МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютеризованих систем управління

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____Литвиненко О.Є.
"_____"_____2020 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"МАГІСТР"

Тема: Системи контролю і управління доступом до об'єктів, що охороняються

Виконавець: : Царенко В. В.

Керівник: Масловський Б. Г.

Нормоконтролер: Тупота Є. В.

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет Кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп’ютеризованих систем управління
Спеціальність 123 «Комп'ютерна інженерія»
(шифр, найменування)

Освітньо–професійна програма «Системне програмування»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____Литвиненко О.Є.
«____»_____2020 р

ЗАВДАННЯ
на виконання дипломної роботи
Царенко Владислава Валерійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи: Системи контролю і управління доступом до об’єктів, що охороняються
затверджена наказом ректора від «07» вересня 2020 р. № 1410/ст
2. Термін виконання роботи: з 05.10.2020 р. по 13.12.2020 р.
3. Вихідні дані до роботи: Дослідити існуючі комплексні системи та сформувати вимоги до модернізованої системи. Модернізувати існуючі схеми мереж в СКУД.
4. Зміст пояснювальної записки:
1) Аналіз існуючих систем контролю і управління доступом
2) Система контролю і управління доступом до об’єктів
3) База даних та реалізація програмного забезпечення

5. Перелік обов'язкового графічного (ілюстративного) матеріалу:
1) Архітектура СКУД
2) Модернізована схема мережі
3) Структурна схема організації зв’язку в СКУД
4) Логічна модель бази даних
5) Головна екранна форма бази даних в СКУД

6. Календарний план-графік

№ п/п	Завдання	Термін виконання етапів	Примітка
1	Ознайомлення з постановкою завдання дипломної роботи.	05.10.2020 – 06.10.2020	
2	Вивчення спеціальної літератури і технічної документації.	07.10.2020 – 10.10.2020	
3	Написання розділу 1.	11.10.2020 – 22.10.2020	
4	Вибір методики проектування СКУД.	23.10.2020 – 24.10.2020	
5	Написання розділу 2.	25.10.2020 – 10.11.2020	
6	Модернізація схеми мережі та організація зв’язку в СКУД.	11.11.2020 – 13.11.2020	
7	Написання розділу 3.	14.11.2020 – 02.12.2020	
8	Оформлення пояснювальної записки.	03.12.2020 – 04.12.2020	
9	Підготовлення графічного демонстраційного матеріалу.	05.12.2020 – 07.12.2020	

7. Дата видачі завдання: 05.10.2020 р.

Керівник дипломної роботи _____ Масловський Б. Г.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Царенко В. В.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Системи контролю і управління доступом до об’єктів, що охороняються»: 81 сторінка, 24 рисунки, 17 таблиць, 23 літературних джерел.

СИСТЕМА КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ, ІНФОРМАЦІЙНА СИСТЕМА, ЗАХИСТ ІНФОРМАЦІЇ, БАЗА ДАНИХ, МОДЕЛЬ ЗАГРОЗ І ПОРУШНИКА

Дипломна робота присвячена актуальній тематиці впровадження системи контролю і управління доступом на об’єкти, що охороняються, задля підвищення рівня інформаційної безпеки.

Об’єкт дослідження – процес забезпечення інформаційної безпеки.

Предмет дослідження – система контролю і управління доступом до об’єкта, що охороняється.

Методи дослідження – оцінка ризиків інформаційної безпеки, модель загроз, побудова моделі порушника, методи порівняння, дослідження та аналізу.

Мета дипломної роботи – впровадження системи контролю та управління доступу (СКУД) на об’єкт, що охороняється.

Розроблені схемні та структурні рішення можна застосовувати на об’єктах, які вимагають захисту та забезпечення безпеки інформації та впровадження систем контролю та управління доступом.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

ПД – персональні дані.

СКУД – система контролю і управління доступом.

ACS (англ. *Acess Control System*) – система контролю і управління доступом.

RFID (англ. *Radio Frequency IDentification*) – радіочастотна ідентифікація.

RS-232 – стандарт фізичного рівня для асинхронного інтерфейсу.

RS-485 – стандарт фізичного рівня для асинхронного інтерфейсу.

КПП – контрольно-пропускний пункт.

DAC (англ. *Discretionary access control*) – дискреційний контроль доступу.

MAC (англ. *Mandatory*) – обов'язковий контроль доступу.

RBAC (англ. *Role Based Acess Control*) – рольовий контроль доступу.

САУ – система автоматичного управління .

ПЗ – програмне забезпечення.

АС – автоматизована система.

БД – база даних.

ІБ – інформаційна безпека.

ІС – інформаційна система.

КІ – конфіденційна інформація.

АРМ – автоматизоване робоче місце.

ВСТУП

Предметом захисту в будь-якій інформаційній системі є інформація. Поняття інформація визначається, як відомості про осіб, предмети, факти, події, явища і процеси, незалежно від форми їх подання.

Основними особливостями інформації є те, що вона не матеріальна, її параметри неможливо виміряти фізичними методами і приладами, і те, що інформація зберігається і передається за допомогою матеріальних носіїв. Людина здатна отримати інформацію тільки тоді, коли вона записана на один з матеріальних носіїв: мозок людини, машинні носії, паперовий носій, електромагнітні і звукові хвилі і інші носії інформації.

Інформація має перелік властивостей. З точки зору інформаційної безпеки найбільш значущими є конфіденційність, доступність, цілісність. Так само важливою властивістю є цінність, важливість для власника інформації.

Під інформаційною безпекою розуміється стан захищеності інформаційної сфери (підприємства, організації, суспільства, держави) від внутрішніх і зовнішніх загроз.

Під конфіденційністю розуміється стан інформації, при якому володіння інформацією здійснюється певним колом осіб, встановленим власником інформації.

Під доступністю розуміється стан інформації, при якому особи, які мають право доступу, можуть реалізувати свої права.

Під цілісністю розуміється стан інформації, при якому стан інформації змінюється тільки особами, які мають права на внесення змін.

Під цінністю розуміється стан інформації, при якому власник може отримати певні переваги від володіння інформацією.

Основна інформація, всіх рівнів конфіденційності, в сучасних організаціях, на підприємствах збирається, зберігається, обробляється і передається в комп'ютерних системах. Все менше число організацій в даний час використовує

централізовані системи, зараз найбільш затребувані розподілені комп'ютерні системи.

Зазначені комп'ютерні системи включають в себе велику кількість різних інформаційних систем і програмних продуктів. Кожен компонент може мати в собі вразливість, яка є загрозою для безпеки комп'ютерної системи в цілому. Передача інформації в розподілених системах відбувається по каналам зв'язку, часто не належить організації, за якими зловмисник може отримати доступ до ресурсів організації.

Для запобігання втрат пов'язаних з витоком інформації, несанкціонованих і ненавмисних дій в організаціях проводять діяльність із захисту інформації. Ця діяльність ґрунтується на програмі інформаційної безпеки організації. Дана програма описує вимоги і принципи систем захисту інформації. Система захисту включає в себе правові норми, технічні, програмні та криптографічні засоби, методи і механізми забезпечення інформаційної безпеки. Вся діяльність щодо забезпечення безпеки спрямовані на одночасне забезпечення критеріїв конфіденційності, цілісності та доступності.

Актуальність проблеми, яка розглядається в рамках дипломної роботи, обумовлена необхідністю захисту інформації, розробкою інженерних і організаційних заходів з протидії можливим загрозам і порушникам.

Одним з таких заходів є створення такої системи контролю доступу, яка зможе забезпечити повну інформаційну безпеку безпосередньо для даної організації. Цього можна досягти за допомогою застосування сучасної системи контролю і управління доступом (СКУД).

Створення такої системи спрямоване на модернізацію існуючої політики безпеки і пояснюється тим, що в сучасних реаліях на перший план виходять інформаційні відносини різного змісту.

