуль «Облік робочого часу»	17600	1	17600
Усього:			74570
Усього у перерахунку один пункт проходу			37285

Таким часом можемо побачити, що найвигіднішим було б обрати систему Легос. Але для бюджетного закладу освіти ця система надмірно дорога, тому було обрано рішення подовжувати розробку власної системи контролю управлянням доступу.

2.2 Структура системи контролю і управлінням доступу

Як вже зазначалося вище, основним напрямком розвитку СКУД є їх інтелектуалізація, агрегування максимально можливої кількості функцій по збору, обробки інформації та прийняття рішень. Системи КУД здатні автоматизувати безліч процесів, пов'язаних з організацією доступу до ресурсу. Сюди входять реєстрація суб'єктів (користувачів і персоналу) і об'єктів (ресурсів) СКУД, безпосереднє надання доступу до ресурсу, організація контролю роботи персоналу, збір і надання статистики щодо функціонування системи і багато іншого.

В цілому систему можна поділити на дві підсистеми – апаратну та програмну. До апаратної підсистемі СКУД відносяться:

– зчитувачі (призначені для зчитування ідентифікаторів і передачі відповідної інформації в контролери);

– контролери (здійснюють обробку отриманої від зчитувачів інформації, приймають рішення про допуск або заборону проходу, передають інформацію на сервер системи);

– сервери (здійснюють накопичувати інформацію про всі проходи через БлП – час, дата, П.І.Б. та посада користувачів);

– комп'ютери з ПЗ (забезпечують моніторинг, централізоване управління системою, ведення журналу подій, побудова звітів);

– виконавчі пристрої (в нашому випадку – електромеханічні замки та турнікети, які забезпечують блокування дверей і проходів);

– блоки живлення (забезпечують електроживлення пристроїв системи як від мережі, так і від автономних джерел живлення);

– інше обладнання (кнопки виходу – забезпечують розблокування виконавчих пристроїв при виході з контрольованої зони; дверні дотягувачі – забезпечують закриття дверей).

Так як на сервері крім сервера баз даних буде знаходиться і web-сервер, то необхідно враховувати, що для його ефективної роботи необхідно щоб

машина мала достатньо системних ресурсів. Тобто сервер, на якому буде функціонувати дана система, повинен володіти досить потужною апаратною платформою. Особливо це стосується обсягу оперативної пам'яті і до частоти роботи центрального процесора.

Дані будуть зберігатися в базі даних. А так як втрата цих даних може привести до значних наслідків, отже, на сервері повинні бути передбачені апаратні засоби резервного копіювання цієї бази у вигляді реплікації БД на зовнішній сервер або зовнішній жорсткий диск.

Апаратні засоби управління повинні забезпечувати прийом інформації від зчитувачів, обробку інформації та вироблення сигналів управління на виконавчі пристрої. В якості керуючого елемента в СКУД, що розроблюється, передбачається використовувати мікроконтролер.

Мікроконтролер в СКУД повинен забезпечувати:

– обмін інформацією по лінії зв'язку між контролерами і засобами централізованого управління;

– збереження даних в пам'яті системи, при обриві ліній зв'язку із засобами централізованого управління, відключення живлення і при переході на резервне живлення;

– контроль ліній зв'язку між контролерами і засобами централізованого управління.

Протоколи обміну інформацією повинні забезпечувати необхідну стійкість, швидкість обміну інформацією, а також (при необхідності) імітостойкость (властивість, що характеризує здатність протистояти атакам з боку порушника, метою яких є нав'язування помилкового повідомлення, підміна переданого повідомлення або зміна даних, що зберігаються) і захист інформації (для систем підвищеної та високої стійкості).

Пристрій, що зчитує має забезпечувати:

– зчитування ідентифікаційного ознаки;

– перетворення введеної інформації в електричний сигнал;

– передачу інформації на контролер СКУД.

Пристрій, що зчитує, має бути захищеним від маніпулювання шляхом перебору і підбору ідентифікаційної ознаки. Зчитувач не повинен викликати відкриття БлП в разі злому або розтину, а також при обриві або короткому замиканні електричних ланцюгів.

Оскільки в якості ідентифікатора була обрана RFID карта, то зчитувальний пристрій повинен бути RFID сканером.

Останні роки ціни на апаратну частину стали трохи нижче, крім того опитним шляхом було встановлено, що система послідовного зв'язку не дуже добре працює в умовах школи, де постійно відбуваються якісь події – біг, стрибки, польоти портфелів та взуття, тому було обрано рішення використовувати мережеві контролери Ethernet замість RS232 або RS485, та інтегрувати їх в існуючу шкільну мережу. Для цього, але щоб не заважати один одному та не плутатись у мережевих пристроях, для обладнання СКУД було виділено окремий VLAN.

СКУД, орієнтовані на обслуговування великої кількості клієнтів, зазвичай мають модульну структуру, що дозволяє організувати робочі місця для різних служб, що забезпечують ефективне функціонування системи. Модульна схема забезпечується за рахунок використання архітектури клієнт-сервер. кількість і функціональність модулів залежать від призначення системи і виробника.

Для невеликих систем, де роль обслуговуючого персоналу відіграє лише одна людина, вся необхідна функціональність може бути зведена в єдиний модуль.

Модулі (службові додатки) взаємодіють з центральним сервером СКУД (рис. 2.7), який виконує роль деякого диспетчера, який займається обробкою запити додатків і події контролерів, датчиків і інших виконавчих пристроїв.

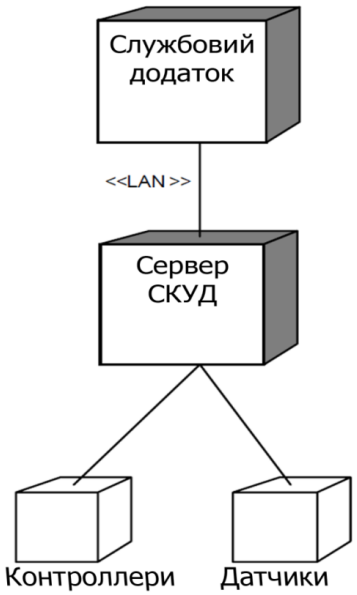

Рисунок 2.7 – Діаграма розгортання СКУД

Як середовище взаємодії службових додатків і сервера СКУД можуть виступати локальна обчислювальна мережа або адресний простір одного комп'ютера.

2.3 Модель предметної області

Моделі дозволяють наочно продемонструвати структуру і поведінку системи. Вони необхідні для візуалізації та управління архітектурою системи, мінімізації ризиків. Моделі дозволяють домогтися кращого розуміння систем, що призводить до їх спрощення і можливостям повторного використання. Система може бути описана з різних точок зору, для чого використовуються різні моделі, кожна з яких є семантично значимої абстракцією системи. Розрізняють структурні моделі, що представляють організацію системи, і поведінкові, що відображають її динаміку.

З появою стандарту в моделюванні, виникли CASE-засоби, що дозволяють візуалізувати цей процес, об'єднати моделі з документацією і навіть генерувати частини програмного коду. Універсальність мови моделювання

дозволяє згенерувати ділянки коду і описів на будь-якому об'єктно-орієнтованої мови Delphi, Java, C ++, Visual Basic і інших.

Модель предметної області наведено на рис. 2.8.

Група являє собою будь-яке об'єднання людей (фірма, сім'я і т.д.). Кожна людина в системі обов'язково приписаний якої-небудь групи. Доступ користувачів до своїх облікових записів здійснюється за паролем. Коли новий клієнт бажає зареєструватися, для нього створюється група, і він вважається її адміністратором. Адміністратор має такі повноваження:

– додавати в групу нових членів,

– налаштовувати права і розкладу доступу членів групи,

– створювати і налаштовувати рахунки,

– призначати рахунки для використання членам групи,

– встановлювати асоціації для своєї групи.

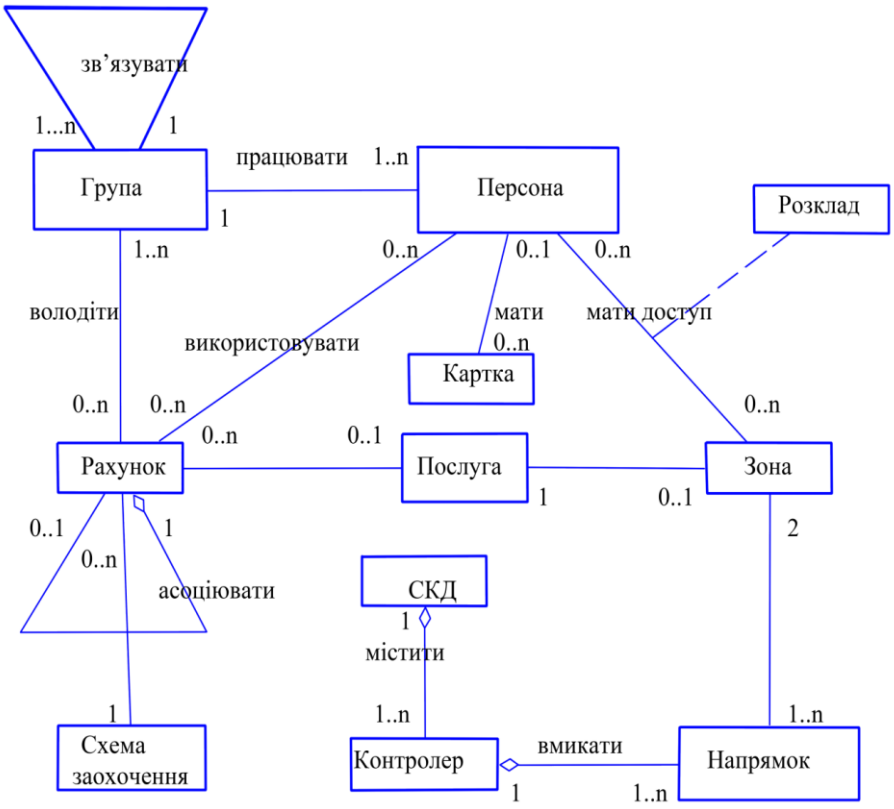

Рисунок 2.8 – Модель предметної області

Для того, щоб людина могла скористатися системою, їй видається RFID-карта. На кожен обліковий запис може бути видано не більше однієї карти. Кілька облікових записів не можуть використовувати одну карту.

Для того щоб побудувати ієрархію груп, між ними можна встановлювати зв'язки. Група, яка встановила зв'язок, дозволяє використовувати свої рахунки для встановлення асоціацію між ними. Група обов'язково має містити хоча б одного члена (її адміністратора).

Залежно від типу контролера-турнікета у нього може бути кілька напрямків доступу. Кожен напрямок пов'язано з двома зонами (зона, звідки здійснюється доступ, і зона, куди здійснюється доступ).

2.4 Програмна архітектура системи

Програмна підсистема має забезпечити функціонування згідно з діаграмами варіантів використання системи контролю та управління доступом до об'єктів, розробку структури бази даних, розробку web-інтерфейсу, розробку алгоритму роботи пристрою, що зчитує.

Діаграми варіантів використання системи контролю та управління доступом до об'єктів. З даною системою можуть працювати оператор і користувачі. Для кожного з них надаються свої права в системі.

Користувачеві (співробітнику або учню) доступні дві дії (рисунок 2.9) – ідентифікація (процес пізнання суб'єкта по властивому йому або наданим йому ідентифікаційним ознакою) і аутентифікація (процес пізнання суб'єкта шляхом порівняння введених ідентифікаційних даних з еталоном).

Всі користувачі, які володіють правом доступу до охоронюваного об'єкту, попередньо повинні пройти ідентифікацію, повинен бути створений ID-номер ідентифікує користувача. Потім, коли користувач хоче отримати доступ до об'єкту, що охороняється, він проходить аутентифікацію, тобто підносить пристрій, що зберігає ID-номер у зчитувальнім пристрої.

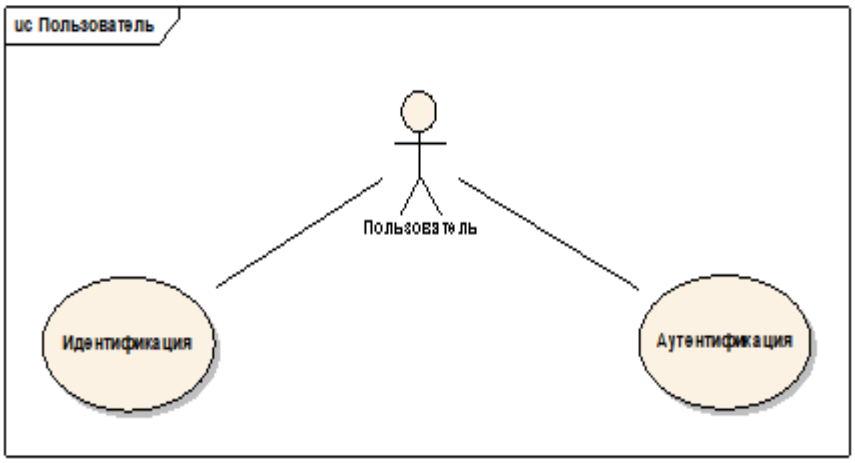

Рисунок 2.9 – Діаграма варіантів використання системи для користувача

Якщо id номера на сервері і пристрої збігаються, то користувач отримує доступ до об'єкту (на сервер відправляється повідомлення про санкціонованому доступі), в іншому випадку – в доступі буде відмовлено, і на сервер буде відправлено повідомлення про несанкціоновану спробу отримання доступу до об'єкта.

Оператор має доступ до налаштування і управління обладнанням, перегляду поточних подій системи, управління списком об'єктів доступу, перегляду архіву, а також отримання звітів (рисунок 2.10).

