

# БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

**РОЗРОБКА СИСТЕМИ КОНТРОЛЮ  
УПРАВЛІННЯ ДОСТУПОМ КАФЕДРИ ЗАХИСТУ  
ІНФОРМАЦІЇ НАЦІОНАЛЬНОГО  
УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»**

Студента групи КБз-21

Савіцького Д.Г.

Керівник

д.т.н., проф. Опірський І.Р.

**Мета роботи:** проаналізувати сучасні системи контролю та управління доступу, розробити політику безпеки, та на основі цього запроектувати СКУД для приміщень 2 кафедри захисту інформації Національного Університету «Львівська політехніка».

**Для досягнення поставленої мети вирішуються наступні завдання:**

- 1) Аналізується стан злочинності в Україні;
- 2) Аналізується стан злочинності в державних структурах;
- 3) Аналізуються та досліджуються методи боротьби зі злочинністю;
- 4) Розробляється постановка завдання для проекрованої СКУД кафедри захисту інформації НУ «ЛП»;
- 5) Визначаються основні комплектуючі СКУД кафедри захисту інформації НУ «ЛП»;
- 6) Визначаються та досліджуються основні вимоги до системи;
- 7) Проводиться розрахунок пропускної здатності системи та вибір обладнання;
- 8) Досліджуються системи ідентифікації та програмного забезпечення та визначаються найбільш оптимальні;
- 9) Проводиться розрахунок автономного живлення СКУД;
- 10) Визначається основна політика безпеки та проблематика її використання в СКУД кафедри захисту інформації НУ «ЛП»;
- 11) Представляються основні проектні рішення СКУД;
- 12) Аналізуються основні переваги та недоліки розробленої системи;
- 13) Приводяться рекомендації щодо підвищення якості роботи СКУД в межах кафедри захисту інформації та в системі глобальної СКУД НУ «ЛП».



**Об'єктом дослідження є методи захисту в системах контролю доступу та політика безпеки.**

**Предмет дослідження – проектні рішення щодо створення СКУД кафедри захисту інформації Національного університету «Львівська політехніка».**

**Практична цінність роботи полягає в тому, що:**

1. Проектування СКУД, а також визначення основних завдань дозволило запроєктувати та визначити прототип політики безпеки кафедри захисту інформації, який досягається зарахунок використання запропонованих нами параметрів політики безпеки, а саме: таблиці користувачів; рівня доступу; таблиці дозволених рівнів доступу; тимчасових зон; наявності святкових днів; режиму заборони повторного проходу; режиму заборони виходу. Використання запропонованих параметрів, дозволило представити прототип політики безпеки проектованої СКУД на прикладі викладачів кафедри ЗІ, студентів кафедри ЗІ, працівників ЗРРЦЗІ та інших відвідувачів і персоналу, що вказані в роботі. Дана політика безпеки може використовуватись, як прототип майбутнім політикам безпеки не тільки корпусу але і всього Університету.

2. Аналіз завдань для проектованої системи дозволив визначити обладнання для проектування СКУД. В якості ПЗ визначено «FortNet», в якості управляючого контролера обрано контролер ABC-E- FortNet, а в якості модулів віддаленого управління доступу ARCP FortNet, в якості турнікету обрано Бізант-5. Це та інше передбачене в роботі обладнання дозволило вперше створити проект СКУД для кафедри захисту інформації НУ «ЛП», що відповідає поставленому завданню та підвищують захищеність матеріальних цінностей корпусу, і дозволяють проводити моніторинг і аудит його відвідувачів;

3. Проектні рішення, розроблена політика безпеки, математичні розрахунки живлення, а також оптимальний вибір обладнання показали нам беззаперечні переваги розробленої системи, проте дозволило й визначити деякі недоліки, що в свою чергу надало подальшого розвитку у створенні рекомендацій, які можуть використовуватись проектними фірмами чи проектантами, щодо проектування таких видів СКУД не тільки в одному корпусі НУ «ЛП», але і при глобальному проектуванні СКУД всього університету.