На сьогоднішній день конфіденційна інформація є одним з найцінніших джерел, у зв'язку з чим, в сучасному інформаційно-комунікаційному світі до захисту персональних даних (ПД) пред'являються високі вимоги, так як крадіжка даної інформації перетворюється в загальносвітову проблему.

В Україні органи державної влади оперативно реагують на існуючу проблематику. Неухильне виконання всіх вимог забезпечує захист всіх ПД працівників підприємств і організацій, а також комерційних партнерів і клієнтів. Так як під поняття ПД потрапляє вся інформація про людину, це означає, що створення спеціального захисту ПД необхідно для будь-якої установи або організації. Невиконання існуючих положень тягне за собою судовий розгляд, а винні особи можуть бути притягнуті як до адміністративної, так і до кримінальної відповідальності.

Для функціонування інформаційної структури організації проблема грамотного забезпечення захисту інформації є однією з найважливіших.

Крім розробки спеціального програмно-апаратного комплексу захисту ПД, необхідним аспектом розробки інформаційної безпеки також є існуючі норми і правила.

Контроль доступу – це метод безпеки, який регулює, хто або що може переглядати або використовувати ресурси в обчислювальному середовищі. Це фундаментальна концепція безпеки, яка зводить до мінімуму ризик для бізнесу або організації.

Подібна система забезпечує доступність і конфіденційність фізичних та інформаційних об'єктів підприємства. Основна концепція побудови систем контролю і управління доступу – наявність диспетчера доступу, який здійснює розмежування доступу до всіх об'єктів доступу, відповідно до заданих правил розмежування, і фіксацію всіх звернень суб'єктів до об'єктів доступу. Основними вимогами до реалізації диспетчера доступу є:

- вимога повноти контрольованих операцій, згідно з яким перевірці повинні піддаватися всім операціям всіх суб'єктів над усіма об'єктами системи; обхід диспетчера передбачається неможливим;
- вимога ізольованості, тобто захищеності диспетчера від можливих змін суб'єктами доступу в цілях впливу на процес його функціонування;
- вимога формальної перевірки правильності функціонування;
- мінімізація використовуваних диспетчером ресурсів.

Для повноважної моделі характерна наявність для кожного об'єкта грифа секретності, вираженого числовим значенням і наявністю рівня допуску для кожного суб'єкта доступу. Допуск до об'єкта в цій моделі суб'єкт отримує тільки в разі, коли у суб'єкта значення рівня допуску не менше значення грифа секретності об'єкта.

Гідність повноважної моделі – відсутність необхідності зберігати великі обсяги інформації про розмежування доступу. Кожному об'єкту доступу необхідно зберігати лише присвоєне значення грифа секретності, а кожному суб'єкту – рівень доступу.

Метою даної випускної кваліфікаційної роботи є впровадження системи контролю та управління доступу (СКУД) на об’єкт, що охороняється.

При написанні роботи були поставлені наступні задачі:

1. Виконати аналіз існуючих систем контролю і управління доступом. Представити сучасні різновиди систем СКУД, визначити актуальність їх впровадження;

2. Виконати розробку моделі загроз і порушника для досліджуваного об’єкта. Представити методику розрахунку для аналізу ризиків та довести актуальність застосування системі контролю і управління доступом на об’єкті, що охороняється;

3. Виконати вибір програмного та апаратного забезпечення, розглянути структуру бази даних.

Об’єктом дослідження дипломної роботи є процес забезпечення інформаційної безпеки.

Предметом дослідження дипломної роботи є система контролю і управління доступом до об’єкта, що охороняється.

При написанні роботи були використані методи аналізу, порівняння, дослідження.

Наукова новизна отриманих результатів при написанні дипломної роботи полягає в тому, що була модернізована система контролю і управління доступом та систематизована методика розрахунку ризиків інформаційної безпеки.

Практичне значення отриманих результатів полягає в тому, що розроблені схемні та структурні рішення можна застосовувати на об’єктах, які вимагають захисту та забезпечення безпеки інформації та впровадження систем контролю та управління доступом.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ СИСТЕМ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

1.1. Сучасні різновиди систем контролю і управління доступом

В межах даного розділу розглянемо існуючі системи контролю і управління доступом.

Системи контролю доступу (*ACS*) – це електронні системи, які управляються через мережу і, в свою чергу, мають доступ до мережі. Система контролю доступу розпізнає облікові дані людини і дозволяє їм вхід на об'єкт, тим самим забезпечуючи його захист [1].

Система контролю доступу (*ACS*, СКУД) забезпечує безпеку, дозволяючи легкий доступ уповноваженим особам.

ACS – одна з найбільш часто використовуваних систем електронного контролю дверей з використанням карти, чіпа або біометричних даних для обмеження доступу уповноважених осіб.

Організації або області, що вимагають високої безпеки, використовують різні типи систем контролю доступу, такі як біометричні, *RFID* і зчитувачі карт. Кожен запис може контролюватися індивідуально політикою компанії, якщо потрібна висока безпека. Мережева безпека також важлива, особливо в компаніях, що працюють з конфіденційними даними [2].

Таким чином, система контролю і управління доступом – комплекс програмно-апаратних технічних засобів контролю і управління, призначений для обмеження і реєстрації в'їзду і виїзду об'єктів (людей, транспортних засобів) на конкретний об'єкт через «точки доступу»: двері, ворота, контрольно-пропускні пункти.

Системи фізичної безпеки і контролю доступу стали необхідними для більшості компаній. Великі або малі компанії повинні захищати свої об'єкти, дані і персонал. Нижче на прикладі наводиться короткий огляд того, що задіяно в системі фізичної безпеки і контролю доступу.

Приклад СКУД наведений на рис. 1.1.

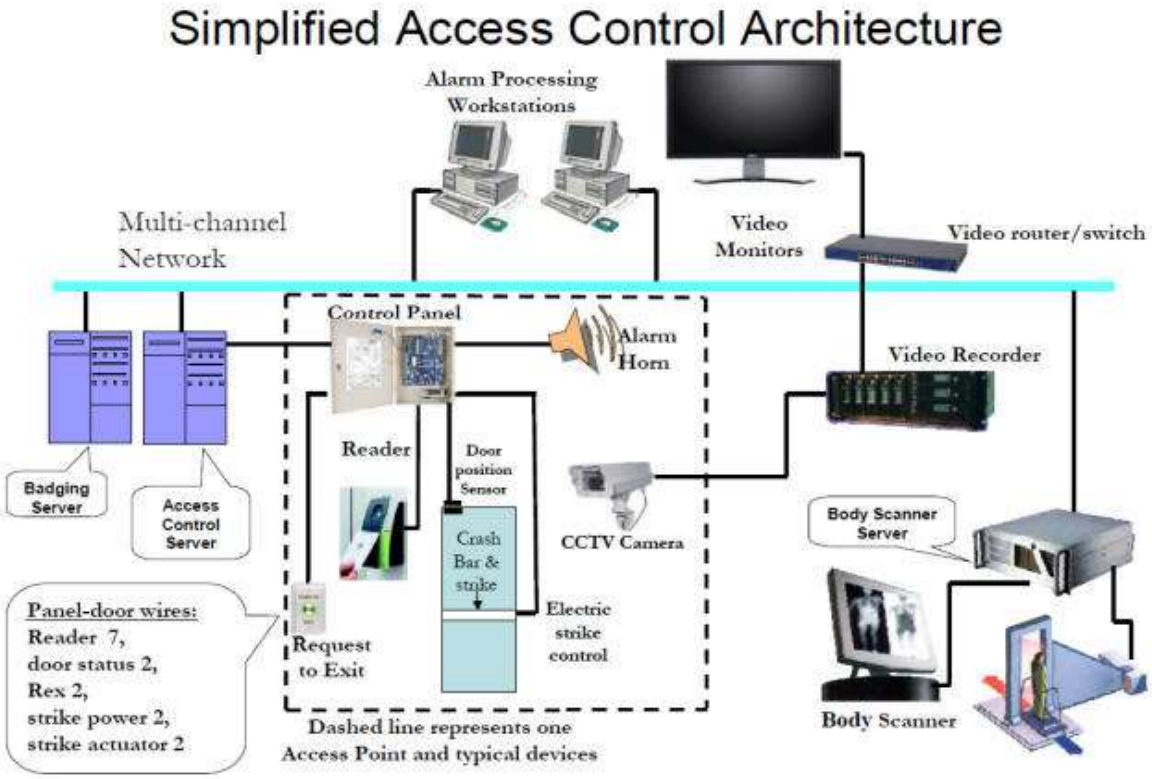

Рис. 1.1. Архітектура СКУД

Розглянемо основні компоненти.