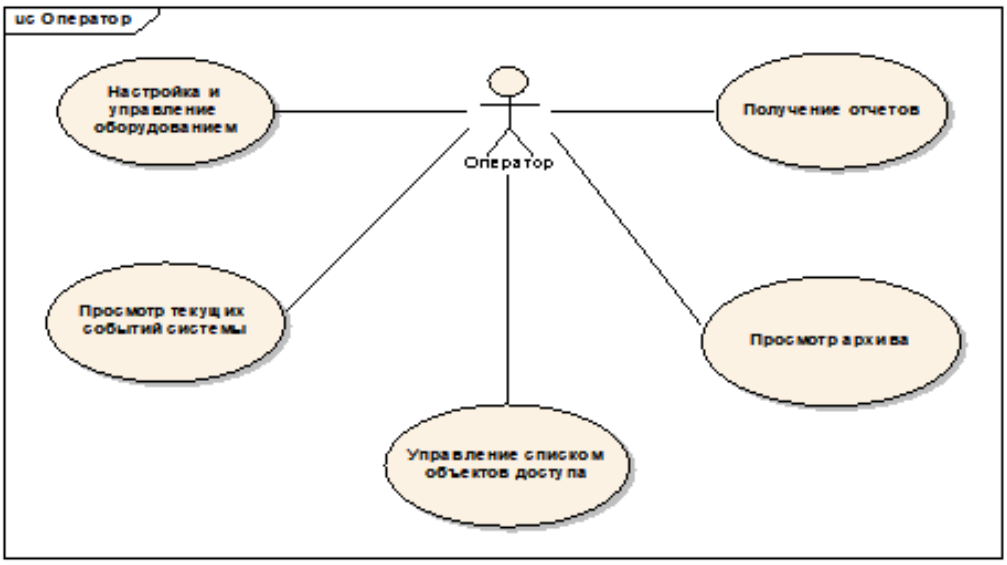

Рисунок 2.10 – Діаграма варіантів використання системи для оператора

Налагодження та управління обладнанням (рисунок 2.11) має на увазі під собою можливість оператора виконувати наступні дії:

– додання нової точки доступу (ТД); точка доступу – це місце, де здійснюється контроль доступу, в розроблюваної системі в якості ТД виступають тільки двері;

– видалення існуючих ТД;

– оцінка якості зв'язку з мікроконтролером;

– ручне управління точками доступу (можлива установка трьох режимів роботи – нормального, заблокованого і розблокованого);

– налаштування ТД (установка IP-адреси);

– управління мікроконтролером (отримання технічної інформації про МК, перегляд і реєстрація або видалення персоналу на обраної ТД).

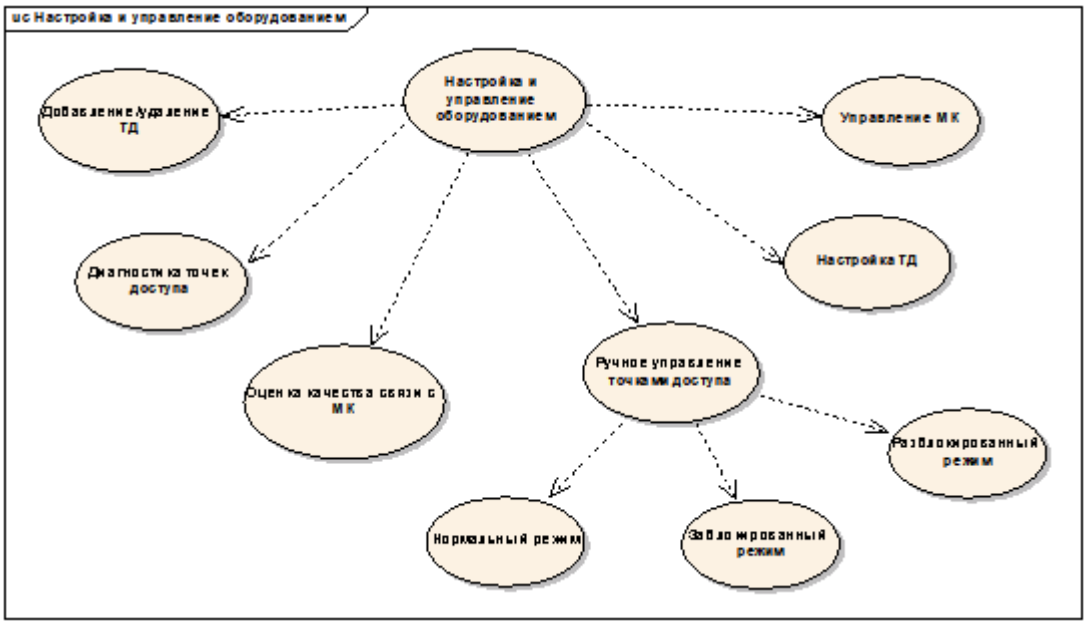

Рисунок 2.11 – Діаграма варіантів використання настройки і управління обладнанням

Перегляд подій системи (рисунок 2.12) полягає в тому, що оператор може вибрати цікавлять його точки доступу (одну, кілька, або ж все), налаштувати фільтр подій системи (наприклад, показувати тільки події по зареєст-

рованих спробах несанкціонованого доступу) і отримати доступ до останніх подібним подіям, що мали місце на даних точках доступу. Також, оператор може переглянути облікові картки користувачів.

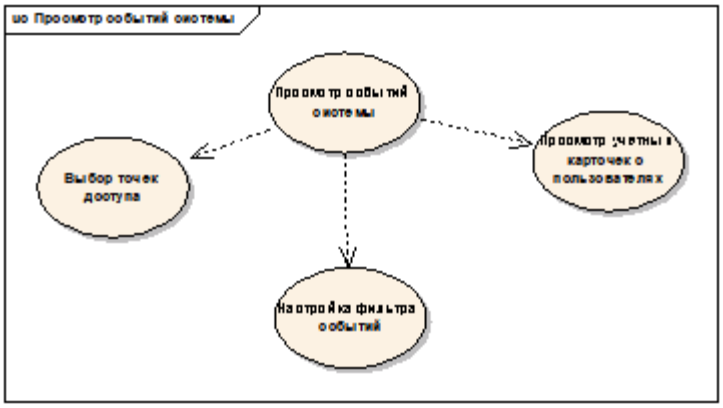

Рисунок 2.12 – Діаграма варіантів використання перегляду подій системи

Події системи – це дозволені або заборонені спроби проходу через точку доступу, а також факти зміни (втрати або появи) зв'язку з контролерами. Події доступу реєструються мікроконтролером автономно і незалежно від наявності зв'язку з сервером, час і дата події реєструються відповідно до вбудованим годинником реального часу. Всі зареєстровані події зберігаються в незалежній пам'яті контролера і автоматично передаються на сервер СКУД при наявності зв'язку. Таким чином, в базі даних сервера зберігаються всі події СКУД, за якими можна отримувати звіти за задані проміжки часу.

Система зберігає всю інформацію про зареєстрованих нею події, починаючи з моменту її першого запуску, без тимчасових обмежень. Кількість подій в системі – необмежена.

Трактування СКУД як системи реального часу вимагає реалізації механізмів диспетчеризації, взаємодії між об’єктами і засобів роботи з таймерами. Паралелізм в обробці одночасно відбуваються зовнішніх подій повинен забезпечується за рахунок використання багатопоточності. Клієнт-серверний підхід вносить необхідність реалізації механізму і способів взаємодії між

сервером і додатками, а загальні вимоги безпеки і надійності змушують вибирати особливі способи зберігання даних і роботи з ними.

Деякі архітектурні механізми використовують нестандартний підхід до створення об'єктів, що вимагає передачі строкового імені класу створюваного об'єкта. Цей підхід також може бути розглянуто як допоміжний механізм (або механізм нижчого рівня).

2.5 Організація взаємодії об'єктів

Диспетчер повідомлень. Для реалізації механізму взаємодії між об’єктами було створено спеціальний об'єкт – диспетчер. Диспетчер «знає» все об'єкти, які бажають обмінюватися повідомленнями, а ці об'єкти в свою чергу «знають» про існування диспетчера. Крім таблиці зареєстрованих об'єктів, важливою частиною диспетчера є черга повідомлень. Принцип відправки повідомлення можна описати таким чином (рис. 2.13):

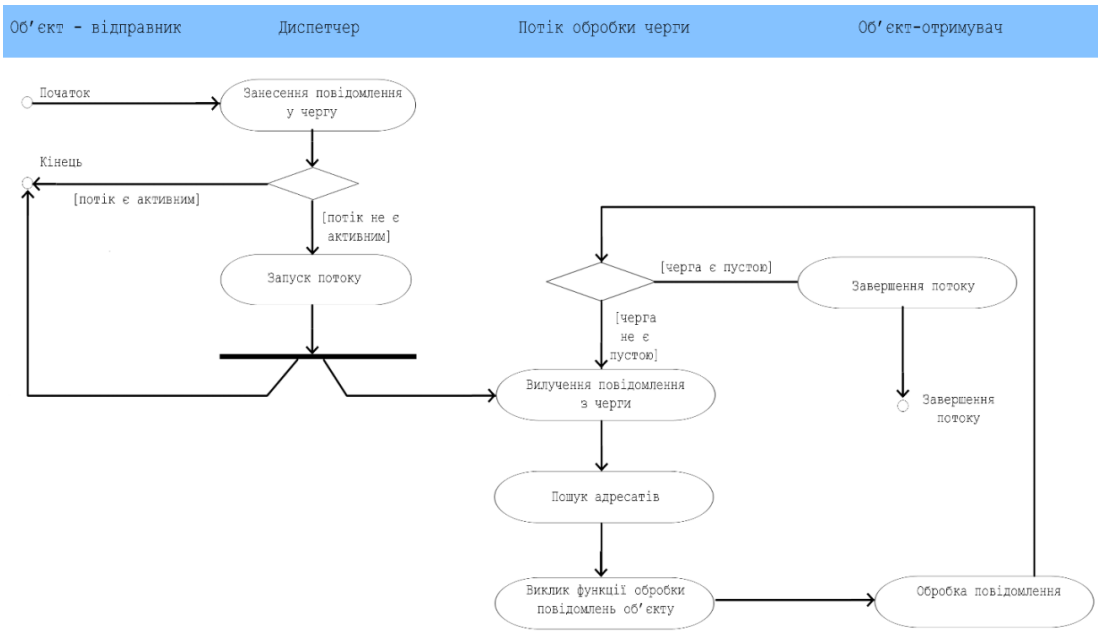

Рисунок 2.13 – Діаграма діяльності, що відображає принцип обробки повідомлення

– об'єкт-відправник створює повідомлення і ініціює його даними, потім він викликає функцію відправки повідомлення (SendEvent) диспетчера;

– диспетчер здійснює постановку повідомлення в чергу, перевіряє, чи запущений потік обробки черги повідомлень; якщо потік не запущений, то диспетчер його запускає, після цього управління повертається об'єкту–відправнику;

– потік обробки повідомлень витягує наступне повідомлення з черги, шукає об'єкт-одержувач по таблиці зареєстрованих об'єктів і викликає функцію обробки повідомлення одержувача (ProcEvent), передаючи їй як параметр об'єкт повідомлення. Коли управління повертається диспетчеру, потік здійснює перевірку наявності повідомлень в черзі. Якщо повідомлення відсутні, то потік завершується, в іншому випадку потік здійснює обробку повідомлення.

Перед викликом функції ProcEvent одержувача здійснюється запуск таймера. Якщо до моменту таймаута управління не повернуто об'єкту диспетчера, то потік переривається і запускається знову з наступного елемента черги повідомлень. Якщо ж одержувач знає, що час обробки повідомлення перевищує час таймаута, то він запускає свій потік і повертає управління диспетчеру.

Черга повідомлень диспетчера є масивом елементів повідомлень. Повідомлення в чергу укладаються послідовно. При досягненні кінця черги наступне повідомлення записується на перше місце, таким чином, чергу зациклена. Обробка черзі потоком припиняється, коли номер наступного оброблюваного елемента дорівнює номеру наступного додається елемента, що означає, що в черзі відсутні повідомлення.

Виділення об'єкта диспетчера з його чергою повідомлень дозволяє всі проблеми синхронізації багатопоточного додатку, за умови, що взаємодія об'єктів здійснюється тільки через чергу обробки повідомлень диспетчера.

Кожен об'єкт, який взаємодіє в системі характеризується трьома значеннями: номером класу, номером об'єкта і додатковим кодом. Для унікаль-

ної ідентифікації об'єкта використовуються перші два значення. Номери об'єктів видаються диспетчером послідовно, із заповненням пустот (тобто об'єкт займає перший вільний номер). Додатковий код покликаний виражати призначену для користувача нумерацію об'єктів. Крім того, він може бути використаний для пошуку об'єктів в системі (Seek, Select).

Трудомісткість пошуку елемента по таблиці взаємодіючих об'єктів є логарифмічною від числа об'єктів, що належать класу шуканого. Це пояснюється тим, що диспетчер працює з класами, як елементами масиву фіксованої довжини, а з об'єктами класу як з розширюваним масивом. Пошук по списку об'єктів здійснюється дихотомічно.

Проведене тестування показало, що диспетчер здатний підтримувати необмежену кількість об'єктів. Єдиним «вузьким» місцем може виступити чергу повідомлень: оскільки вона зациклена, то її переповнення може закінчитися втратою ряду початкових повідомлень.

Диспетчер подій. Для реалізації можливості підписки одних об'єктів на події інших диспетчер повідомлень був розширений функціями диспетчера подій. Це виразилося в додаванні таблиці передплатників і функцій роботи з подіями. об'єкт, бажаючий заявити про подію, створює об'єкт-повідомлення і заповнює частину його полів, що стосуються події. Після цього здійснюється виклик функції повідомлення про подію (ThrowEvent). Ця функція знаходить всіх передплатників, і відправляє їм повідомлення про подію, видаляючи їх підписні записи з таблиці. Якщо об'єкт бажає отримати подія знову, він повинен знову на нього підписатися.

Об'єкти мають можливість підписуватися на події монопольно (для цього в об'єкті повідомлення передбачений відповідний атрибут). При виникненні події диспетчер визначає наявність монопольних підписок, і розсилає повідомлення, повідомляючи адресатів, чи була заявлена монопольна підписка і чи є він монопольним адресатом. Залежно від цього об'єкт приймає рішення про відповідної реакції на подію.

Диспетчер таймерів. Для зниження завантаженості системи таймерами було вирішено організувати службу таймерів на основі диспетчера повідомлень. Для цього були додані таблиці таймерів об'єктів. При запуску диспетчера автоматично запускається періодичний таймер. Після закінчення кожного періоду лічильник кожного об'єкта, який замовив таймер (SetTimer), зменшується на одиницю. При досягненні нульового значення об'єкту надсилається повідомлення про закінчення часу очікування, при цьому запис таймера не видаляється і може бути ініціалізовано знову повторним викликом SetTimer. Для видалення запису таймера використовується функція DeleteTimer. Якщо викликається деструктор об'єкта, зареєстрованого у диспетчера, то відбувається видалення реєстрації даного об'єкта, видалення всіх його підписок (як входять, так і вихідних), а також видалення всіх його таймерів. Крім цього організовується перегляд черги повідомлень диспетчера і видалення всіх повідомлень, спрямованих тому об’єкту, що видаляється.