# Аналіз злочинності в Україні та методи протидії їм

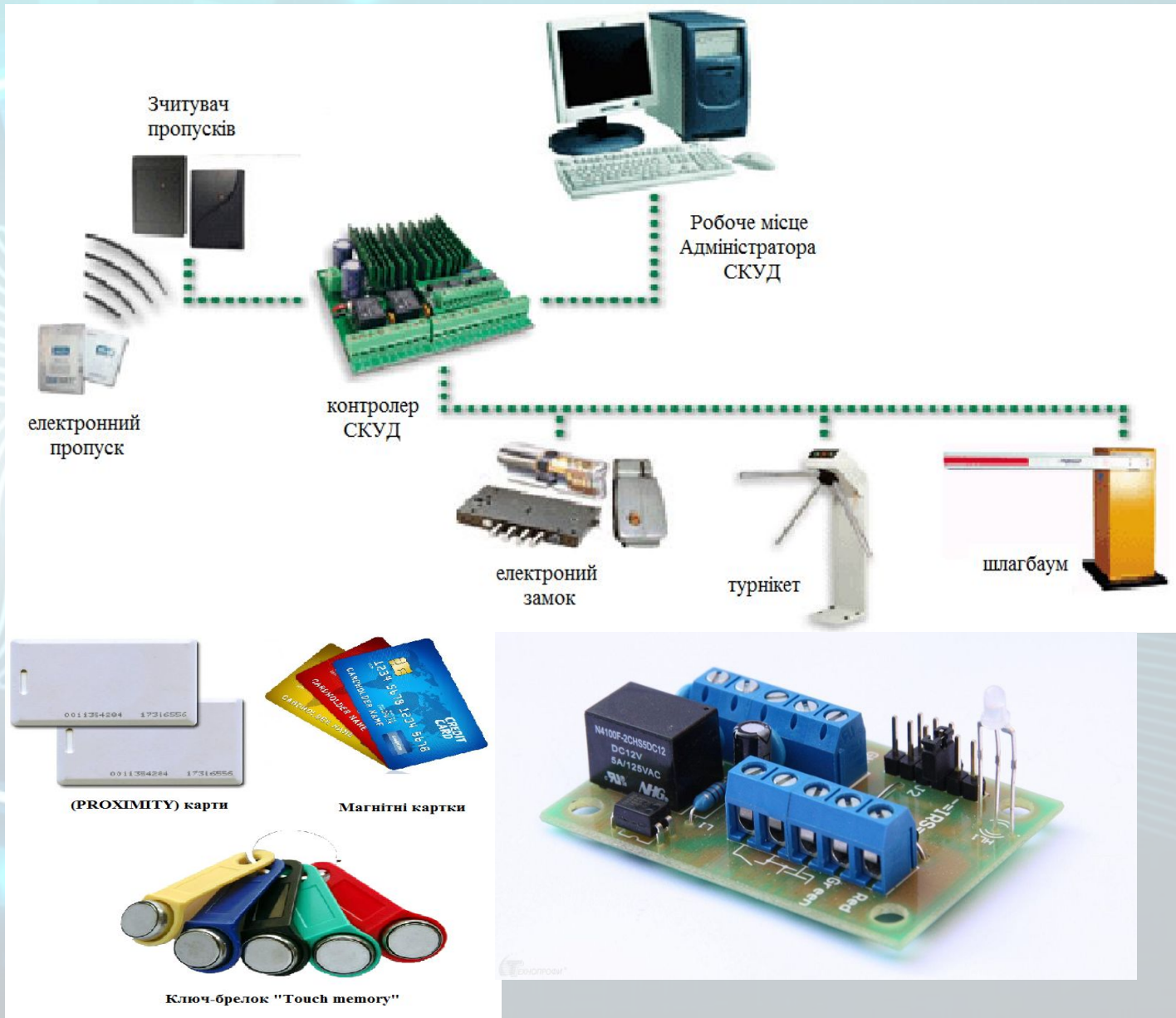


## Основні фізичні методи протидії злочинності

- Система охоронної сигналізації
- Системи відеоспостереження
- Система контролю управління доступом (СКУД)



# Основні складові для системи контролю та управління доступом



# Основні рішення за вибором обладнання для СКУД

Основним обладнанням проектом передбачено використання:

## Верхнє програмне забезпечення:

- «FortNet».