Сервер системи контролю доступу (*ACS*) запускає програмне забезпечення. Він може містити безліч серверів на одній машині або розподілятися по безлічі машин. Цей сервер відповідає за надання доступу та відстеження трафіку в захищених областях. Також підтримує базу даних власників облікових даних і їх рівень доступу. Взаємодіє з панелями *ACS* для завантаження певних даних на кожну панель для локального флеш-сховища. Цей сервер може взаємодіяти з панелями *ACS* різними способами. Якщо панелі оснащені картами *Ethernet*, зв'язок може бути заснований, наприклад, на *TCP / IP* [3].

Якщо панелі оснащені багатоточковим інтерфейсом *RS-485*, то сервер (через перетворювач *RS-232* в *RS-485*) буде зв'язуватися з кожною панеллю по послідовній шині, опитуючи кожну панель і обробляючи дані панелі. Сервер *ACS* також може надати хост за запитом від панелей, які не мають останньої інформації. Сервер *ACS* оновлює панелі за розкладом, однак до цього часу персоналу буде надано хостинг.

Сервер Бейджинг – це місце, де зберігаються дані уповноваженого персоналу. Сервер обробить дані і видасть (роздрукує) облікові дані (значки). Зазвичай співробітник або підрядчик отримує бейдж з закодованою інформацією, включаючи фотографію, ім'я, адресу, організацію, дані про видачу, області доступу, дату закінчення терміну дії, обмеження і іншу необхідну інформацію. Якщо на об'єкті використовуються біометричні зчитувачі, зразок відбитка пальця або скан райдужної оболонки ока також може бути закодований.

Сервер Бейджинг підключений до мережі з сервером *ACS*, тому бейджи можна оновлювати в базі даних сервера *ACS* і завантажувати на панелі доступу, до яких дозволений доступ держателям облікових даних.

Це завантаження відбувається при внесенні змін до області доступу, персоналу, рівня доступу і т.д. [3].

Перетворювач *RS-232* в *RS-485*: *RS-232* – це послідовний інтерфейс з паралельними лініями управління для управління потоком даних. Не всі сигнали необхідні у всіх випадках. Послідовний порт комп'ютера використовує контакти 2, 3 і 5. Лінія *RTS* зазвичай підключається до *CTS* для додатків, які пов'язані з управлінням потоком, і, оскільки немає телефонного модему, *RI* і *CD* не використовуються. *RS-232* використовує «несиметричні» драйвери та приймачі.

Відеомаршрутизатор / комутатор забезпечує можливість спостереження за будь-якою камерою або мультиплексним зображенням на клієнтській робочій станції системи.

Цифровий відеомагнітофон зазвичай включений і записує події в циклі. Тривалість циклу залежить від вимог замовника.

У великій корпоративній системі багато камер і, можливо, багато записуючих пристроїв. Реєстратори зазвичай призначаються обмеженій кількості камер в залежності від їх ємності зберігання, але, тим не менш, вони повинні знаходитися в одній *IP*-мережі, щоб події можна було викликати і відтворювати за запитом для кожної області.

Панелі управління забезпечують шлюз між контрольними точками (двері, КПП) і сервером СКУД.

З боку дверей вони обробляють дані зчитувача, повідомляють про становище двері (відкрито, закрито), приймають запит на вихід з захищеної сторони і наказують електричному замку двері відкриватися або залишатися закритим. На стороні сервера вони відповідають на опитування, повідомляють про вторгнення, сигнали тривоги, проблеми з обліковими даними, сигнали несанкціонованого доступу і ряд іншої інформації, необхідної для забезпечення безпеки [3,4].

Панелі зберігають облікові дані користувача у флеш-пам'яті на випадок, якщо зв'язок між панеллю і сервером недоступний. Панелі будуть працювати в автономному режимі до відновлення зв'язку.

Існує безліч різновидів панелей і інтерфейсів, що з'єднують панель з сервером.

Деякі панелі спілкуються з сервером по протоколу *Ethernet*, деякі на шині *RS-485*.

Однак з боку контрольно-пропускних пунктів сигнали досить стандартні.

Панелі зазвичай контролюють 2 контрольно-пропускні пункти (двері), але є панелі зі слотами розширення, які можна розширити до декількох дверей. Типове з'єднання панелі з дверима показано на рисунку 1.2 (*Honeywell® NS2 +*).