Трудомісткість пошуку по таблиці подій і таблиці таймерів логарифмічна від числа всіх елементів відповідної таблиці. На рис. 2.14 представлена діаграма класів системи взаємодії між об’єктами.

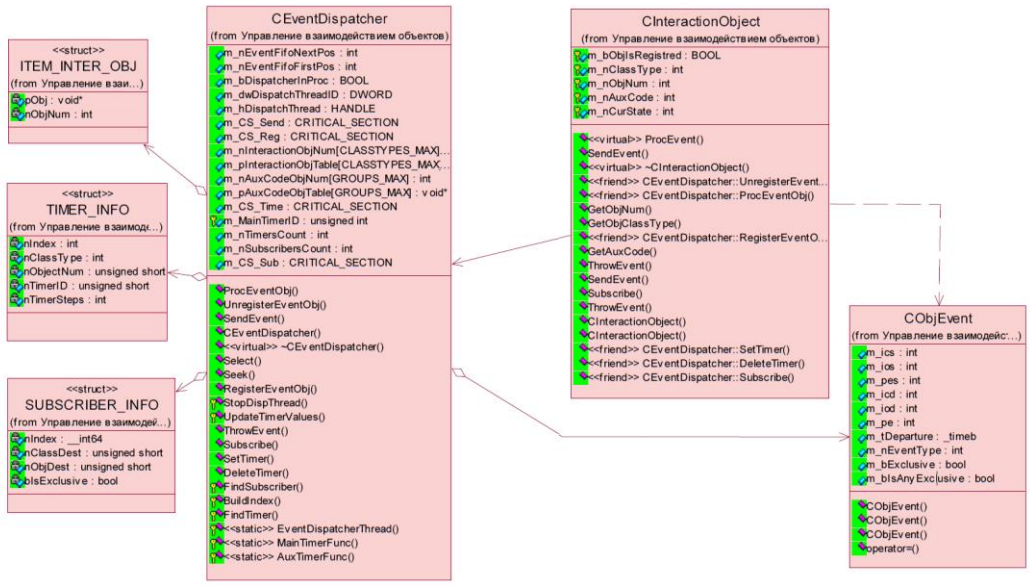

Рисунок 2.14 – Діаграма класів системи взаємодії між об’єктами

Клас CEventDispatcher реалізує диспетчер подій, повідомлень і службу таймерів. Клас CObjEvent є об'єктом подія, що містить інформацію про відправника, одержувача, тип повідомлення, структурі події і часу відправлення. Клас CInteractionObject задає загальний інтерфейс для всіх взаємодіючих об'єктів в системі. Структури ITEM_INTER_OBJ, TIMER_INFO, SUBSCRIBER_INFO представляють, відповідно, записи в таблиці об'єктів, таблиці таймерів і таблиці передплатників. Даний механізм реалізований в модулях InteracitonObject.cpp (h), EventDispatcher.cpp (h), ObjEvent.cpp (h).

2.6 Взаємодія додатків

Команди. Архітектура «клієнт-сервер» має на увазі, що програми-клієнти посилають запити серверу, а той їх виконує. Часто до сервера висуваються вимоги організації протоколювання цих запитів. Для реалізації такої схеми був використаний шаблон проектування «Команда». Він інкапсулює запит як об'єкт, дозволяючи тим самим задавати параметри клієнтів для обробки відповідних запитів, ставити запити в чергу або протоколювати їх, а також підтримувати скасування операцій.

Всі команди мають загальний інтерфейс, що задається класом CCommand (рис. 2.15). В цьому класі визначена віртуальна функція Execute, яка ініціює виконання команди. Такий підхід дозволяє виконати команду, не знаючи, яка це команда і що вона повинна зробити.

Якщо потрібно виконати не одну команду, а кілька, то можна визначити клас CMacroCommand як спадкоємець класу CCommand, доповнивши його операціями додавання і видалення команди і переписавши операцію Execute таким чином, щоб вона здійснювала послідовне виконання списку команд.

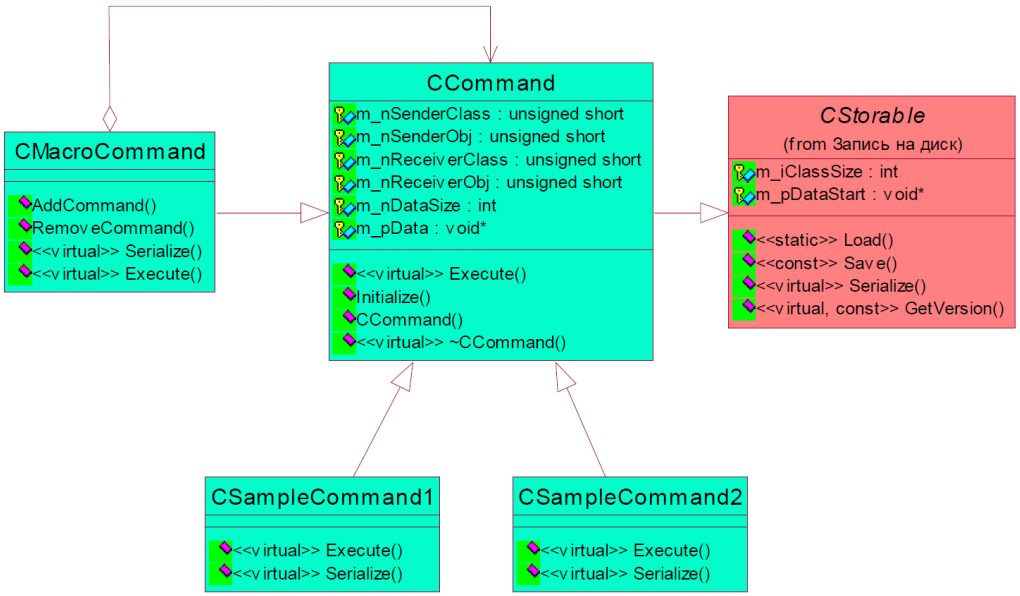

Рисунок 2.15 – Діаграма класів механізмів команд

Сервер і клієнти проводять обмін даними. Часто ці дані представляють собою різні об'єкти. Для того щоб організувати передачу об'єкта від одного додатка іншому, можна скористатися механізмом, аналогічним серіалізації, і здійснювати перетворення об'єкта в рядок. Тоді весь процес передачі об'єкта буде виглядати наступним чином:

– додаток-відправник створює об'єкт, ініціює його даними і викликає функцію перетворення в рядок (Transform).

– отриманий рядок передається з додатком-одержувачу разом з ім'ям класу об'єкта (або іншим ідентифікатором, що визначає об'єкт).

– одержувач створює об'єкт і викликає функцію перетворення, передаючи їй отриманий рядок.

Використання цього механізму передбачає, що і відправник і одержувач знають про клас об'єктів, що передаються. Вагомою перевагою є той факт, що тільки самі об'єкти знають, як себе упакувати. Це дозволяє не розробляти додатковий формат пакета для передачі кожного об'єкта і полегшує можливості заміни об'єктів і їх повторного використання, оскільки змінити потрібно лише логіку функцій класу об'єкта.

3 ВИБІР ЗАСОБІВ РЕАЛІЗАЦІЇ

3.1 Вибір архітектури апаратної та програмної реалізації системи

Загальна схема системи, що проектується, виглядатиме наступним чином. В якості апаратної платформи було використано такі елементи системи:

– персональний комп’ютер для виконання ролі сервера бази даних, програмних модулів та обробки подій;

– контролери зчитувачів та електромеханічних замків Z-5R NET (рис. 3.1);

– безконтактні зчитувачі RFID-карток (браслетів, кілець тощо) Iron Logic Matrix-II (рис. 3.2) [16][1)];

Рисунок 3.1 – Контролер електромагнітних замків та зчитувачів

Рисунок 3.2 – Безконтактний зчитувач RFID-карток

[1)] [16] Гильманов А.А., Клименко А.Я., Странгуль О.Н., Тарасенко В.П. Карткові технології в автоматизації маркетингу. Томськ: Видавництво НТЛ, 2000. 379 с.

– безконтактний USB зчитувачі-програматор RFID-карток Z-2 USB EM & HID PROX II & Mifare для програмування RFID-карток для працівників, учнів, відвідувачів тощо (рис. 3.3);

– електромагнітні замки МЕТАКОМ ML-250 для блокування дверей (рис. 3.4).

Рисунок 3.3 – Безконтактний USB-зчитувач-програматор RFID-карток

Рисунок 3.4 – Електромагнітний замок з дверним дотягувачем

– універсальний турнікет-тріпод півростовий Praktika–t–01 (рис. 3.5), якій може працювати як від пульту оператора (працівника служби охорони), так і під управлінням СКУД. Його стильний сучасній концептуальний дизайн і представницький зовнішній вигляд дозволяють органічно вписуватися в будь-який сучасний інтер'єр і задовольнити вимоги самого вимогливого клієнта. Корпус, планки і пульт управління з нержавіючої сталі, що гарантує тривалий термін служби виробу, а благородно матова поверхня перешкоджає

утворенню відбитків пальців і надає турнікету особливу естетичну привабливість. Ергономічний корпус без гострих кутів виключає травмування стегон і ліктів при проходженні, що особливо важливо при використанні у школі, а великий світлодіодний дисплей з полірованого штучного каменю розташований під зручним кутом зору і наочно відображає стан турнікета.

Рисунок 3.5 – Турнікет Praktika–t–01

Турнікет має автоматичну функцію «Антипаніка» (рисунок 3.6). При виникненні тривожної ситуації – після натискання кнопки на пульті управління або за сигналом від пожежної сигналізації електропривод автоматично переводить планки в нижнє положення, повністю звільняючи прохід.

Захист від зворотного провороту і утримання планок з вбудованою світловою та звуковою сигналізацією запобігає несанкціоновані проходи «ланцюжком».

Рисунок 3.6 – Турнікет Praktika-t-01 в режимі «Антипаніка»

Додатково було встановлено обладнання для обмеження в'їзду на прилегливу територію, щоб до будівлі була можливість під'їхати автомобілі постачальників продуктів або інших матеріалів, а саме швидкодіючий автоматичний шлагбаум Came GARD 4000 (рис. 3.7).

Рисунок 3.7 – Шлагбаум Came GARD 4000

Він зроблений для проїздів шириною до 4 метрів з унікальною особливістю: напруга електроживлення двигуна 24 В. Технологія низьковольтного електроживлення дозволяє отримати максимальну ефективність управління і повну безпеку роботи. Всі основні компоненти, необхідні для функціонування системи навіть у разі відключення електроживлення, змонтовані всередині корпусу шлагбаума; додатково до двигуна і блоку управління, в корпусі шлагбаума передбачено місце для установки аварійних акумуляторів.

До того ж, в комплекті є кілька пультів дистанційного керування і можна їх також купити окремо і під’єднати до системи, щоб мінімізувати участь працівника охорони. Наприклад, такі пульти отримають працівники школи та постачальники, які регулярно приїздять до школи, а реєстрацією за державним номерним знаком та ідентифікацією працівника.

Також було придбано систему відеоспостереження – реєстратор та камери виробництва компанії Hikvision. Сучасні 3 та 4 мегапіксельні камери та цифровий реєстратор з продвинутими алгоритмами запису дозволяють досить економно розпоряджатись місцем на жорстких дисках, отримуючи максимум якісного відео при мінімумі зайнятого простору, а також покращити систему охорони. Наприклад, функція «виявлення вторгнення» (рис. 3.8) дозволяє автоматично активувати режим запису або подати сигнал тривоги, коли в області з'являється людина або автомобіль.

Рисунок 3.8 – Виявлення вторгнення (А) та детектор обличчя (В)

Функція «детектор обличчя» (рис. 3.8) вже далеко не нова і є поширеним інструментом відеоаналітики. Але в 4-й серії камер вона підтримує різні тривожні сценарії, а також лежить в основі додаткової функції підрахунку людей в області огляду і може спільно працювати з іншими смарт-функціями.

Також досить цикава функція виділення області інтересу (ROI – Region of Interest). Ця функція дозволяє перерозподілити якість зображення прямо в кадрі, отримавши поліпшену деталізацію «області інтересу», не збільшуючи швидкість потоку передачі даних. Оператор за допомогою звичайної миші може виділити до 4-х прямокутних областей, в яких якість відео буде збільшено за рахунок зниження якості в суміжних областях. Така функція дозволяє раціонально використовувати ширину каналу і оптимізувати подальше зберігання. Це робить технологію виявлення вторгнення більш досконалої порівняно зі звичайним виявленням руху, яка реагує на птахів або коливання гілок дерев [17][1)].

Всі елементи системи з’єднуються та вмикаються до локальної мережі школи за допомогою кабелю «вита пара» п’ятої категорії та існуючих комутаторів, що підтримують локальну мережу школи, паралельно та послідовно за комбінованою схемою «зірка + кільце», приблизно таким чином, приклад якого наведений на рис. 3.9. Електромагнітні замки мають окреме резервоване живлення від електричної мережі та резервного акумулятора. Вибір апаратного забезпечення було зроблено на основі швидкого аналізу існуючих систем організації безпеки, можливості спільної роботи апаратних засобів та доступних цін. Майже всі елементи масово виробляються в Китайській Народній Республіці на великих заводах під пильним наглядом інженерів та контролерів якості, чому набули великої популярності та витримали випробування часом.

---

1) [17] Аналітика в камерах Hikvision: огляд смарт-камер. URL: https://hikvision.org.ua/ru/articles/analitika-v-kamerah-hikvision-obzor-smart-kamer (дата звернення 29.09.2019).