Управляючі контролери:

- FORTNET ABC V 12.3 для кількості контролерів до 64 шт з кількістю вбудованих карток – 65000.

Модулі віддаленого управління точкою проходу:

- ARCP;

Модуль релейних виходів:

- RRM-8;

Роторні турнікети:

- Турнікет Бізант-5 ;

Електронний замок для дверей:

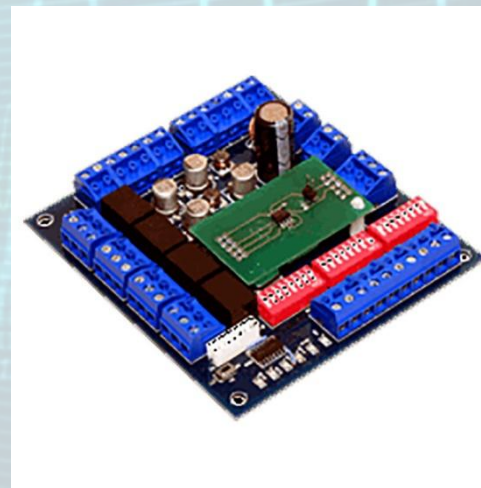
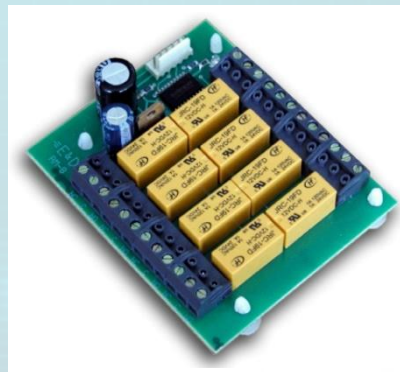
- ATIS AS-133NC;

Зчитувач для карт:

- СШКЛ-01-;

Або

- Бізант-5 СПКТ;





# Вибір системи ідентифікації для проектнової СКУД

Повна назва вищого навчального закладу	
Серія номер AA №00000000	Місце для фотокартки
Виданий ЧЧ місяць РРРР	
Дійсний до ЧЧ місяць РРРР	
Прізвище, ім'я, по батькові	
Прізвище Ім'я По батькові	
Назва факультету (відділення), структурного підрозділу, Форма навчання.	
Група	Місце для штрих-коду
Номер групи	
Посада <i>Місце</i> Прізвище	



Основною проблемою при проектуванні системи, є питання визначення. Як відомо існують декілька видів ідентифікації користувачів в системі, в нашому випадку ми мали б обрати найбільш придатну на наш розсуд систему ідентифікації – штрих-кодову. Хоч цей вибір не є дивним, оскільки переважна кількість відвідувачів корпусів університету є саме студенти, то виробити кожному з них радіо брелок, або rfid-мітку було б надто складно і дорого. Проте в кожного студента завжди присутній (або має бути присутній) студентський квиток, в якому вже при виготовленні прописаний власний штрих-код, який ми можемо використати в нашій системі. Та і виготовити пластикові викладацькі посвідчення, на нашу думку було б правильно і для працівників і персоналу політехніки, де так само можна було б при виготовленні нанести ідентифікатор-штрих-код. Проте, доцільніше при виготовленні студентських забезпечити їх і електронною міткою, а саме проводити друк студентських квитків та посвідчень вже на готовій проксиміті-карті, що в свою чергу підвищить рівень захищеності нашої системи. Ціна їх є невисокою (від 10грн), і їхнє використання на наш погляд буде доцільнішим.