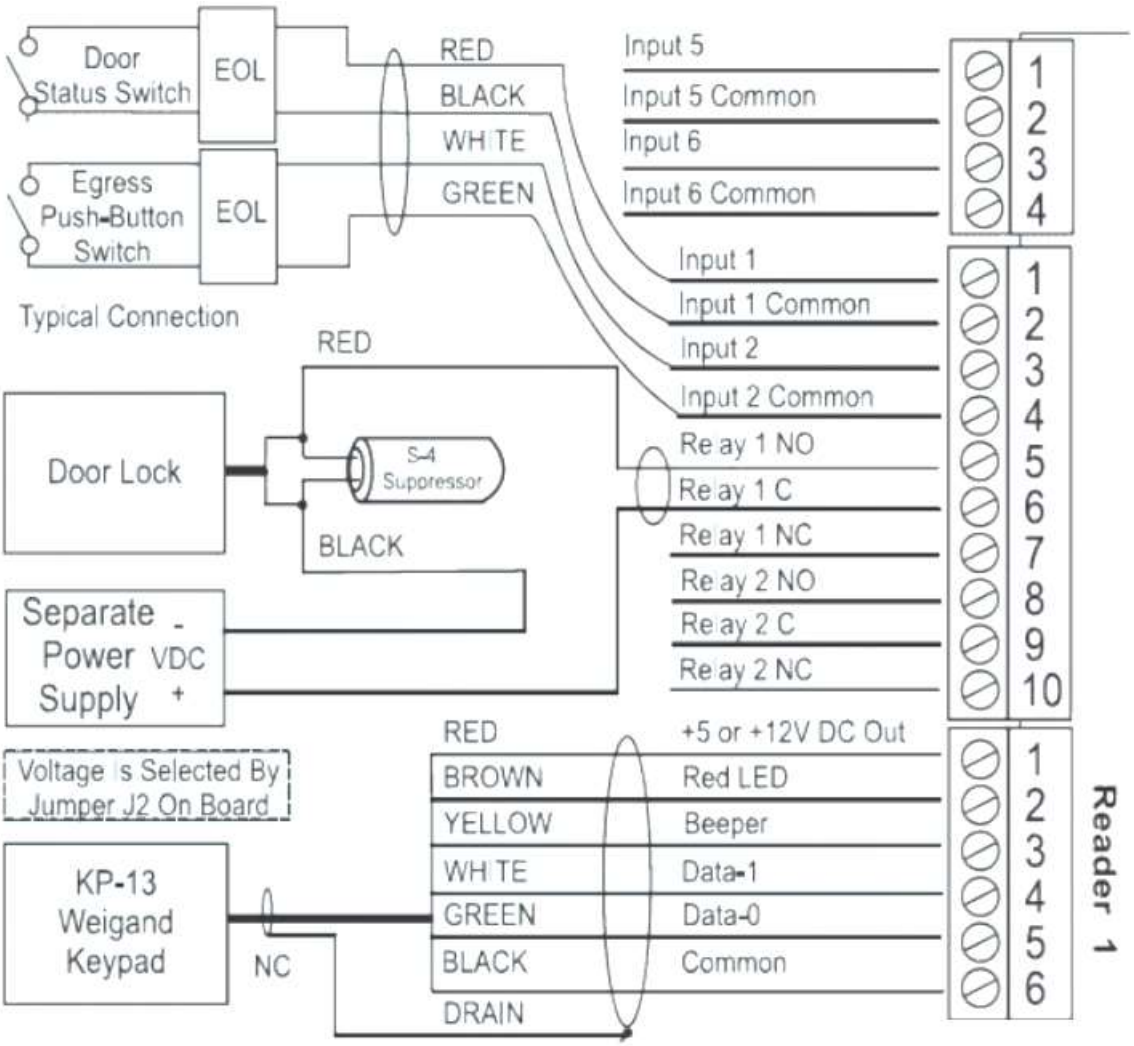

Рис. 1.2. Типове з'єднання панелі з дверима

Дверна фурнітура складається з пристрою для читання, перемикача положення двері, кнопки запиту на вихід і електричного дверного замка. Є багато різновидів зчитувачів з різними технологіями.

Зчитувачі використовують дротяну обмотку для створення магнітного поля. Коли карта підноситься до пристрою читання, магнітне поле створює електричне поле в обмотці карти, подає живлення на процесор карти, і пакет даних, що містить інформацію про користувача, передається з карти на пристрій читання.

Приклади зчитувачів представлені на рис. 1.3.

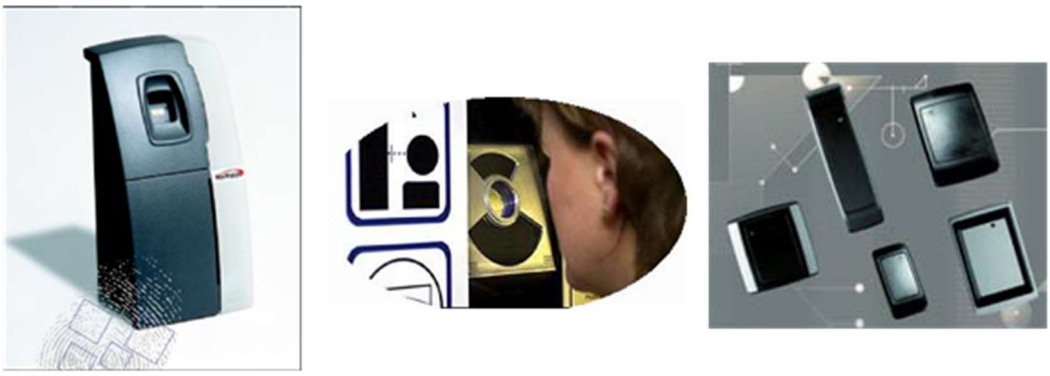

Рис. 1.3. Приклади зчитувачів

Перемикач положення двері (рис. 1.4) зазвичай магнітний перемикач. Поки обидві частини перемикача знаходяться поруч один з одним, перемикач замкнутий, в іншому випадку – розімкнути.

Рис. 1.4. Перемикач положення двері

Електричний замок – це пристрій, що приводиться в дію за допомогою соленоїда, який відкриває замок, щоб двері можна було штовхнути, не повертаючи дверну ручку. Вхідна потужність становить 12 або 24 *В* постійного струму. У деяких випадках використовуються магнітні замки, тому при подачі напруги двері магнітно утримуються дверною рамою замку (рис. 1.5).

Рис. 1.5. Електричний замок

Запит на вихід / вихід – це перемикач миттєвого закриття. При натисканні ланцюг замикається і сигналізує панелі, щоб розблокувати дверний замок, з метою забезпечення виходу з безпечної зони (рис. 1.6).

Рис. 1.6. Запит на вихід/вхід

Отже, контроль доступу використовується для ідентифікації людини, яка виконує певну роботу, аутентифікації його, а потім для передачі цій людині тільки ключа від дверей або робочої станції, доступ до якої їй потрібен доступ [5].

Існують три варіанти систем контролю доступу: дискреційний контроль доступу (*DAC*), обов'язковий контроль доступу (*MAC*) і контроль доступу на основі ролей (*RBAC*).

Дискреційний контроль доступу (*DAC*).

Дискреційний контроль доступу – це тип системи контролю доступу, який покладає на людину, яка приймає рішення, відповідальність за прийняття рішення про те, яким людям дозволено перебувати в певному місці, фізично або в цифровому вигляді.

DAC є найменш обмежуючою системою в порівнянні з іншими системами, оскільки він по суті дозволяє кожній людині повністю контролювати будь-які об'єкти, якими вони володіють, а також програми, пов'язані з цими об'єктами.

Недолік дискреційних контролю доступу є те, що вона дає кінцевому користувачу повного контроль для налаштування рівня набору безпеки для інших користувачів і право доступу. Дані кінцевого користувача успадковуються в інші програми, які вони використовують, що може потенційно призвести до

шкідливих програм, які впроваджуються на підприємство без відома кінцевого користувача.

Обов'язковий контроль доступу (*MAC*).

Обов'язковий контроль доступу частіше використовується в організаціях, які вимагають підвищеної уваги до конфіденційності та класифікації даних (наприклад, у військових установах). *MAC* не дозволяє власникам мати право голосу в організаціях, що мають доступ до підрозділу або об'єкта, замість цього тільки власник має управління контролем доступу. *MAC* зазвичай класифікує всіх кінцевих користувачів і надає їм мітки, які дозволяють їм отримати доступ через систему безпеки з встановленими правилами безпеки.

Контроль доступу на основі ролей (*RBAC*) *RBAC*, також відомий як управління доступом на основі правил або ролей, є найбільш затребуваним в системах управління доступом. *RBAC* не тільки користується великим попитом серед домашніх господарств, але також користується великим попитом в діловому світі.

У системах *RBAC* доступ призначається системним адміністратором і строго заснований на ролі суб'єкта в господарстві або організації, а більшість привілеїв заснована на обмеженнях, визначених їх посадовими обов'язками.

Таким чином, замість того, щоб призначати людину менеджером безпеки, у посаді менеджера безпеки вже призначений дозвіл на управління доступом.

RBAC значно спрощує життя, тому що замість того, щоб призначати конкретний доступ кільком особам, системний адміністратор повинен призначити доступ тільки певним людям.

Основні переваги контролю доступу [7]:

– Багато підприємств мають цінне обладнання та матеріальні активи на місці. Система контролю доступу відслідковує, хто приходить і йде, щоб ніхто не пробрався на територію підприємства;
– Якщо бізнес великий, з великою кількістю співробітників, кожному може бути важко зрозуміти, хто є співробітником, а хто ні. Система

контролю доступу допомагає запобігти проникненню незнайомців непоміченими;

- Слідкування за діями співробітників. Якщо в компанії кілька змін, коли великі групи співробітників приходять і йдуть в позаурочний час, система контролю доступу може допомогти проінформувати, чи знаходиться співробітник в будівлі. Це також може допомогти відстежувати, хто прийшов на роботу, а хто ні;
- Захист конфіденційних документів і даних. У багатьох підприємств є документи або дані, які не повинні бути доступні для всіх в компанії. Система контролю доступу дозволяє компанії обмежувати доступ до певних областей, що містить обладнання або програмне забезпечення, на яких зберігається ця інформація;
- Зменшується кількість крадіжок і нещасних випадків. Система контролю доступу дозволяє надавати доступ тільки затвердженим або спеціально навченим співробітникам до ділянок, де може перебувати цінне або небезпечне обладнання;
- Захист декількох об'єктів власності. Інтегрована система контролю доступу дозволить надавати доступ співробітникам, яким необхідно увійти в кілька закритих сегментів;
- Більше не потрібно турбуватися про ключі. Коли співробітник звільняється і не може повернути свої ключі, бізнес застряє в витратах на виготовлення нових ключів і, можливо, навіть на заміну замків. Те ж саме стосується, коли співробітник втрачає ключі від своєї компанії. Якщо співробітник пішов в поганих умовах, це також виключає ймовірність того, що він спробує повторно увійти в будівлю і завдати шкоди.