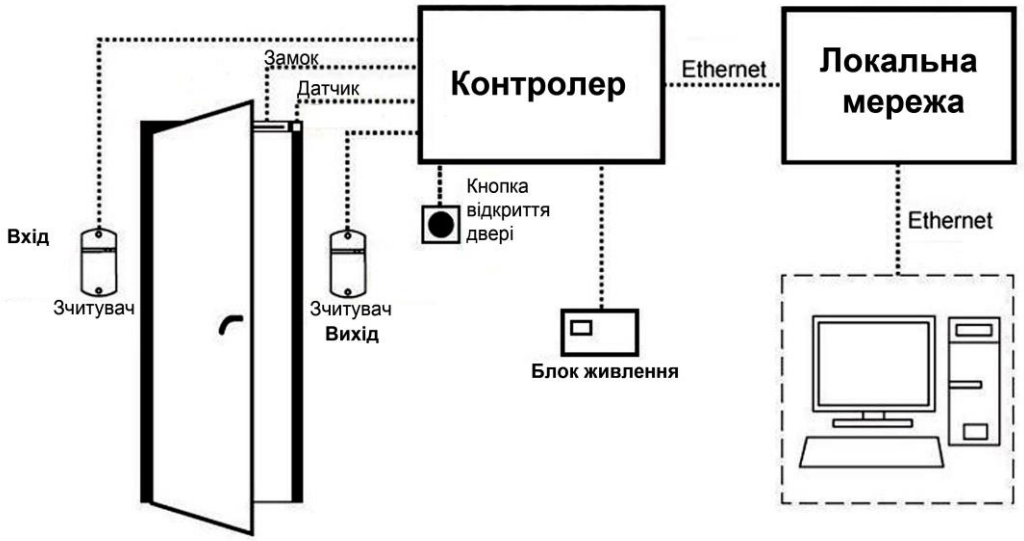

Рисунок 3.9 – Апаратна архітектура побудови СКУД

3.2 Вибір програмних засобів реалізації

Вибір системи управління баз даних (СУБД) являє собою складне багатопараметричне завдання і є одним з важливих етапів при розробці додатків баз даних. Обраний програмний продукт повинен задовольняти як поточним, так і майбутнім потребам, при цьому слід враховувати фінансові витрати на придбання необхідного обладнання, самої системи, розробку необхідного програмного забезпечення на її основі, а також навчання персоналу. Крім того, необхідно переконатися, що нова СУБД здатна принести реальні вигоди.

З переліку вимог до СУБД можна виділити кілька груп критеріїв:

– моделювання даних;
– особливості архітектури і функціональні можливості;
– контроль роботи системи;
– особливості розробки додатків;
– продуктивність;
– надійність;
– вимоги до робочого середовища.

У таблиці 3 наведені основні переваги і недоліки трьох найбільш популярних open-source СУБД – PostgreSQL, MySQL і FirebirdSQL.

Таблиця 3 – Переваги і недоліки різних СУБД

СУБД для зберігання даних	MySQL	PostgreSQL	FirebirdSQL
Переваги	швидкодія; безпека та надійність; відсутність високих апаратних вимог; кросплатформеність	підтримка БД майже любого розміру міцні та надійні механізми транзакцій та реплікацій; успадкування; масштабованість.	багатоверсійна архітектура; компактність; висока ефективність і міцна мовна підтримка для процедур і тригерів.
Недоліки	відсутність транцакцій і тригерів; відсутність процедур та вкладених запитыв немає підтримки інструкції UNION; відсутність каскадного оновлення даних.	відносна складність інсталяції; невірна робота оточення PostgreSQL; відсутність повної підтримки мов програмування VB и C#; відсутність Intellisense при програмуванні.	відсутність кеша результатів запитів; відсутність повнотекстових індексів.

Кожна база даних має свої особливості і відмінності. Але так як для розроблюваної системи необхідно швидке сховище для простих запитів з мінімальною налаштуванням, то в якості СУБД для зберігання даних буде використовуватися СУБД MySQL.

Програмна платформа буде базуватись на сервері з операційною системою Linux Centos 8.0. Вибір обумовлений тім, що CentOS (Community ENTerprise Operating System) – це дистрибутив Linux з відкритим кодом. Багато хто ставиться до неї, як до копії Red Hat Enterprise Linux (RHEL) – найбільш поширеного рішення для корпоративних завдань в світі IT. Це клас операційних систем для великих проектів, має підтримку спільноти і почала

випускатись ще з далекого 2004 року [18][1]. Велика схожість з RHEL надає чудову можливість розвиватися в домінуючому і одному з кращих дистрибутивів Linux. Дана ОС підтримує практично всі панелі управління хостингами, тому не буде проблем налаштувати веб-сервер так, як це буде потрібне.

Вона прекрасно настроюється, безпечна і стабільна, що теж важливо для додання їй цінності. Близьку спорідненість з RHEL дозволяє CentOS мати чимало оновлень захисту корпоративного рівня, що робить його безпечним вибором для кожного користувача [19][2].

Apache і Nginx – це два найпопулярніших веб-сервера в світі. Обидва використовуються для обробки HTTP-запитів, але кожен з них має власний набір характеристик. В основі роботи веб-сервера Apache створення окремого процесу або потоку у відповідь на кожен користувальницький запит. Дана технологія досить легка в реалізації, але, на жаль, однозначно не підходить для проектів, у яких багато завдань. Будь-який процес «з'їдає» пам'ять і ресурси системи. Тому Apache підходить для сайтів з низьким рівнем завантаженості. В основі роботи веб-сервера Nginx – створення дочірніх процесів, які і обробляють запити. Тому дана технологія підходить більше для високонавантажених сайтів, які обслуговують тисячі з'єднань одночасно.

За способом видачі контенту беб-сервер Apache генерує статичний і динамічний контент, тому його вибирають користувачі, які не мають бажання налаштовувати проксі і додаткові можливості для роботи з динамікою. На відміну від нього, Nginx видає тільки статичний контент, а ось динамічний не генерує. Правда, його можна використовувати в зв'язці з Apache, PHP-PFM або будь-яким іншим web-додатком, наприклад, Python (Django), Ruby on Rails, nodejs і т.і.

---

[1] [18] Алла Рудь. Яку ОС обрати для роботи сервера. URL: https://hyperhost.ua/info/kakuyu-os-vyibrat-dlya-rabotyi-servera/ (дата звернення 02.10.2019).

[2] [19] Жданов А.А. Сучасний погляд на ОС реального часу. URL: http://asutp.interface.ru/articles/ display_topic_threads.asp?ForumID=13&TopicID=299 (дата звернення 04.10.2019).

Серед можливостей роботи з Apache слід виділити функцію конфігурації обробки запитів на рівні каталогів за допомогою прихованого файлу htaccess. За допомогою нього є можливість налаштувати авторизацію і аутентифікацію, кешування і права доступу користувачів. Конфігурацію міняти можна прямо під час роботи, при цьому не потрібно перезавантаження сервера і додаткова настройка сервера. Веб-сервер Nginx таких можливостей не має. Надається тільки один конфігураційний файл, який обробляє майстер. Для запуску оновлень конфігурації, необхідно відправити сигнал майстру і зробити перезавантаження сервера [20][1)].

На основі цього було зроблено вибір в бік веб-серверу Apache.

Таким чином, було обрано майже стандартну серверну збірку LAMP – Linux, Apache, Mysql, PHP. LAMP – це абревіатура набору вільного ПЗ з відкритим кодом, в який входять ОС Linux, веб-сервер Apache, СУБД MySQL, та інтерпретатор Perl/PHP/Python – основні компоненти для побудови життєздатного багатоцільового веб-сервера.

Також важливий момент – збірка веб-серверу буде здійснено з підтримкою SSL, та буде придбано сертифікат безпеки від гідного центру сертифікації. Оскільки передбачається, що доступ до системи буде не лише з шкільної мережі, а й з зовні, за допомогою глобальної мережі інтернет – для контролю батьками учнів, електронного щоденника та інших сервісів.

Додатково розглянемо вибір мов програмування. Для створення програмного забезпечення під мікроконтролер існують різні мови програмування, але, мабуть, найбільш придатними є асемблер і Сі, оскільки в цих мовах в найкращій мірі реалізовані всі необхідні можливості по управлінню апаратними засобами мікроконтролерів.

Асемблер – це низькорівнева мова програмування, що використовує безпосередній набір інструкцій мікроконтролера. Створення програми на цій

[1)] [20] Apache vs Nginx: обираємо оптимальний веб-сервер. ITSource. URL: https://itsource.com.ua/ blog/apache-vs-nginx-vy-biraem-optimal-ny-j-veb-server/ (дата звернення 04.10.2019).

мові вимагає хорошого знання системи команд програмованого чіпа і достатнього часу на розробку програми. Асемблер програє С в швидкості і зручності розробки програм, але має помітні переваги в розмірі кінцевого виконуваного коду, а відповідно, і швидкості його виконання.

С дозволяє створювати програми з набагато більшим комфортом, надаючи розробнику всі переваги мови високого рівня. Компіляція вихідних текстів, написаних на С, здійснюється швидко і дає компактний, ефективний код. Основні переваги С перед асемблером:

– висока швидкість розробки програм;
– універсальність, яка не потребує досконального вивчення архітектури мікроконтролера;
– найкраща документовані і читаність алгоритму; наявність бібліотек функцій;
– підтримка обчислень з плаваючою точкою.

У мові С гармонійно поєднуються можливості програмування низького рівня з властивостями мови високого рівня. Можливість низькорівневого програмування дозволяє легко оперувати безпосередньо апаратними засобами, а властивості мови високого рівня дозволяють створювати легко читається і модифікується програмний код. Крім того, практично всі компілятори С мають можливість використовувати асемблерні вставки для написання критичних за часом виконання і займаним ресурсів ділянок програми.

Проаналізувавши основні особливості мов програмування С та асемблера, вибір був зупинений на С.

Для розробки серверної частини у свою чергу було прийнято рішення використовувати мову високого рівня, а саме об'єктно-орієнтовану мову програмування. На розгляд було запропоновано дві мови програмування, що задовольняють умови (об'єктно-орієнтовані, з синтаксисом, успадкованим від С):

– C#, розроблена групою інженерів під керівництвом Андерса Хейлсберга в компанії Microsoft як мова розробки додатків для платформи Microsoft.NET Framework;

– Java, розроблена компанією Sun Microsystems. Програми Java зазвичай компілюються в спеціальний байт-код, тому вони можуть працювати на будь-який віртуальної Java-машині (JVM) незалежно від комп'ютерної архітектури.

Вирішено використовувати, як мову розробки серверної частини – Java, який, на відміну від C#, є міжплатформеним.

Для створення web-інтерфейсу буде використовуватися бібліотека Vaadin. Це платформа з відкритим вихідним кодом для створення повнофункціональних інтернет-додатків. На противагу бібліотекам JavaScript і рішенням на основі браузерів/модулів, в її склад входить архітектура на стороні сервера, що означає виконання більшої частини програмної логіки на серверах. На стороні клієнта Vaadin будується на основі GWT і може бути розширена з її допомогою. Основним елементом Vaadin є бібліотека Java, розрахована на спрощення створення і обслуговування високоякісних веб-інтерфейсів користувачів. Основна ідея сервероцентрічной моделі програмування Vaadin полягає в тому, що вона дозволяє забути про мережі та програмувати інтерфейси користувачів точно так же, як ми програмуємо все настільні додатки Java, тобто за допомогою звичайних наборів засобів, таких як AWT, Swing або SWT – тільки ще простіше. Така модель програмування дозволяє Vaadin взяти на себе управління призначеним для користувача інтерфейсом в браузері і зв'язок AJAX між браузером і сервером. Підхід Vaadin дозволяє не витрачати сили на вивчення і налагодження технологій на стороні браузерів, таких як HTML або JavaScript [21][1)].

Можливості Vaadin досить широкі. Використання Java як єдину мову програмування при створенні веб-додатків і веб-контенту – одна з найбільш

[1)] [21] Введення до Vaadin. URL: https://www.codeflow.site/ru/article/vaadin (дата звернення 12.10.2019).

важливих функцій в Vaadin. Фреймворк використовує подієву модель і певні елементи призначеного для користувача інтерфейсу, віджети, що робить його дуже близьким до моделі розробки десктоп-додатків на Java з використанням HTML і Javascript.

Організація моделі даних і віджетів дозволяє відображати в браузері великі обсяги даних без значної завантаження пам'яті і без додаткових дій з стороніразработчіка.

Використання Google Web Toolkit для відображення сторінок з результатами пошуку і обробки дій користувача (на зразок термінального клієнта). Так як Google Web Toolkit функціонує тільки на стороні клієнта, Vaadin додає додаткову затвердження даних на стороні сервера: це вирішує проблеми безпеки, пов'язані з можливістю підміни даних або коду Javascript. Відповідно, при зміні і пошкодженні даних, що надходять від браузера, сервер, визначивши це, не пропускає запити [22][1)].

Можливість розширення стандартного набору віджетів Vaadin за рахунок інших віджетів, написаних для GWT, а також кастомізації його за допомогою CSS. Однак стандартний додаток, що створюється на Vaadin, не вимагає програмування саме на GWT та подальшої компіляції GWT-компілятором, якщо тільки розробник не додає в проект нестандартні віджети.

3.3 Розробка класів-сутностей

При розробці системи, було прийнято рішення використовувати ORM. ORM (абревіатура від Object Relational Mapping – Об'єктно-реляційна проекція) – технологія програмування, яка зв'язує бази даних з концепціями об'єктно-орієнтованих мов програмування, створюючи «віртуальну об'єктну базу даних». Суть проблеми, яка вирішується за допомогою ORM-шару, полягає в необхідності перетворення об'єктних структур в пам'яті програми в форму,

[1)] [22] Юрій Артамонов. Vaadin Flow – дивовижний олень. URL: https://habr.com/ru/company/ haulmont/blog/416893/ (дата звернення 12.10.2019).

зручну для збереження в реляційних базах даних, а також для розв'язання оберненої задачі – розгортання реляційної моделі в об'єктну, при цьому зберігаються властивості об'єктів і відносин між ними.

JPA – це технологія, що забезпечує об'єктно-реляційне відображення простих JAVA об'єктів і надає API для збереження, отримання та управління такими об'єктами. Також це специфікація (документ, затверджений як стандарт, що описує всі аспекти технології), частина EJB3 специфікації.

Сам JPA не вміє ні зберігати, ні управляти об'єктами. JPA визначає інтерфейси, які повинні будуть бути реалізовані провайдерами. JPA визначає правила про те, як повинні описуватися метадані відображення і про те, як повинні працювати провайдери. Далі, кожен провайдер, реалізуючи JPA, визначає отримання, збереження і управління об'єктами. У кожного провайдера реалізація різна.