# Розрахунок ББЖ та акумуляторів для безперебійної роботи

Зони ББЖ, прийняті в проекті визначимо таким чином:

- 1- СКУД Кафедри «Захисту інформації» (201-208 аудиторії+ додатковий вхід-вихід);
- 2- СКУД Кафедри «Захисту інформації» (вхід+208-214 аудиторії);
- 3- СКУД кафедри і вхід в ЗРНЦЗІ;
- 4- Приміщення кафедри 20 корпусу;

Приклад розрахунку: 1 зона – СКУД Кафедри «Захисту інформації» (3 турникета, 24 зчитувачів, 12 мікроконтролерів, 9 електрозамків)

Тип прибору	Кількість	I (чергове), мА	I (трєв.), мА	Загальне I (чер. .спож.), мА	Загальне I (трєв.спож), мА	тип ББЖ
<b>Розрахунок</b>						
Контроллер ARCP	12	120	120	1440	1440	Блок безпереб йного живлен ня ВВГ-121 0/8 12В, 10А  2 ББЖ, 30А/г
Зчитувач СПКТ-01	24	80	80	1920	1920	
Турникет Бізант-5	3	1500	2400	4500	7200	
Електрозамок	9	280	280	2520	2520	
Разом:				10380	13080	
Час роботи				5 год 45хв	4 год 35хв	

Отже проектом передбачено встановлення 5 ББЖ 10А з акумуляторами 30А/г.



# Параметри політики безпеки розробленої СКУД

- 1) Група 1- Викладачі та лаборанти кафедри ЗІ;
- 2) Група 2- Лаборанти та допоміжний персонал кафедри;
- 3) Група 3- Студенти кафедри ЗІ;
- 4) Група 4- працівники ЗРНЦЗІ;
- 5) Група 5- Ректорат, дирекція, завідувач кафедри.
- 6) Група 6- Гості/інші студенти;

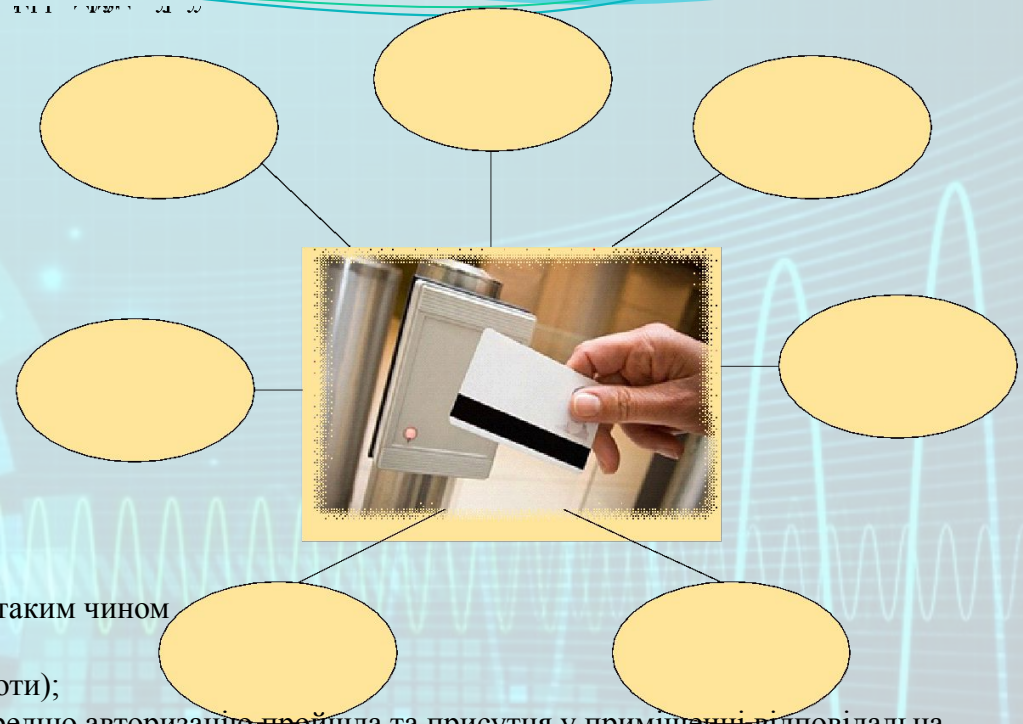
І розіб'ємо наше СКУД на такі зони входу-виходу:

- Зона 1- Вхідні-вихідні турнікети;
- Зона 2- Серверна СКУД;
- Зона 3 Навчальні аудиторії та викладацька кафедри;
- Зона 4- РСО;
- Зона 5-ЗРНЦЗІ;
- Зона 6-Допоміжні приміщення кафедри;
- Зона 7-Приміщення завідувача кафедри;

Політика доступу до зон в цьому випадку буде визначатись таким чином

- А) Доступ цілодобовий у всі дні;
  - Б) Доступ в робочий час з 7:00 до 20:00 ( з понеділка до суботи);
  - Б1) Доступ в робочий час з 7:00 до 20:00 за умови, що попередню авторизацію пройшла та присутня у приміщенні відповідальна особа (програмується на контролері);
  - В) Тимчасовий доступ в певні години наприклад, для прибиральників вхід буде доступний з 7 по 11, а для студентів груп тільки у відведені під пари години. Зокрема під час перерви доступ до аудиторій буде припинятися. Даний тип піддоступа матиме окремі налаштування для прибиральників, студентів, персоналу корпусу.
- Наприклад В1-доступ прибиральників до аудиторій та викладацької з 7:00 по 8:30 і після 17:00.  
В2-доступ студентів до аудиторій, тільки під час пари з коридором до 5х при запізненні та заборону доступу до викладацької.
- Г) Повна заборона;
  - Д) Тимчасовий пропуск (гостьовий допуск);

Гості кафедри та інші студенти матимуть повну заборону для доступу до приміщень кафедри крім входу, проєктом передбачено, що в таких випадках для перебування сторонніх осіб у приміщеннях має бути обов'язково інша особа хто має відповідний допуск. Доступ до зони РСО окремо програмується на контролері з метою відсіяти осіб, хто не має допуску до державної таємниці, а також унеможливити потрапляння у середину осіб, якщо перед тим не було авторизовано відповідальну особу (доступ Б1), що знаходиться у середині.



# Політика безпеки розробленої СКУД кафедри захисту інформації

Перелік проєктованих зон доступу	Група 1 Викладачі та лаборанти кафедри ЗІ	Група 2- допоміжний персонал корпусу;	Група 3 Студенти кафедри ЗІ	Група 4-працівники ЗРНИЦЗІ;	Група 5- Ректорат, дирекція, завідувач кафедри.	Група 6- Гості/інші студенти;
Зона 1- Вхідні-вихідні турнікети;	Б	Б	Б	Б	А	Д
Зона 2- Серверна СКУД;	Г	Г	Г	Г	А	Г
Зона 3 Навчальні аудиторії та викладацька кафедри;	Б	В1	В2	Г	А	Г
Зона 4- РСО;	Б1	Г	Г	Б1	Б1	Г
Зона 5- ЗРНИЦЗІ;	Г	Г	Г	Б	А	Г
Зона 6- Допоміжні приміщення кафедри;	Б	В1	Г	Г	А	Г
Зона 7- Приміщення завідувача кафедри;	Б1	Б1	Г	Б1	Б1	Г