Маючи систему контролю доступу, підприємство може просто видалити доступ співробітника з системи в цифровому вигляді.

Додаткові функції СКУД [7]:

– облік робочого часу;

– розрахунок заробітної плати (при інтеграції з системами обліку);

– ведення бази даних співробітників / відвідувачів;

– інтеграція з іншими видами систем безпеки: з системою відеоспостереження для об'єднання архівів системних подій, відправки команд в систему відеоспостереження для початку запису підозрілої події; з охоронною сигналізацією, наприклад, для обмеження доступу до об'єктів; з системою пожежної сигналізації для автоматичного відмикання аварійних виходів та відкриття протипожежних дверей в разі пожежної тривоги за сигналом пожежних сповіщувачів.

1.2. Обґрунтування необхідності застосування СКУД

Контроль доступу – одна із складових частин комплексного поняття, процесу забезпечення безпеки підприємства [7].

Сучасні мережеві системи контролю та управління доступом (СКУД) за своїми можливостями можуть забезпечити необхідний рівень захисту даних, що містять тисячі точок доступу і десятки тисяч користувачів. Крім цього, системи служать основою для побудови інтегрованих систем безпеки.

Якісний аналіз та проектування є необхідними умовами успішної розробки інформаційних систем. Саме на початкових стадіях визначаються фундаментальні аспекти моделювання системи і рішення, від яких багато в чому залежить успіх проекту.

Послідовність розробки СКУД моделей є каркасом, який може бути нарощений в залежності від типу і призначення інформаційної системи.

Етап визначення функціональних вимог може супроводжуватися безліччю проблем через складність чітко вираженого завдання, яке покладається на ІС, різноманітності поглядів на роботу майбутньої системи, відсутність у замовника

знань про можливості сучасних обчислювальних систем і уявлення про процес автоматизації.

Побудова функціональної моделі має вирішити більшу частину цих проблем.

Таким чином, необхідність розробки методики проектування СКУД є дійсно актуальною.

1.3. Висновки до розділу

В результаті написання першого розділу роботи встановлено, що система контролю і управління доступом (СКУД) – сукупність сумісних між собою апаратних і програмних засобів, виділених для обмеження і реєстрації доступу людей, транспорту та інших об'єктів в (з) приміщення, будівлю, зону і територію.

До складу СКУД входять:

– Пристрій з керованим блокуванням. Наприклад, турнікети, двері, оснащені керованими замками, хвіртки, шлагбауми, шлюзи;

– Зчитувальні пристрої. Наприклад, пристрої радіочастотної ідентифікації, сканери пальців, пристрої машинного зору;

– Контролери СКУД. Електронні мікропроцесорні модулі, що реалізують аутентифікацію об'єктів доступу, логіку авторизації для доступу в ті чи інші приміщення і області;

– Програмне забезпечення САУ. Необов'язковий елемент, що дозволяє здійснювати централізоване управління контролерами СКУД з персонального комп'ютера (ПК) – формування звітів, та інші різні додаткові функції;

– Конвертери для підключення апаратних модулів СКУД один до одного і до ПК. Наприклад, перетворювачі *EIA-485, RS232, EIA–485 Ethernet*;

– Допоміжне обладнання (блоки живлення, кнопки), з'єднувальні дроти;

В межах наступних розділів роботи буде розглянуто проектування СКУД. Проектування СКУД буде включати в себе наступні етапи:

– Розробка моделі загроз і порушника організації;

– Побудова методики проектування СКУД на базі розробленої моделі;

– Розробка моделі СКУД та бази даних.

В результаті проведеного аналізу існуючих систем контролю і управління доступом до об’єктів, що охороняються, необхідно зробити наступне:

1) Оцінити ризики інформаційної безпеки;

2) Розглянути модель загроз і модель порушника;

3) Вибрати методики проектування СКУД;

4) Провести обґрунтування вибору складових системи;

5) Розробити структурну схему зв’язку в СКУД;

6) Створити базу даних для СКУД.

РОЗДІЛ 2
СИСТЕМА КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ ДО ОБ’ЄКТІВ

2.1. Оцінка ризиків інформаційної безпеки

В межах даного розділу розглянемо необхідність в побудові системи контролю і управління доступом. В першому розділі було встановлено, що основним засобом вразливості систем є саме доступ до інформації, яка знаходиться в комп’ютері, тому варто розглядати інформаційну систему, яка націлена на захист інформаційної складової.

Тому актуальним стає питання розробки моделі загроз.

При аналізі та класифікації джерел загроз інформації,, виходимо з припущення, що для однієї і тієї ж загрози методи відображення для зовнішніх і внутрішніх джерел можуть бути різними.

Особливу групу внутрішніх джерел становлять спеціально впроваджені і завербовані агенти з числа допоміжного, основного, технічного персоналу і представників відділу інформаційної безпеки.

Було вирішено розділити всі джерела загроз безпеці інформації на три основні групи:

– антропогенні джерела загроз (помилки експлуатації, помилки проектування і розробки компонентів АС, навмисні дії порушників і зловмисників;

– техногенні джерела загрози (аварії, збої і відмови устаткування (технічних засобів));

– обумовлені стихійними джерелами (Стихійні лиха, катаклізми).

Таким чином, класифікація і перелік джерел загроз властивих об'єкту інформатизації представлені таблицях 2.1 і 2.2.

Таблиця 2.1

Антропогенні джерела загроз системи

№	Зовнішні антропогенні джерела	№	Внутрішні антропогенні джерела
1.	Кримінальні групи та окремі злочинні суб'єкти	1.	Працівники
2.	Потенційні злочинці (недобросовісні платники податків) і хакери	2.	Адміністратори АС Адміністратор безпеки, програмісти, адміністратор домену
3.	Персонал постачальників телематичних послуг (Провайдери)	3.	Технічний персонал
4.	Представники наглядових організацій і аварійних служб	4.	Працівники відділу безпеки

В якості антропогенних джерел загроз виступають суб'єкти, які мають санкціонований / несанкціонований доступ до роботи зі штатними засобами об'єкта інформатизації, дії яких можуть бути розпізнані, як умисні або вчинені з необережності.

Дана група джерел загроз становить найбільший інтерес, так як дії суб'єкта завжди можна оцінити, спрогнозувати, і вжити відповідних заходів. Контрзаходи в цьому випадку безпосередньо залежать від дій організаторів інформаційної безпеки.

Таблиця 2.2

Техногенні джерела загроз

№	Зовнішні техногенні джерела загроз	№	Внутрішні техногенні джерела загроз
1.	Засоби зв'язку, промислові установки іонізуючого випромінювання, системи енергозабезпечення	1.	Неякісні технічні засоби обробки інформації
2.	Мережі інженерних комунікацій (Водопостачання, каналізації)	2.	Неякісні програмні засоби обробки інформації
3.	Транспорт (авіаційний, залізничний, автомобільний, водний)	3.	Допоміжні засоби (Охорони, сигналізації, телефонії, відеоспостереження, СКУД)
4.		4.	Інші технічні засоби

Техногенні джерела загроз характеризуються технократичною діяльністю людини і розвитком техніки.