При виборі ORM не виникло особливих проблем, так як в проекті використовується синтаксис лише JPA, без доповнень унікальних функціональностей різних бібліотек ORM, тому була вибрана бібліотека «Hibernate». Варто відзначити, що можна підключити будь-яку іншу ORM бібліотеку, без внесення змін до класи-сутності. Було розроблено ряд сутностей, які розглянемо нижче.

«Рівень доступу» – дану сутність буде створено для обмеження або ж дозволу доступу тому чи іншому співробітнику в різні приміщення.

«Група доступу» – сутність служитиме для об'єднання співробітників з однаковими правами доступу в одну підмножину. Для об'єднання персоналу або учнів з одним і тим же рівнем доступу буде створена дана сутність.

«Доступні місця» – сутність вказує в які кімнати зможе входити людина, володіючи певними правами доступу. Ця сутність необхідна, так як, перш ніж пустити когось в приміщення, необхідно знати, чи має він на це право.

«Користувач» – робочий персонал, учні, батьки. Дана сутність зберігає персональні дані кожного працівника школи, учнів, постачальників, членів

батьківського комітету та інших, хто має право доступу на територію та в окремі приміщення школі, такі як П.І.Б., дата народження або посаду.

«Пропущено через хворобу» – для обліку днів, проведених співробітниками або учнями на лікарняному. За допомогою даної суті система може точно підрахувати яку суму заробітної плати варто нарахувати співробітникам, з урахуванням лікарняних днів та скільки пропусків в учнів.

«Реальна зарплата» – сума зароблених працівником грошей за місяць, з урахуванням лікарняних, преміальних і штрафних.

«Переходи» – сутність для контролю і зберігання всіх переходів з одного приміщення в інше. Містить інформацію про час входу в приміщення, про місце від куди був здійснений перехід. Якщо співробітник вперше за день увійшов в цю кімнату, то в поле «від куди» буде зберігатися 0. Таким чином, можна відстежити, куди в першу чергу ходив співробітник. Так само сутність зберігає дані про проведений час в тому чи іншому приміщенні.

«Кімната» – зберігає номер кабінету або приміщення і необхідний рівень доступу, для здійснення позитивного переходу.

«Поверх» – служить для зберігання номера поверху і шляхи до SVG файлу (векторний малюнок), на якому зображений план приміщення поверху.

«Будівля» – сутність на випадок, коли приміщення розташовані на території більш ніж 1-го будинку. В нашому випадку слюсарні та столярні майстерні знаходяться у окремій будівлі. Сутність зберігає номер будівлі, адреса за яким воно розташоване і файл SVG, на якому розміщено схематичне зображення будівлі.

Під час проектування системи були створені діаграми класів, для спрощення розуміння «логіки» системи. Розглянемо набір класів, за допомогою яких забезпечується обмін даними між системою і базою даних.

Зверху перебуває інтерфейс IID, який розширюють все класи сутіності. Він створений для спрощення сприйняття коду програми. Для того що б не представляти всі класи у вигляді AbstractClass <ClassName, ID>, за допомо-

гою даного інтерфейсу, ми представляємо класи як AbstractClass <ClassName>. Розглянемо кожну сутність окремо. Клас «AccessLevel» існує для зберігання рівня доступу до того чи іншого об'єкту для кожної групи персоналу. Клас «GroupWorker» необхідний для об'єднання персоналу в якесь безліч, за різними принципами, для забезпечення прав доступу. «WorkBench» зберігає дані про те, в яких приміщеннях працювати той чи інший співробітник або учень. Це необхідно для того що б коректно підрахувати час проведений на робочому місці. Відсутність будь-якого з приміщень в даному списку вказує на те, що відповідна група користувачів не має права доступу до приміщення. Клас «RealSalary», зберігає інформацію про заробітну плату за місяць, з урахуванням лікарняних, штрафних або ж преміальних. Клас «MissByIll» для ведення обліку про лікарняних кожного співробітника, ця інформація необхідна, для коректного підрахунку заробітної плати, за місяць.

Клас «User» служить для зберігання і верифікації персональної інформації про співробітників підприємства. Використовуючи ці дані система приймає рішення щодо дозволу доступу в приміщення. Якщо співробітника з даними ID не існує в базі даних, то система заборонить доступ до будь-якому приміщенню. «Transition» необхідний для обліку інформації про переходах скоєних робочим персоналом. На основі цієї інформації будується список переходів певного співробітника, вираховується час проведений на робочому місці і розрахунок заробітної плати, а так само грунтуючись даною інформацією можна дізнатися де знаходитися працівник в даний момент.

Нижче подано діаграму класів бізнес логіки системи контролю та управління доступом. Клас «Index» виступає в ролі головної сторінки системи, він створює об'єкт класу в якому започатковано всі необхідні компоненти розміщені на головній сторінці та проводиться розмітка сторінки. Так само клас «Index» відповідає за виклик всіх форм, усередині яких розміщена вся необхідна інформація для управління системою, на приклад форма «User» відображає список всіх користувачів з можливість фільтрувати список за різними критеріями. На формі «Stage» відображений план поверху, клікнувши

на потрібну кімнату на плані приміщення відкривається список всіх співробітників знаходяться в цій кімнаті в даний момент. Так само можна знайти певного користувача на плані приміщення задавши його id або ж Прізвище та ініціали.

Клас «AbstractForm» містить всі узагальнені методи всіх класів форм, такі як додавання, видалення, заміна, які відкривають користувачеві компоненти полів для введення даних. Кожна з форм займається відображенням даних на екран, а так само їх додаванням, видаленням і заміною.

Так само на схемі присутній допоміжний клас. «SpringContextHelper»-цей клас забезпечує отримання даних з репозиторіїв до контролерів. Замість DAO класів використовується PagingAndSortingRepository – це інтерфейс бібліотеки spring-data, який входить до складу фреймворка «Spring». Використовуючи дану бібліотеку, не потрібно створювати абстрактну фабрику DAO і успадковувати усіма DAO класами узагальнені методи. Але для нормальної передачі інформації з бази даних, через репозиторії, до контролера, необходмо створити SpringContextHelper. Усередині цього класу необхідно створити конструктор всередині якого передати змінну яка визначає набір методів, які сервлет використовує для зв'язку з його контейнером сервлетів. В іншому випадку дані не виводитися не будуть.

У класі «Components» описана розмітка, яка буде застосована до головної сторінки, там же не започатковано всі компоненти інтерфейсу головної сторінки.

3.4 Алгоритми обліку доступу до приміщень

При розробці системи було реалізовано безліч алгоритмів, але не хотілося б зупинятися на всіх. Тому будуть розглянуті кілька алгоритмів основного призначення системи, а саме алгоритми обліку доступу в приміщення.

Спочатку були розглянуті алгоритми обліку про вхід у приміщення. При здійсненні події входу в приміщення, система створює об'єкт класу

Transition (перехід) і в локальну змінну tempId заносяться дані з картки, а саме Id користувача, які зчитуються пристроєм читання. Далі проводиться пошук даного користувача в системі по його Id, якщо користувач не знайдений, то в поля класу Transition, «isAccessPermitted» заносяться дані булевого типу «false», а в поле «reason» – «nu» (No User), після чого відбувається завершення методу і повернення false. В іншому випадку, тобто у разі якщо користувач з наявними Id присутній в системі відбувається запис в поля класу «toRoom» заносяться відповідні дані – номер кімнати, в яку здійснюємо перехід, «timeIn»-час входження в кімнату. Після чого система перевіряє чи має право співробітник увійти в дане приміщення, якщо працівник не володіє таким правом, то система заносить в поля класу «isAccessPermitted» дані булевого типу «false», а в поле «reason» – «na» (No Access) і завершує метод з поверненням false. У разі позитивного результату перевірки система заносить дані в поля «isAccessPermitted» булевого типу «true», а в поле «reason» – «ok» (і завершує метод повертаючи true.

Другий алгоритм забезпечує облік виходу з приміщення. При здійсненні виходу система здійснює пошук вже вчиненого входу в кімнату цім працівником. У разі повернення результату null методом пошуку, метод виходу завершується повертаючи false. В іншому випадку в поля об'єкта (об'єкт передається методом findTransition) знайденої транзакції заносяться дані, а саме в поле timeout заноситься час виходу а в поле «spendtime» вводиться число часу проведене в приміщенні.

Клас «Index» виступає в ролі головної сторінки системи, він створює об'єкт класу в якому започатковано всі необхідні компоненти розміщені на головній сторінці та проводиться розмітка сторінки. На формі «Stage» відображений план поверху, якщо клікнути на потрібну кімнату на плані приміщення, відкриється список всіх людей, що знаходяться в цій кімнаті в даний момент. Так само можна знайти певну особу на плані приміщення задавши його id або ж прізвище та ініціали.

3.5 Реалізація структури бази даних

Основними критеріями, що висуваються до інформаційної БД є:

– простота і зручність в створенні бази даних і подальшій роботі з нею;

– зручний, призначений для користувача інтерфейс, який дозволяє мати доступ до будь-якої інформації, а також оперативно змінювати інформацію в БД;

– зручне і наочне відображення результатів пошуку потрібної інформації;

– можливість виведення на друк будь-якої інформації з БД.

Перш ніж почати створювати будь-яку базу даних, треба чітко визначити наступне:

– призначення бази даних;

– як БД буде використовуватися;

– які відомості в цій базі даних будуть зберігатися, тобто треба виявити ціль створення бази даних.

У базі даних будуть міститися такі відомості:

– про групу (назва);

– про рівень доступу (номер доступу);

– про робоче місце (номер кабінету);

– про користувачів (П.І.Б., адреса, телефон, фото, паспортні дані, дата народження);

– про зарплатні (місяць, зарплата, час проведений на робочому місці);

– про пропусках через хворобу (дата початку лікарняного, дата закінчення лікарняного);

– про переході (час проведений, перехід з, перехід в, індикатор вдалого переходу, причина заборони, час входу, час виходу);

– про кімнату (номер кімнати, рівень доступу);

– про поверх (номер поверху, шлях до макету креслення);

– про будівлі (адреса, номер будинку, шлях до макету плану).

При побудові моделі даних в сукупність реквізитів об'єктів має відповідати вимогам нормалізації. Реквізити кожного об'єкта повинні відповідати вимогам, відповідним третій нормальній формі реляційної моделі даних. Виконання вимог нормалізації забезпечує побудова реляційної БД без дублювання даних і можливість підтримки цілісності при внесенні змін.

Аналізуючи мета створення БД системи контролю та управління доступом, є можливість відразу виділити об'єкт «Оператор», який матиме такі характеристики, наведені у таблиці 4.

Таблиця 4 – Опис таблиці «Operator»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор групи користувачів
groupname	Varchar(255)	not null	Назва групи

Дані цього об'єкту відповідають вимогам нормалізації:

– він має унікальний ідентифікатор – ключ;

– між описовими реквізитами немає функціональної залежності;

– кожен описовий реквізит функціонально залежить від ключа.

Тобто в отриманих об'єктах все описові реквізити логічно пов'язані.

Також, в БД, що проектується, необхідно ввести ще дев'ять об'єктів: «Рівень доступу», «Робоче місце», «Користувач», «Пропущені через хворобу», «Зарплата», «Перехід», «Кімната», «Поверх» і «Будівля» описані в таблицях 5–13.

Таблиця 5 – Опис таблиці «AccessLevel»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор групи користувачів
levelnumber	bigint(20)	not null	Рівень доступу до кімнати, яку дозволено відвідувати

Таблиця 6 – Опис таблиці «WorkBench»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор групи робочого місця
workbenchNumber	bigint(20)	not null	Номер приміщення, що є робочим місцем

Таблиця 7 – Опис таблиці «User»

Назва	Тип даних	Обмеження	Опис
id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор групи робочого місця
FirstName	bigint(20)	not null	Им’я працівника
LastName	Varchar(255)	not null	Прізвище працівника
birthday	Date	not null	Дата народження
job	Varchar(255)	not null	Посада працівника
salary	Bigint(20)	not null	ставка
address	Varchar(255)	not null	Домашня адреса
phone	Varchar(255)	not null	Телефон
PassportData	Varchar(255)	not null	Серія и номер паспорту
photo	Varchar(255)	not null	Шлях до фото на сервері
departmentName	Varchar(255)	not null	Назва відділу
obligedspendTime	Bigin(20)	not null	Час присутності на місці

Таблиця 8 – Опис таблиці «ReralSalary»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор заробітньої платні.
Date	Date	not null	Номер приміщення, що є робочим місцем
RealTimeWork	Bigint(20)	not null	Час перебування на робочому місці за місяць
Salary	Bigint(20)	not null	Нарахована заробітня платня з урахуванням премій, лікарняних та штрафів

Таблиця 9 – Опис таблиці «MissedByIllnes»

Назва колонки	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор лікарняного
FromDate	Date	not null	Дата початку лікарняного
ToDate	Date	not null	Дата закінчення лікарняного

Таблиця 10 – Опис таблиці «Transition»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор переходу
fromRoom	Bigint(20)	not null	Номер приміщения
Io	Varchar(255)	not null	Час перебування на робочому місці за місяць
isAccessPermited	Tinyint(1)	not null	Нарахована заробітня платня з урахуванням премій, лікарняних та штрафів
Reason	Varchar	not null	Привід заборони доступу
spendTime	Bigint(20)		Час перебування у приміщенні
timeIn	Date	not null	Час входу
Timeout	Date	not null	Час виходу
toRoom	Bigint(20)	not null	Номер приміщення, з якого виходимо

Таблиця 11 – Опис таблиці «Room»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор приміщення.
roomNumber	Int(11)	not null	Номер кімнати
acessLevel	Int(11)	not null	Рівень доступу

Таблиця 12 – Опис таблиці «Stage»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор поверху
StageNumber	Int(11)	not null	Номер поверху
svgFilePath	Date	not null	Шлях до SVG файлу

Таблица 13 – Описание таблицы «Buildings»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор лікарняного
Address	Varchar(255)	not null	Дата початку лікарняного
buildingsNumber	Int(11)	not null	Дата закінчення лікарняного
svgFilePath	Varchar(255)	not null	Шлях до SVG файлу

Були виділені всі об'єкти предметної області, спираючись на фундаментальне базове поняття функціональних залежностей. Сукупність реквізитів об'єктів предметної області відповідає вимогам нормалізації. Зв'язки між об'єктами предметної області приведені в таблиці 14.