# Рекомендації щодо підвищення якості роботи СКУД в межах корпусу та в системі глобальної СКУД НУ"ЛП"

- 1) З метою підвищення рівня захищеності і моніторингу корпусу НУ «ЛП», рекомендовано використання СКУД в взаємодії з іншими системами захисту інформації, наприклад, системою відео нагляду чи охоронної сигналізації, що ще більше підвищить захист матеріальних цінностей корпусу.
- 2) З метою унеможливити підробку ідентифікаторів рекомендовано в майбутньому змінити систему ідентифікації на біометричну;
- 3) Для захисту лабораторій або приміщень з дорогим обладнанням рекомендується створення додаткової зони в політиці безпеки для цього приміщення з використанням додаткового обладнання для СКУД;
- 4) Для розширення СКУД в межах всіх корпусів Національного університету «Львівська політехніка» обов'язковим є використання однакового ПЗ, в нашому випадку «ForNet».
- 5) Окрім того не рекомендується створення Баз даних окремо кожних корпусів, оскільки пересування викладачів і студентів відбувається не в межах одного корпусу, тому бажано представити одразу ж загальну базу даних на централізованому сервері, з дублюванням її локально у кожному корпусі, наприклад для підвищення швидкості обробки даних, для протидії зміни даних чи видалення, і що, дуже важливо, при втраті зв'язку з основним сервером;
- 6) З метою забезпечення працездатності СКУД при вимкненні світла рекомендується використовувати обладнання яке працюватиме від 12В постійної напруги, це дозволить при проектуванні і монтажі передбачити використання спеціальних блоків живлення з акумуляторними батареями, що по-перше забезпечать неперервність роботи системи при перепадах напруги та дозволять працювати системі деякий час від автономного живлення;
- 6) Для забезпечення роботи СКУД і оперативності налаштування рекомендується операторам Баз Даних СКУД або обслуговуючому персоналу тісно співпрацювати з внутрішніми відділами «Львівської політехніки»: відділом кадрів, ректоратом, диспетчерською, деканатами тощо. Це дозволить своєчасно вносити всі зміни в базу даних і гнучко переробляти відповідні модулі політики безпеки для студентів і викладачів;
- 7) Для зменшення ризиків пов'язаних з потраплянням сторонніх людей у режимно-секретні відділи, в приміщення з цінним обладнанням, в приміщення які мають цінність для НУ ЛП або інші важливі приміщення при побудові політики безпеки передбачати підтримку функції обмеження доступу відвідувачів без супроводу ("правило двох осіб");
- 8) для більш зручного користування системою в моменти пов'язані з надзвичайними ситуаціями, або ситуаціями, які не передбачені політикою безпеки або у форс-мажорах бажано встановлювати в приміщеннях охорони корпусів спеціальні виносні пульти, які дозволятимуть провести дистанційне відключення/відкривання турнікетів чи магнітів в конкретних зонах.



1. Аналіз завдань для проекрованої системи дозволив визначити обладнання для проектування СКУД. В якості ПЗ визначено «FortNet», в якості управляючого контролера обрано контролер ABC-E- FortNet, а в якості модулів віддаленого управління доступу ARCP FortNet, в якості турнікету обрано Бізант-5. Це та інше обладнання цілком задовольняє поставленому завданню.

2. Аналіз проблематики визначення ключів-ідентифікаторів дозволив розробити два варіанта визначення користувача: перший – більш економічніший, але з можливістю компрометації або підробки – використання як ключ-ідентифікатор штрих-коду, що міститься на студентських квитках, а також може розміщатись на пластикових посвідченнях викладачів і персоналу, і другий – використання проксиміт-карт, з вбудованим радіочастотним ключом. Причому проектом пропонується в процесі виготовлення проксиміт-карт для більшої зручності, використовувати тло карти для виготовлення студентських квитків, викладацьких посвідчень тощо.

3. На основі математичних розрахунків проектом передбачено використання автономного живлення для системи, що складається з блоків живлення 10А, що дозволить безперебійно працювати системі у випадку перепадів напруги та акумуляторів на 30 А/Г (5шт) у випадку втрати світла на протязі 4-5 годин автономної роботи.

4. Проектування СКУД, а також визначення основних завдань дозволило запроектувати та визначити прототип політики безпеки приміщень кафедри захисту інформації, який досягається використанням запропонованих нами параметрів політики безпеки, а саме: таблиці користувачів; рівня доступу; таблиці дозволених рівнів доступу; тимчасових зони; наявності святкових днів; режиму заборони повторного проходу; режиму заборони виходу. Використання запропонованих параметрів, дозволило представити прототип політики безпеки проекрованої СКУД на прикладі викладачів кафедри ЗІ, студентів кафедри ЗІ, працівників ЗРРНЦЗІ та інших відвідувачів і персоналу, що вказані в роботі. Дана політика безпеки може використовуватись, як прототип майбутнім політикам безпеки не тільки кафедри але і всього Університету.

**Дякую за увагу!**