Група стихійних джерел загроз об'єднує обставини, складові непереборної сили, тобто такі обставини, які носять об'єктивний і абсолютний характер, який поширюється на всіх, які неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти. Захисні заходи від стихійних джерел загроз повинні застосовуватися завжди, тому що їх неможливо спрогнозувати.

Інформаційна система являє собою розподілену інформаційну систему, що складається з робочих станцій і серверів. Аналіз показав, що дана система має підключення до мереж зв'язку загального користування.

На сьогоднішній момент обробка даних, в тому числі ті, які підпадають під категорію комерційної таємниці, проводиться в розрахованому на багато користувачів режимі з розмежуванням прав доступу.

На об'єкті захисту є:

– загрози витоку інформації технічними каналами;

– загрози несанкціонованого доступу до даних, які обробляються на автоматизованих робочих місцях.

Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації.

У процесі аналізу ризику вивчаються компоненти інформаційної системи компанії, які можуть піддатися загрозам, які визначають вразливі місця системи, оцінюють ймовірність для кожної конкретної загрози і очікувані розміри втрат, вибирають можливі методи захисту і прораховують їх вартість.

На заключному етапі оцінюється вигода від застосування передбачуваних заходів захисту. Ця вигода може мати як позитивний, так і негативний знак: в першому випадку – очевидний виграш, у другому – він означає додаткові витрати на забезпечення власної безпеки.

На етапі розробки політики безпеки можна виділити наступні підзадачі:

– Інвентаризація ресурсів;

– Категоріювання ресурсів;

– Оцінка захищеності інформаційної системи;

– Оцінка інформаційних ризиків;

– Аналіз інформаційних ризиків;

– Впровадження запропонованих заходів;

– Контроль за виконанням та ефективністю вибраних заходів.

Перед адміністратором інформаційної безпеки стоїть завдання організувати цикл заходів щодо забезпечення безпеки інформаційної системи, в загальному випадку має таку черговість:

1. Аудит інформаційної безпеки;

2. Складання звіту про знайдені вразливості;

3. Складання рекомендацій;

4. Одним з основних факторів аналізу ризиків та економічного обґрунтування витрат на інформаційну безпеку є розрахунок вартості збитку,

оскільки витрати на інформаційну безпеку повинні бути менше вартості об'єкта захисту або розміру збитку.

На основі [8] пропонується використовувати наступну спрощену модель розрахунку вартості збитку.

Вартість втрат від зниження продуктивності співробітників атакованого вузла або сегмента буде дорівнювати [8]:

$$П_П = \frac{\sum_{N_C} Z_C}{192} \times t_П, \quad (2.1)$$

де $П_П$ – втрата продуктивності;

$t_П$ – час простою внаслідок атаки;

Z_C – зарплата співробітників атакованого вузла або сегмента;

N_C – число співробітників атакованого вузла або сегмента.

Вартість відновлення працездатності атакованого вузла або сегмента складається з декількох складових:

$$П_В = П_{ВІ} + П_{ВВ} + П_{ЗЧ}, \quad (2.2)$$

де $П_В$ – вартість відновлення працездатності атакованого вузла або сегмента;

$П_{ВІ}$ – вартість повторного введення інформації;

$П_{ПВ}$ – вартість відновлення вузла (перевстановлення системи, конфігурація і т.д.);

$П_{ЗЧ}$ – вартість заміни обладнання або запасних частин.

$$П_{ВІ} = \frac{\sum_{N_C} Z_C}{192} \times t_{ВІ}, \quad (2.3)$$

де $t_{ВІ}$ – час повторного введення втраченої інформації;

Z_C – зарплата співробітників атакованого вузла або сегмента;

N_C – число співробітників атакованого вузла або сегмента.

$$П_{ПВ} = \frac{\sum_{N_0} Z_O}{192} \times t_B, \quad (2.4)$$

де t_B – час відновлення: після атаки;

Z_o – зарплата обслуговуючого персоналу (адміністраторів і т.д.);

N_O – число обслуговуючого персоналу (адміністраторів і т.д.).

Втрачена а вигода від простою атакованого вузла або сегмента становить:

$$U = П_П + П_В + V, \quad (2.5)$$

де U – упущена вигода від простою атакованого вузла сегмента.

$$V = \frac{O}{52 \times 5 \times 8 t_П + t_B + t_{BI})}, \quad (2.6)$$

де $t_П$ – час простою внаслідок атаки;

t_B – час відновлення: після атаки;

t_{BI} – час повторного введення втраченої інформації.

Таким чином, загальний збиток від атаки на вузол або сегмент мережі складе:

$$OY = \sum_{год} \sum_t U, \quad (2.7)$$

Модель розрахунку може бути інтерпретована відповідним чином адекватно:

а) умовами конкретного підприємства;

б) об'єктом захисту;

в) можливим інцидентом.

Слід зазначити кілька труднощів в цій області, з якими можна зіткнутися:

– хоча проблеми обґрунтування витрат на інформаційну нерозривно пов'язані з проблемами розрахунку вартості збитку, з питаннями про

фінансування заходів щодо захисту і про ефективність такого фінансування, хоча інтерес до них не згасає, до сих пір немає сформованих методик щодо їх вирішення, які б знайшли відображення в нормативних документах;

– питання про використання для оцінки збитку об'єктивних і суб'єктивних ймовірностей також є спірним, але оскільки метою цієї роботи не ставилося підтвердити або спростувати будь-яку з точок зору, то в розрахунках зазначені ймовірності використовувалися;

– ризик – поєднання ймовірності подій і їх наслідків;

– ймовірність – міра того, що подія може відбутися;

– оцінка ризику – загальний процес аналізу ризику та оцінювання ризику.

Математичне визначення ймовірності: дійсне число в інтервалі від 0 до 1, що відносяться до випадкової події [8].

Якщо ступінь впевненості досить висока, то ймовірність близька до одиниці. Найбільш часто зустрічаються два тлумачення ймовірності: об'єктивна і суб'єктивна.

Під об'єктивною (фізичною) ймовірністю розуміється «відносна частота появи якої-небудь події в загальному обсязі спостережень або відношення числа сприятливих результатів до загальної кількості спостережень».

Це поняття застосовується при аналізі результатів великого числа спостережень, що відбувалися в минулому або отриманих в якості результатів з моделей, які описують деякі процеси.

Під суб'єктивною ймовірністю мається на увазі міра впевненості чоловіка одного або групи людей в тому, що дана подія в дійсності буде мати місце.

Найбільш часто вона являє собою вірогідну міру, отриману емпіричним шляхом, що розділяються на три етапи:

– підготовчий;

– отримання оцінок;

– аналіз оцінок.

Під час першого етапу формується об'єкт дослідження – множина подій, а також проводиться підготовка експерта або групи експертів і ознайомлення їх з методом.

Другим етапом є застосування методу, обраного на першому етапі. Результатом цього етапу буде набір певних чисел, який відображає суб'єктивний погляд експерта або групи експертів на ймовірність тієї чи іншої події, але не завжди може вважатися остаточним розподілом, оскільки часто містить суперечності.

На третьому етапі досліджуються результати опитування. Якщо ймовірності, представлені експертами, не відповідають аксіомам ймовірності, то відповіді експертів уточнюються і приводяться у відповідність до вибраної системи аксіом.

Індивідуальність аналізу інформаційних ризиків для кожного підприємства обумовлена ще й тим, що у кожного з них свій розмір збитків, пов'язаних як з кількістю інформаційних ресурсів, так і з унікальною для кожної організації оцінкою їх важливості.

У стандарті *BS* (Керівництво з управління ризиками інформаційної безпеки) до провідного оцінку ризиків фахівця висувають такі вимоги:

– розуміння бізнесу та готовності прийняти зазначений рівень ризику в процесі отримання прибутку;

– розуміння концепції ризику;

– розуміння загроз і вразливостей;

– розуміння типів контрольних механізмів інформаційної безпеки;

– навички використання методик оцінки ризиків;

– аналітичні здібності;

– здатність визначати необхідні контактні особи;

– комунікабельність.