Таблиця 14 – Зв’язки об’єктів предметної області

Головний об’єкт	Підлеглий об’єкт	Тип зв’язку	Ключ зв’язку
Група	Робоче місце	1:M	Код_групи
Група	Рівень доступу	1:M	Код_ групи
Група	Користувач	1:M	Код_ групи
Користувач	Зар. платня	1:M	Код_користувача
Користувач	Пропуск за хвороби	1:M	Код_користувача
Користувач	Перехід	1:M	Код_користувача
Перехід	Календар	M:1	Код_календара
Перехід	Кімната	M:1	Код_кімнати
Будівля	Поверх	1:M	Код_будівлі
Поверх	Кімната	1:M	Код_поверху

4 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ

4.1 Головне меню та меню адміністратора системи

Серверна частина СКУД, була розроблена за допомогою мови Java з використанням класів, системою управління базами даних було використано MariaDB – сучасний розвиток проекту СУБД MySQL. Також для написання власно обробника була використана Vaadin. Дизайн було вирішено залишити схожим на попередню версію. При цьому було додано функціоналу, повністю перероблене серверну частину та клієнтський модуль. В результаті роботи головна сторінка для входу користувача складається з двох зон, фона та форми-запрошення до вводу логіну та паролю (рис.4.1). В полі «Логін» слід ввести ім’я користувача, відповідно у полі «Пароль» – власний пароль користувача, що відповідає зареєстрованому у системі користувачу.

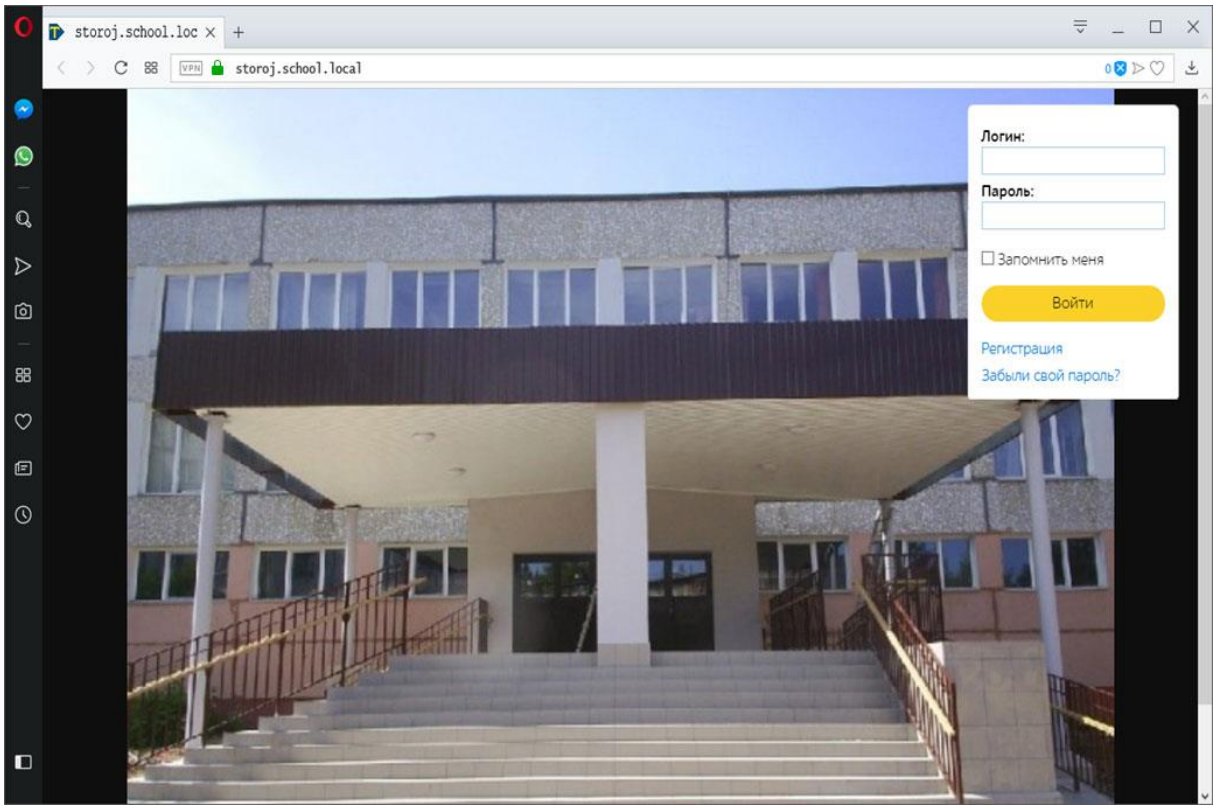

Рисунок 4.1 – Головна сторінка ІСКУД.

Важливе зауваження: Для забезпечення безпеки інформації та запобіганню зламу системи було прийняте рішення налаштовувати сервер з підтримкою SSL. Протокол SSL являє собою стандартну технологію безпеки, яка використовується для встановлення шифрованого з'єднання між веб-сервером і веб-клієнтом. SSL дозволяє безпечно обмінюватися даними завдяки ідентифікації і перевірки автентичності сервера, а також забезпечення конфіденційності і цілісності всіх переданих даних. SSL-сертифікат потрібен для того, щоб шахраї не могли перехопити особисті дані, які користувачі вводять у вас на сайті. Особисті дані – це логіни і паролі від акаунтів, номери банківських карт, адреси електронної пошти і т.д. Це означає, що SSL-сертифікат стане в нагоді на сайтах банків, платіжних систем, корпорацій, інтернет-магазинів, соціальних мереж, державних підприємств, онлайн-форумів тощо [23][1)].

SSL-сертифікат вигідний для власника сайту: так ви підтвердите, що на сайті безпечно вводити особисті дані та проявіть турботу про клієнтів. Якщо людина переживає, що конфіденційна інформація потрапить не в ті руки, він отримає додаткові гарантії. Менше ризику для користувачів, вище репутація компанії.

SSL дозволяє захистити імена, паролі та іншу важливу інформацію від дешифрування в каналі зв'язку між Web Adaptor і сервером. При використанні SSL підключення до веб-сторінок і ресурсів здійснюється по протоколу HTTPS, а не HTTP.

Тому на скріншоті можна побачити зелену позначку замка, або зелену строку, яка каже переглядачу сторінки, що інформація на цій сторінці достовірна та захищена. В нашому випадку це зелений замочок та мультідоменний сертифікат Positive SSL Multi-Domain від відомого міжнародного центру сертифікації Comodo. Мультидоменний сертифікат тому що використовуються кілька доменів, внутрішній, існуючий у локальній мережі школи,

---

[1)] [23] Що таке SSL-сертифікат и нащо він потрібен. URL: https://ssl.com.ua/info/what-is-ssl/ (дата звернення 16.11.2019).

та два зовнішніх – один використовується для інформаційного сайту школи, другий – для внутрішніх сервісів, на кшталт, цієї системи.

Вхід в систему після набору логіну з паролем здійснюється або кнопкою Enter на клавіатурі, або натисканням на посилання «Увійти».

Після входу в систему залежно від наданих прав доступу відкриється меню, яка пропонує обрати потрібні пункти для роботи. Адміністраторові надається меню, в якому доступні чотирнадцять пунктів плюс кнопка «вихід» (рис. 4.2). Інші користувачі побачать менше кнопок, в залежності від наданих прав доступу. Наприклад, працівник охорони побачить лише два модулі – Монітор подій, Управління шлагбаумом, Персонал, Відчинити двері, Пожежна сигналізація, Відеонагляд, Зміна оператора та вихід з системи.

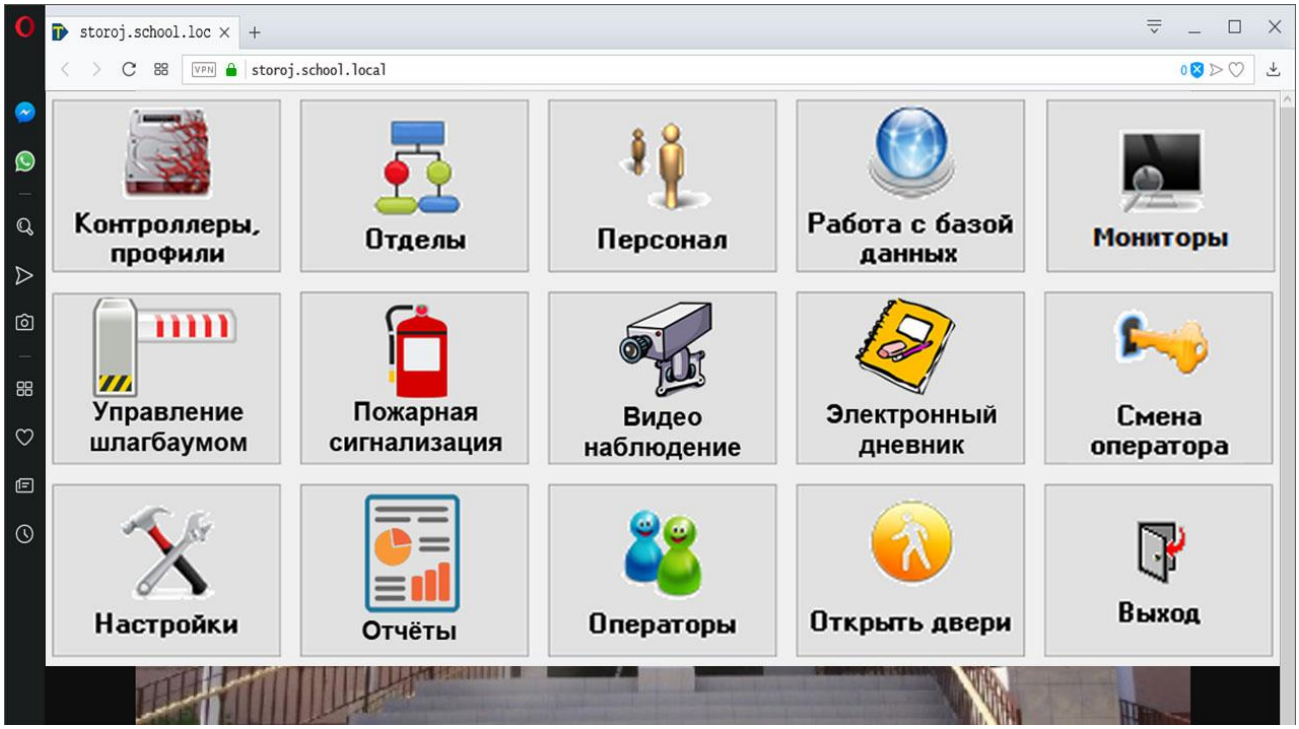

Рисунок 4.2 – Головне меню Інформаційної СКУД

Далі, в залежності від вибору пункту меню, буде відкрито відповідна сторінка, де можна обирати далі або виповняти певні дії.

4.2 Контролери та профілі

Кнопка «Контролери та профілі» логічно веде до сторінки управління власно контролерами електромеханічних замків дверей та шлагбауму, а також розкладу роботи контролерів і синхронізованих з ними профілів пропуску працівників школи, учнів, відвідувачів та технічного персоналу (рис. 4.3).

Можна прописати майже будь-який режим і розклад роботи для кожного контролера на кожній двері, наприклад, двері 1 на 2 поверсі будуть відкриті для входу відвідувачів лише з 14 до 16 години у вівторок та середу, в той самий час він буде випускати працівників та учнів у будь-який час та час доби 24/7. Аналогічно можна настроїти і будь-який контролер з цього робочого місця, скопіювати налаштування с одного контролера та встановити їх на всі або на деякі обрані.

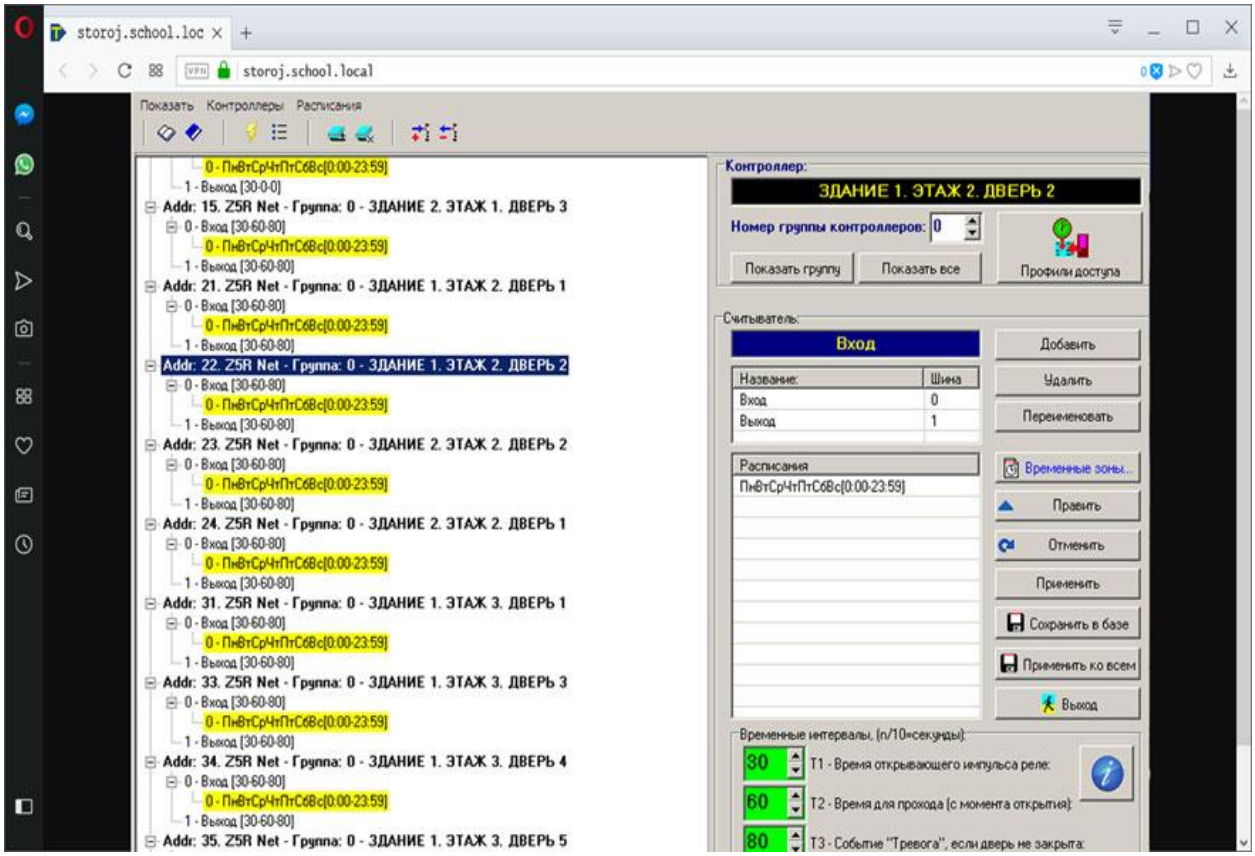

Рисунок 4.3 – Сторінка «Контролери та профілі»

Також додано можливість редагувати час, протягом якого буде відкрито електромеханічний замок на двері після піднесення RFID метки, час, який минув з моменту відкриття двері (на рис. 4.3 це показано в нижньому правому куті) і час підняття тривоги, якщо двері було не зачинено протягом, на кшталт, 80 секунд з моменту подачі сигналу на її відкриття. Модель запису «група контролерів – № будови – № поверху – № двері» було обрано для зручності програмування поведінки контролерів та буде записано в проектної документації, а також щоб мінімізувати помилки у проектуванні та програмуванні обладнання. Таким чином, фізичний контролер, який встановлюється біля двері, маючий свій апаратний код та внутрішній адрес (наприклад, 0121), буде відповідати нульовій групі (нумерація починається з 0) у будівлі №1, 2 поверху, першої двері.

4.3 Робота з меню «Персонал» та сервісними меню

Далі, адміністратору доступне меню «Персонал». В цьому меню можна дивитись, додавати, редагувати профілі і групи користувачів, надавати право проходу скрізь двері, налаштувати час та інше (рис. 4.4).

Наприклад, розділити доступ учням молодших та старших класів, щоб уникнути конфліктів, до того ж – система зможе вести облік «робочого часу» – слідкувати за спізненнями учнів або вчителів, видавати відповідь на запити батьків «Чи прийшов мій син до школи? А коли моя дитина вийшла додому?». Працівник служби охорони зможе видавати пропуск на одноразове відвідування – наприклад, для візиту когось з батьків до директора з обмеженнями руху по школі, щоб візитер попав лише туди, куди йому можна попасти, потенціального працівника до відділу кадрів, або для проходу на батьківські збори. З обов’язковим внесенням даних відвідувача у систему та попередженням візитера про обробку його персональних даних.

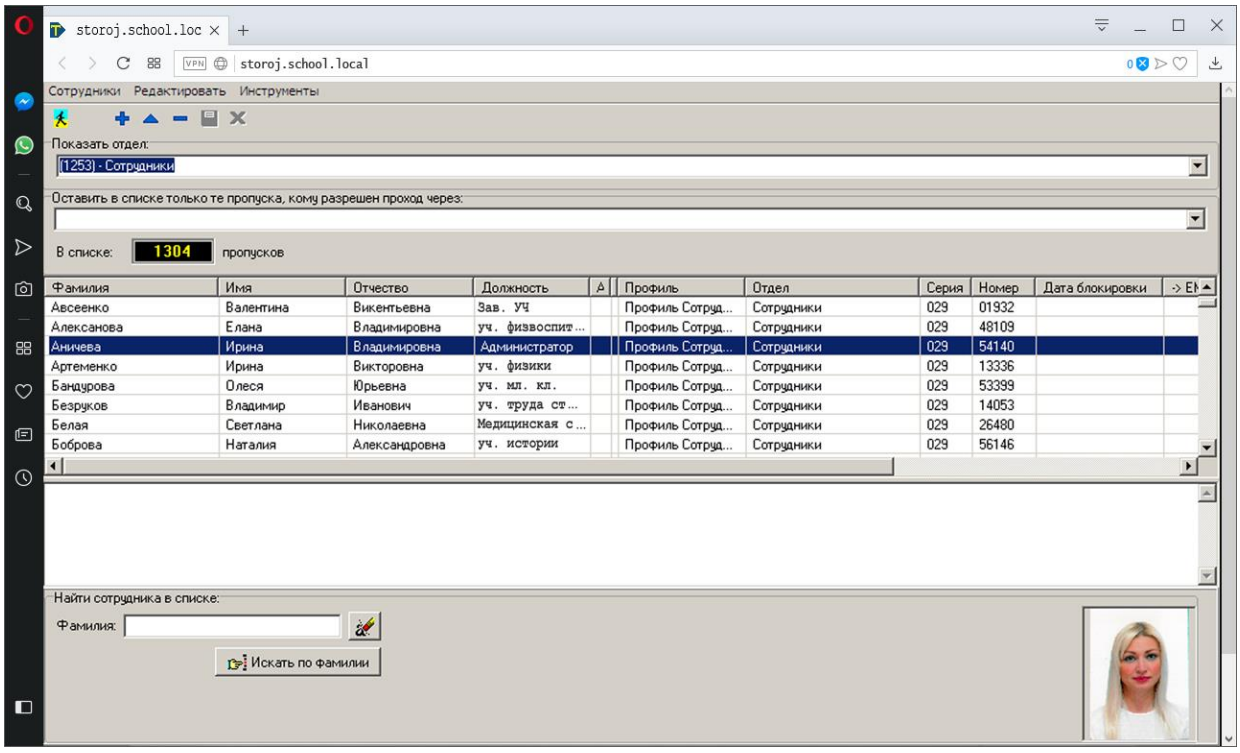

Рисунок 4.4 – Сторінка «Користувачі і групи»

У вікні цієї формі можна встановити ФІП-б візитера, працівника або учня, посаду, профіль, за яким буде працювати його RFID-картка, час дії картки, а також можливість її блокування у разі крадіжки або втрати. Номер телефону, фотографію та інші дані. Також є можливість додати марку и державний номер автівки – наприклад, для працівника постачальника продуктів до шкільної їдальні або персональних авто працівників – щоб працівник служби охорони міг вирішити – чи дозволено цьому транспортному засобу знаходитись на території школи, відкрити йому шлагбаум на в'їзді чи ні. Разові картки не мають поміток та поліграфії, можуть містити лише друковані або наклеєні примітки з номером. Але ж для зручності учнів та вчителів було розроблено дизайн картки, який було за прикладом сервісу Смарсі названо Електронним паспортом учня. Ця картка замовляється в постачальника карток, містить крім RFID мітки ще друковану інформацію: логотип, назву, адресу та телефонні номери шкільного закладу, фотографію учня (або викладача для викладачів, відповідно), прізвище, ім'я та по-батькові, штрих-код з кодовим

номером учня у електронній системі, що відрізняється від його ID – для підвищення захищеності, дату народження та дату видачі документа. Вся ця інформація завіряється підписом директора та печаткою школи (рис. 4.5).

Рисунок 4.5 – Електронний паспорт учня

За допомогою цього коду батьки та сам учень можуть зареєструватись на сайті партнерського сервісу Smarsy.com та користатись перевагами електронного щоденника та наглядом за дитиною.

Сервіс для вчителів, батьків та учнів Смарсі був розроблений для допомоги у забезпеченні обліку, контролю та аналізу успішності, відвідування та документообігу, а також для створення більш конструктивного діалогу вчителів з батьками учнів, використовуючі засобі XXI сторіччя [24][1)].

Вчителі після уроку додають до щоденника оцінки та домашнє завдання, свої помітки щодо учнів. Учні не зможуть сказати «Нам нічого не завдали», напроти, якщо хтось забув записати домашнє завдання, йому не потріб-

[1)] [24] Проект Smarsy. Безпека та інновації навчальним закладам. URL: https://smarsy.ua/html/ua/ project.html (дата звернення 18.11.2019).

но розшукувати однокласників, щоб його спитати, а достатньо скористатись смартфоном, планшетом або персональним комп’ютером будь-якого виробника з доступом до Інтернету. Батьки можуть бачити, коли дитина прийшла до школи та коли вийшла з неї, навіть у реальному часі, за допомогою інтеграції системи з сервісом в Telegram (рис. 4.6).

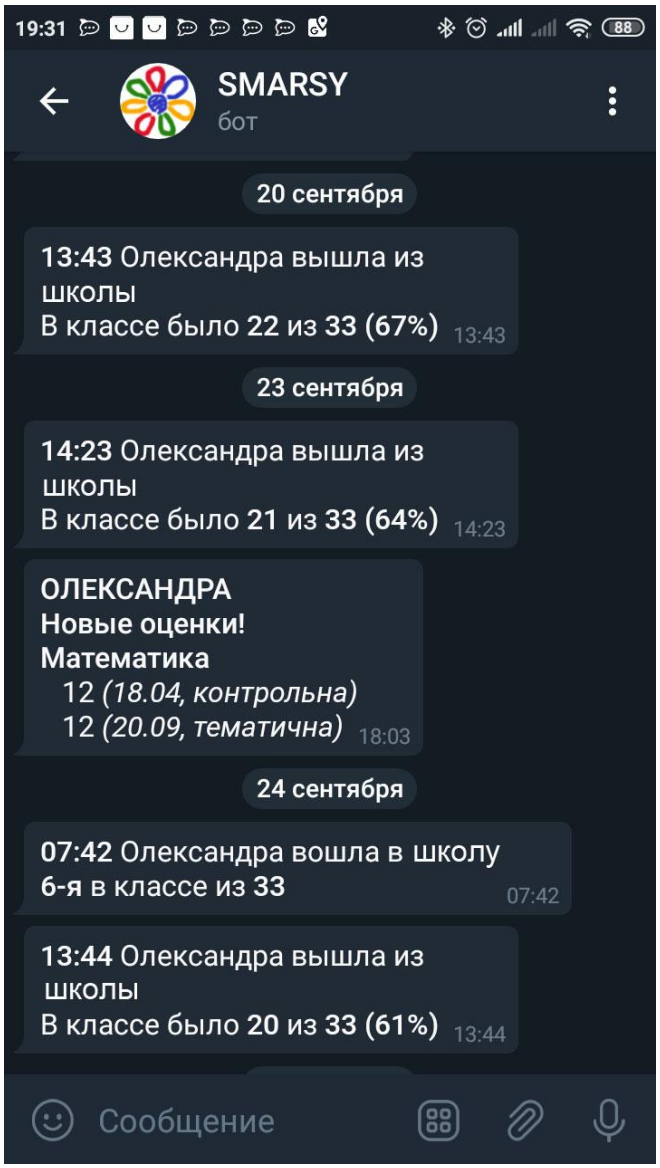

Рисунок 4.6 – Вікно телеграм-інформатора Смарсі

Можуть також бачити оцінки, список зауважень, розклад зайнять та дзвінків, оголошення та іншу корисну інформацію (рис. 4.7).

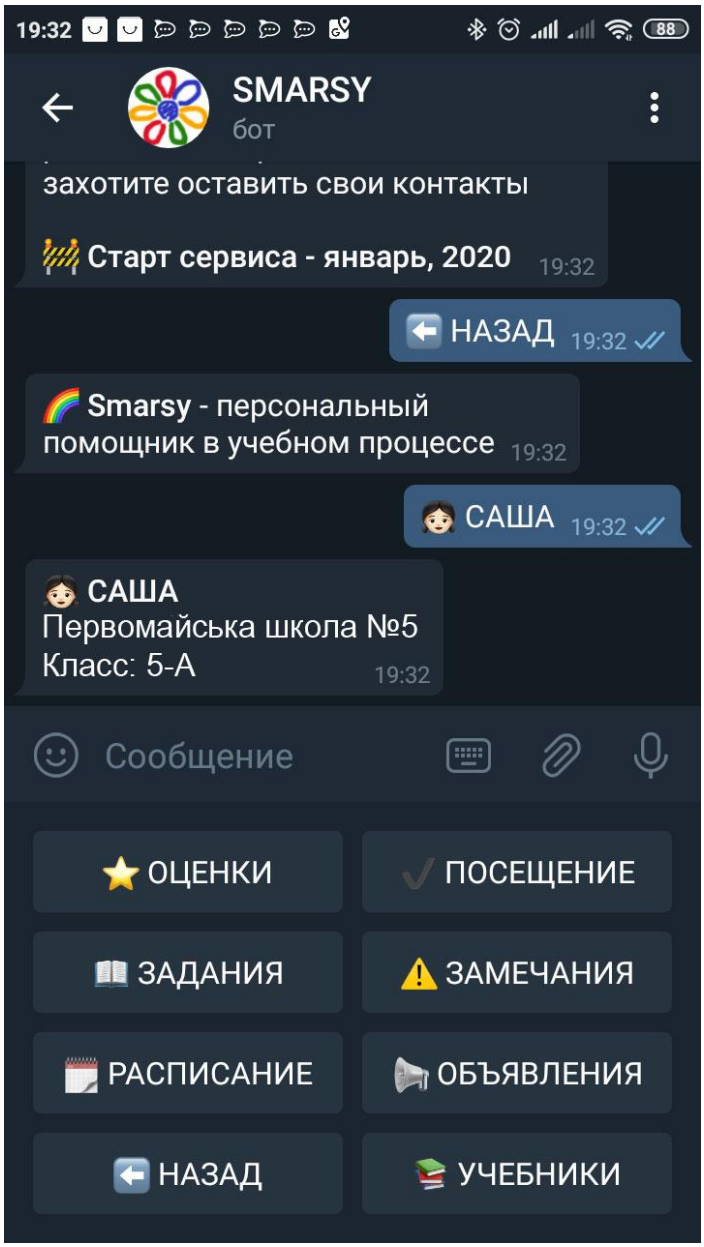

Рисунок 4.7 – Додаткові можливості системи

Далі є пункт роботи з базою даних. Це суто адміністративна функція, що включає в себе резервне копіювання, підключення резервної бази, відновлення бази з копії або тестування цілісності структури бази даних.

Пункт «Зміна оператора» зроблений для зручності зміни оператора, адміністратора, працівника служби охорони, щоб не було необхідності закривати сторінку и браузер взагалі. Швидка зміна оператора при передачі робочої зміни дозволяє не втрачати контролю за подіями.