Тобто недостатньо просто вміти розрахувати загрози і вразливості. Найголовніше і найскладніше – розбиратися в тій сфері, в якій розвивається і функціонує підприємство.

Для даної роботи інтерес представляла ситуація, коли аналіз ризиків на підприємстві не проводився.

Забезпечити безпеку інформації всередині організації можливо лише при наявності і неухильному дотриманні правил захисту інформації, що чітко регламентують, яку інформацію, де і як потрібно захищати, і діючих для всіх без винятку співробітників. В рамках організації ці правила перетворюються в досить складну ієрархічну систему інструкцій і регламентів, призначених для виконання різними категоріями співробітників, задіяних в процесі забезпечення безпеки інформації.

Сукупність взаємопов'язаних документів, що визначають такий порядок забезпечення безпеки інформації в конкретній організації, а також висувають вимоги по підтриманню подібного порядку, являє собою політику безпеки інформації.

Розробка політики безпеки – обов'язковий, основоположний етап при проектуванні практично будь-якої системи забезпечення безпеки інформації.

Від правильного формування корпоративних правил і процедур забезпечення безпеки залежить рівень всіх подальших проектних рішень і рівень безпеки [9].

Створення нормативної бази повинно проводитися відповідно до чинного законодавства.

Дане положення, зрозуміло, може бути застосовано до будь-якого виду діяльності, однак, оскільки інформаційні технології розвиваються дуже швидкими темпами, то нормативна база сильно відстає від виникаючих на практиці потреб. А тут виявляється особливо критичним і відставання законів і стандартів, і відсутність методичного забезпечення.

Що стосується міжнародної нормативної бази, то, «фактично, загальні критерії пропонують набір історично сформованих і, найголовніше, звичних в галузі підходів до безпеки, які використовуються, щоб створювати вироби або системи, що відображають не стільки потреби замовника, скільки можливості розробника».

Таким чином, вони є не стільки критеріями, скільки загальними технічними вимогами.

Перш ніж приступати до категорування, слід виконати наступні операції:

– провести інвентаризацію інформаційних ресурсів;

– визначити вартість інформаційних ресурсів;

– визначити рівень критичності інформаційних ресурсів.

На основі отриманих даних проводиться категорування ресурсів відповідно до їх рівня критичності.

На етапі інвентаризації визначається перелік всіх інформаційних ресурсів, що обробляються в організації. Вартість інформаційного ресурсу оцінюється його власником. Рівень критичності інформаційного ресурсу визначається шляхом віднесення ресурсу до певного рівня критичності відповідно до його вартості.

Після цього виконується категорування інформаційних ресурсів відповідно до їх рівня критичності.

В процесі категорування необхідно оцінити критичність ресурсів для бізнес-процесів, тобто визначити, яких збитків зазнає компанія в разі порушення інформаційної безпеки ресурсів.

Даний процес викликає найбільшу складність, тому що цінність ресурсів визначається на основі експертних оцінок їх власників. На даному етапі часто проводяться обговорення між консультантами по розробці системи управління і власниками ресурсів [9].

Це допомагає власникам ресурсів зрозуміти, яким чином слід визначати цінність ресурсів з точки зору інформаційної безпеки (як правило, процес визначення критичності ресурсів є для власника новим і нетривіальним).

Інвентаризація полягає в перерахуванні користувачами оброблюваних користувачами інформаційних ресурсів. При визначенні переліку оброблюваних інформаційних ресурсів користувачеві слід вказати, для яких із зазначених ресурсів він є власником. Власник інформаційного ресурсу – співробітник, який створює ресурс, а також несе відповідальність за забезпечення його безпеки.

Для визначення інформаційних ресурсів слід розробити перелік інформації, що обробляється в організації. Після інвентаризації інформаційних ресурсів слід визначити їх вартість.

Це основний етап процесу категорування інформаційних ресурсів і, в більшості випадків, найбільш складний.

Вартість ресурсу.

В даному випадку вартість буде визначатися власником інформаційного ресурсу (його оцінка вважається компетентною і не перевіряється).

Для визначення вартості інформаційних ресурсів використовувався наступний перелік:

1. По загрозам порушення конфіденційності:

– вартість упущеної вигоди;

– вартість виплати неустойок, штрафів за невиконання зобов'язань контракту;

– вартість витрат на відновлення репутації.

2. За загрозу порушення цілісності:

– вартість упущеної вигоди від неадекватного функціонування інформаційної системи;

– витрати на відновлення інформаційного ресурсу.

3. По загрозам порушення доступності:

– вартість упущеної вигоди від неможливості надання послуги;

– заробітна плата співробітників за час простою;

– витрати на заміну устаткування;

– витрати на відновлення працездатності інформаційної системи.

Критичність ресурсу визначається тим, наскільки критично для бізнесу порушення конфіденційності, цілісності або доступності ресурсу.

Рівень критичності ресурси можна визначити у вигляді таблиці 2.3.

Таблиця 2.3

Рівень критичності ресурсу

Назва рівня	Визначення в грошових одиницях	Визначення з точки зору впливу на репутацію компанії
Низький рівень	Незначний збиток	Незначний вплив на репутацію компанії
Середній рівень	Помітний або великої шкоди	Істотний вплив на репутацію компанії або обмеження її інтересів
Високий рівень	Значної шкоди	Шкода репутації компанії і її інтересам, яка може становити загрозу для продовження діяльності компанії аж до повного банкрутства

Під простотою реалізації загрози розуміється наступне (таблиця 2.4).

Таблиця 2.4

Реалізація загрози

Реалізація загрози	Необхідні для реалізації знання
Низька	Немає детальних знань про принципи функціонування системи; може бути реалізована будь-яким користувачем
Середня	Висока кваліфікація, навички в програмуванні, наявність прав адміністратора, знання про помилки в реалізації ПЗ
Висока	Знання помилок в реалізації ПЗ, знання вихідного коду, високі навички програмування, значні матеріальні та часові ресурси

Під критичністю реалізації загрози розуміється її ступінь впливу на ресурс (таблиця 2.5).

Таблиця 2.5

Критичність реалізації загрози

Критичність реалізації загрози	Опис
Висока	Інформація втрачена або спотворена, доступ до ресурсу повністю блокований
Середня	Зловмисником отримана інформація для здійснення подальших атак, доступ до ресурсу важко або взагалі тимчасово блокований
Низька	Зловмисником отримана суттєва (з точки зору реалізації подальших атак) інформація про ресурс

Ідентифікація загроз.

Найбільш докладним каталогом загроз із загальнодоступних є каталог загроз, запропонований стандартом *BSI*. Каталог загроз містить наступні групи загроз:

1. Загрози в зв'язку з форс-мажорними обставинами;
2. Загрози на організаційному рівні;
3. Загрози, пов'язані з помилками людей;
4. Загрози, пов'язані з технікою;
5. Загрози, що виникають на передпроектному етапі.

Ідентифікація та аналіз вразливостей системи.

На першому етапі складається список загроз по кожному ресурсу, що містить інформацію, яка захищається.

Пропонується ідентифікувати уразливості методом суб'єктивної ймовірності, а саме прямою оцінкою ймовірностей подій. По кожному ресурсу, що містить інформацію, експертам пропонується набір можливих загроз.

Зі списку загроз потрібно вибрати найбільш ймовірно здійсненну загрозу і визначити ймовірність її здійснення.

Далі ця загроза видаляється зі списку і процедура визначення найбільш вірогідної загрози повторюється [10].

Сума всіх отриманих ймовірностей повинна дорівнювати одиниці.

На другому етапі визначається ймовірність реалізації тієї чи іншої загрози.

Аналіз і оцінка збитку.