Пункт «Налаштування» також є адміністративним пунктом, де можна налаштувати базові функції СКУД, наприклад, змінити мову інтерфейсу, ір-адресу сервера і ім’я бази даних, змінити пароль, налагодити поштовий сервер для відправлення листа з описом тривоги або різноманітних звітів.

4.4 Моніторінг подій та повноваження операторів

На сторінці «Монітори» (рис. 4.8) визначається список апаратних контролерів, на яких буде включено журналювання або аудит всіх спроб доступу а також буде з’являтись на робочому місці працівника охорони – які двері відкрилися та власник якої картки пройшов. Якщо убрати галку – можна убрати контролер зі списку дверей, за якими ведеться моніторинг.

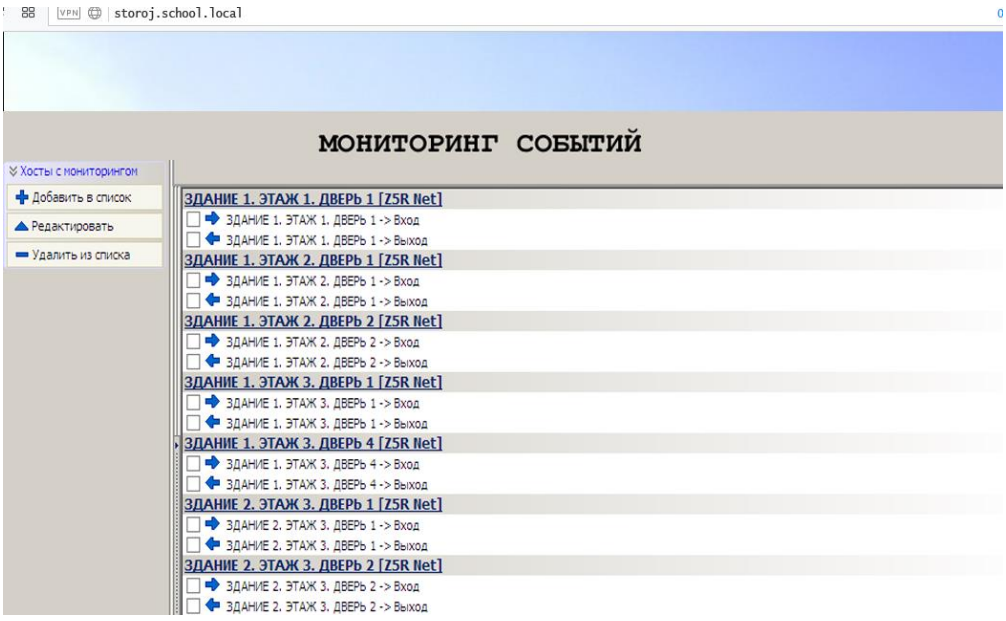

Рисунок 4.8 – Сторінка «Моніторинг подій по контролерах»

Виявилося, що ця функція дуже затребувана працівниками служби охорони, які рані власноруч перевіряли деякі важливі напрямки, а тепер можуть покластися на автоматику.

Кнопка “Оператори» визначає повноваження категорій операторів, тобто осіб, що працюють з системою – що їм можна робити, а чого ні і власне які кнопки їм показувати (рис. 4.9). Наприклад, адміністраторові доступні всі пункти меню, працівнику служби охорони закладу – лише кілька перелічених вишче, адміністративної службі моніторінгу – «Персонал», «Відділи», «Монітор подій» та «Звіти». Можна створювати, редагувати та конструювати будь-які групи та надавати їм окремі привілеї за бажанням адміністрації навчального закладу. Таким же чином можна конструювати звіти, що надаються програмою.

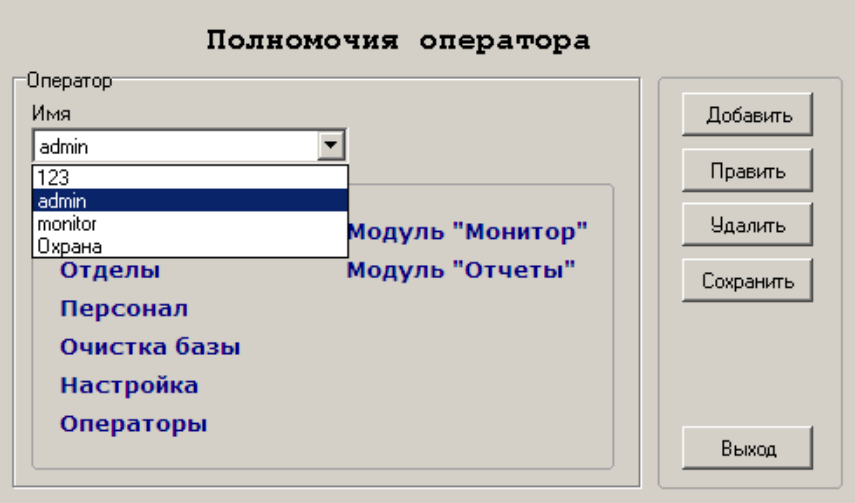

Рисунок 4.9 – Повноваження операторів

Форма дозволяє створити, обрати групу операторів, надати їм певних прав доступу або редагувати їх. Впливає на кількість кнопок переходів, що будуть доступні користувачеві.

Досить важливою є кнопка «Відімкнути двері» (рис. 4.10). У надзвичайних ситуаціях, наприклад, пожежа, затоплювання або щось інше у операторів є можливість примусового відкриття всіх або окремих дверей. За допомогою цього пункту меню можна відкрити будь-які двері, одну, групу, поверх або всі разом.

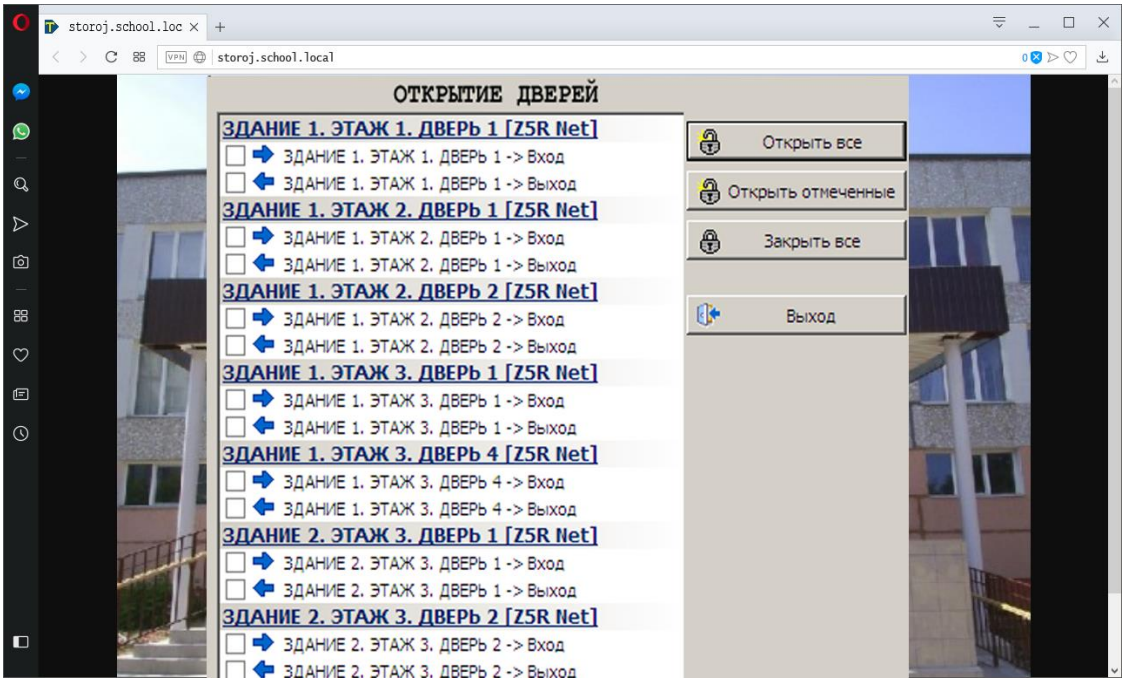

Рисунок 4.10 – «Відімкнути двері»

Також цей пункт має виконуватись автоматично при зниканні сигналу с контролера на сервері у час, коли в школі хтось є. Також дія цієї кнопки розповсюджується на шлагбаум – його контролерові віддається наказ піднятись за звільнити проїзд. Це можна використовувати на свята, День Відкритих Дверей, або при навчаннях громадської оборони, оператор або працівник службі охорони може відкрити певні двері, а після закінчення свята або навчальної тривоги – закрити всі двері, що увімкнути систему у звичайний режим роботи.

Виклик кнопки «Пожежна сигналізація» та «Відеоспостереження» визивають сторонні модулі у окремому вікні відповідно.

ВИСНОВКИ

В результаті виконаних робіт була створена гнучка архітектура системи контролю доступу, яка підтримує схему розрахунків користувачів за використання ресурсів. Реалізовано на мові Java, за допомогою Vaadin, двигуна баз даних MySQL та мови PHP, були протестовані всі використовувані архітектурні механізми. Отримані наступні результати:

– проведено системне дослідження предметної області. На його основі і на основі попередньої розробки була побудована відповідна модель;

– повністю перероблено, змодельовано, реалізовано і протестовано основні архітектурні механізми (взаємодія між всіма вбудованими об’єктами, інтеграція до системи сторонніх модулів та об’єктів, взаємодія клієнт-сервер за допомогою протоколу TCP/IP, параметризоване створення об'єктів, команди, механізми взаємодії додатків);

– розроблено архітектуру модулів програмного забезпечення і створені відповідні структурні моделі цих модулів;

– здійснено покращений захист даних, що могли бути втрачені завдяки шахраям, система працює під підписом та захистом сертифікату безпеки від надійного центру сертифікації.

Практична цінність роботи полягає в наступному:

– розроблена архітектура модулів програмного забезпечення системи контролю доступу може бути і є використана в якості бази для побудови цілого ряду систем автоматизації систем контролю доступу бюджетного рівня, але досить надійного та гнучкого;

– створені механізми можуть бути повторно використані в будь-якому проекті, який висуває відповідні вимоги;

– система може працювати на пристроях під керуванням будь-якого сімейства ОС, що можуть підключатись до локальної мережі або Інтернет, включаючи мобільні системи Apple iOS, Google Android та інші.

ПЕРЕЛІК ПОСИЛАНЬ

1. МОН України: Україна приєдналась до Декларації про безпеку шкіл. URL: https://mon.gov.ua/ua/news/ukrayina-priyednalasya-do-deklaraciyi-pro-bezpeku-shkil-mi-stali-100-oyu-krayinoyu (дата звернення 22.11.2019).

2. Довідник заступника директора школи. Безпека у школі. URL: https://www.menobr.ru/rubric/17-bezopasnost-v-shkole (дата звернення 13.08.2019).

3. Система контролю і управління доступом – Вікіпедія. URL: https://uk.wikipedia.org/wiki/Система_контролю_і_управління_доступом (дата звернення 13.08.2019).

4. ДСТУ 4000-2000 Системи тривожної сигналізації. Охоронні теле(відео)системи і системи контролювання доступу. [Чинний від 1.07.2001]. К.: Держстандарт України, 2000. 20 с.

5. Енциклопедія UML. URL: http://ooad.asf.ru/standarts/uml/spr/Architecture.asp (дата звернення 02.09.2019).

6. Про Системи управління доступом. URL: http://www.gamma.kz/gt/sud.html (дата звернення 02.09.2019).

7. Волковіцький В.Д., Волхонський В.В. Системи контролю і управління доступом. М .: Екополіс і культура, 2007. 164 с.

8. Картки-ідентифікатори, для систем контролю доступу. URL: http://www.avtolik.ru/access/systems/identifikotor.htm (дата звернення 17.08.2019).

9. Давлетханов М. Увага, чужий, 2003. URL: http://daily.sec.ru/dailypblshow.cfm?rid=5&pid=6637&pos=1&stp=50 (дата звернення 09.09.2019)

10. Принципи роботи систем контролю доступу. URL: http://www.secret-c.ru/uphp/default.php?id=41 (дата звернення 11.09.2019).

11. Ринок СКУД. URL: http://sio.su/ (дата звернення 12.09.2019).

12. Офіційний сайт Legos. URL: http://legos.ru/ (дата звернення 24.08.2019).

13. Офиційний сайт Parsec. URL: http://www.parsec.ru/ (дата звернення 24.08.2019).

14. Официальный сайт PERCo. URL: http://www.perco.ru/ (дата звернення 26.08.2019).

15. Сравнение СКУД. URL: http://biometricsecurity.ru/ (дата звернення 29.08.2019).

16. Гильманов А.А., Клименко А.Я., Странгуль О.Н., Тарасенко В.П. Карткові технології в автоматизації маркетингу. Томськ: Видавництво НТЛ, 2000. 379 с.

17. Аналітика в камерах Hikvision: огляд смарт-камер. URL: https://hikvision.org.ua/ru/articles/analitika-v-kamerah-hikvision-obzor-smart-kamer (дата звернення 29.09.2019).

18. Алла Рудь. Яку ОС обрати для роботи сервера. URL: https://hyperhost.ua/info/kakuyu-os-vyibrat-dlya-rabotyi-servera/ (дата звернення 02.10.2019).

19. Жданов А.А. Сучасний погляд на ОС реального часу. URL: http://asutp.interface.ru/articles/display_topic_threads.asp?ForumID=13&TopicID=299 (дата звернення 04.10.2019).

20. Apache vs Nginx: обираємо оптимальний веб-сервер. ITSource. URL: https://itsource.com.ua/blog/apache-vs-nginx-vy-biraem-optimal-ny-j-veb-server/ (дата звернення 04.10.2019).

21. Введення до Vaadin. URL: https://www.codeflow.site/ru/article/vaadin (дата звернення 12.10.2019).

22. Юрій Артамонов. Vaadin Flow – дивовижний олень. URL: https://habr.com/ru/company/haulmont/blog/416893/ (дата звернення 12.10.2019)

23. Що таке SSL-сертифікат и нащо він потрібен. URL: https://ssl.com.ua/info/what-is-ssl/ (дата звернення 16.11.2019).

24. Проект Smarsy. Безпека та інновації навчальним закладам. URL: https://smarsy.ua/html/ua/project.html (дата звернення 18.11.2019).