Для кожного ресурсу з ідентифікованими уразливими готуються дані для оцінки збитку. Вхідними даними цього етапу алгоритму є:

– час простою внаслідок реалізації;

– число співробітників уразливого вузла;

– зарплата співробітників вузла;

– зарплата і кількість обслуговуючого персоналу.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі, згідно з оцінкою збитку буде розраховувати згідно формули 2.7.

Оцінка ризику.

На першому етапі розраховуємо рівень загрози по уразливості *Th* на основі критичності і ймовірності реалізації загрози через дану уразливість.

Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її реалізації [10].

$$\boldsymbol{Th} = \frac{\boldsymbol{ER}}{\boldsymbol{P(V)}}, \tag{2.8}$$

де *ER* – критичність реалізації загрози (вказується у відсотках);

P(V) – ймовірність реалізації загрози через дану уразливість (вказується у відсотках).

Отримуємо значення рівня загрози по уразливості в інтервалі від 0 до 1.

Щоб розрахувати рівень загрози за всіма загрозами *CTh*, через які можлива реалізація даної загрози на ресурсі, підсумуємо отримані рівні загроз через конкретні уразливості за такою формулою:

$$\boldsymbol{CTh = 1 - \prod_{i=1}^{n\prod}(1 - Th_i())}, \quad (2.9)$$

де *Th* – рівень загрози по уразливості.

Отже, значення рівня загрози по всім вразливостям отримаємо в інтервалі від 0 до 1.

Розраховуємо загальний рівень загроз по ресурсу *CThR* (враховуючи всі загрози, які діють на ресурс):

$$\boldsymbol{CThR = 1 - \prod_{i=1}^{n}(1 - CThi)}, \quad (2.10)$$

Значення загального рівня загрози отримаємо в інтервалі від 0 до 1.

Ризик по ресурсу *R* розраховується наступним чином:

$$\boldsymbol{R = CThR \times D}, \quad (2.11)$$

де *D* – критичність ресурсу (задається в грошах або рівнях);

CThR – загальний рівень загроз по ресурсу.

Інформація, з якою працює, і вартість збитку. Вартість інформаційного ресурсу визначалася його власниками.

Вартість інформаційної системи: 9665 тис.грн.

Для спрощення моделі будемо нехтувати втратами від простою устаткування, і, таким чином, максимальний збиток інформаційній системі буде дорівнювати вартості інформаційної системи.

Перелік загроз, що діють на інформаційні ресурси компанії, і ймовірність реалізації загроз.

1. Вплив на ресурс:

– неавторизоване проникнення порушника всередину об'єкту, що охороняється;

– читання цінної інформації з паперових носіїв і екранів персональних комп'ютерів;

– модифікація цінної інформації на паперових носіях;

– знищення або псування носіїв з цінною інформацією;

– крадіжка носіїв з цінною інформацією (паперових носіїв, дискет, компакт-дисків, флеш-карт);

– установка пристроїв зняття електромагнітних коливань;

– отримання конфіденційної інформації без застосування спеціальних засобів (прослуховування, візуальне спостереження).

2. На канал зв'язку:

– пошкодження кабелів;

– несанкціоноване бездротове підключення до кабельної лінії;

– несанкціоноване дротове підключення до кабельної лінії.

3. Загрози «природнього» характеру [8]:

– пожежа;

– затоплення;

– удар блискавки;

– неприпустима температура і вологість;

– катастрофи в навколишнє середовище;

– вимкнення електрики;

– відмова резервних (що належать підприємству) джерел енергопостачання;

– скачки напруги в електричній мережі.

4. Загрози, пов'язані з відмовою устаткування:

– втрата даних в результаті відмови носіїв даних;

– дефектні носії даних;

– закінчення терміну експлуатації обладнання;

– переповнення пристроїв зберігання інформації (в цьому випадку можливі втрати даних).

5. Загрози операційній системі / прикладного програмного забезпечення:

– розширення привілеїв користувача при реалізації локальних вразливостей, що використовують помилки розробки операційної системи;

– розширення привілеїв користувача при реалізації локальних вразливостей, що використовують помилки адміністрування операційної системи;

– підміна системних конфігураційних файлів / прикладного програмного забезпечення;

– відмова в обслуговуванні операційної системи.

6. Загрози інформації:

– неавторизована зміна електронних документів / інформації в базі даних;

– неавторизоване читання конфіденційної інформації в базі даних / в електронних документах;

– неавторизоване використання електронної пошти порушником від імені легального користувача;

– видалення порушником цінної інформації, що зберігається в базі даних / міститься в електронних документах;

– навмисне використання конфіденційної інформації з метою особистої вигоди;

– ненавмисне використання конфіденційної інформації.

7. Загрози мережних служб:

– відмова в обслуговуванні мережевої служби (внутрішній збій програмного забезпечення);

– підбір аутентифікаційних даних користувача;

– перехоплення інформації, що надається мережевими службами (повідомлень електронної пошти), використовуючи вразливості протоколів передачі даних.

8. Атаки на мережеве обладнання:

– неавторизований доступ до мережних пристроїв на програмному рівні;

– відмова в обслуговуванні на програмному рівні.

9. Атаки на протоколи зв'язку:

– перехоплення мережевого трафіку на логічному рівні.

Рівень загрози складається з ймовірності реалізації даної загрози (*P*) і ймовірності того, що реалізація загрози вплине на даний ресурс (*ER*).

Згідно аналізу існуючих загроз, на об'єкті захисту зробимо оцінку, наведену в таблиці 2.6.

Таблиця 2.6

Загрози, що впливають на ресурси

ЗАГРОЗА	P,%	ER
1.Влив на ресурс		
Читання цінної інформації з паперових носіїв і екранів персональних комп'ютерів	50	55
Знищення або псування носіїв з цінною інформацією	30	5
Крадіжка носіїв з цінною інформацією (паперових носіїв, компакт-дисків, флеш-карт)	40	5
2.Загрози «природного» характеру		
Стихійні лиха	3	5
Неприпустима температура і вологість	1	10
Вимкнення електрики	10	1
3.Вплив на інформацію		
Неавторизоване читання, зміна, видалення електронних документів / інформації в базі даних	20	55
Навмисне використання співробітниками конфіденційної інформації з метою особистої вигоди	60	75
Вимкнення електрики	10	1

Закінчення таблиці 2.6

Ненавмисне використання співробітниками конфіденційної інформації	40	65
4.Вплив на мережеві служби		
Відмова в обслуговуванні мережевої служби (внутрішній збій програмного забезпечення)	35	40
Розширення привілеїв віддаленого користувача при реалізації вразливостей, що використовують помилки розробки або адміністрування мережевих служб	15	50
Підбір автентифікаційних даних користувача	15	60
Перехоплення інформації, що надається мережевими службами (повідомлень електронної пошти), використовуючи вразливості протоколів передачі даних	20	45

Сумарна ймовірність реалізації загроз для всіх інформаційних ресурсів (таблиця 2.7) [9].

Таблиця 2.7

Рівень загроз

Ресурс	Загальний рівень загроз по ресурсу
1.Вплив на ресурс	0,31
2.Загрози «природнього» характеру	0,004
3.Вплив на інформацію	0,82
4. Вплив на мережеві служби	0,395

Оцінка ризику наведена в таблиці 2.8.

Таблиця 2.8

Оцінка збитку

Ресурс	Максимальний збиток по ресурсу, тис. грн.	Рівень загрози по всім вразливостям	Ризик ресурсу, тис. грн.
1.Вплив на ресурс	3256	0,31	1009,36
2.Загрози «природного» характеру	790	0,004	5
3.Вплив на інформацію	5700	0,82	4674
4. Вплив на мережеві служби	200	0,395	79

Сумарний ризик інформаційної системи становить 5767,36 тис. грн.

Витрати на забезпечення ІБ представлені в таблиці 2.9.

Таблиця 2.9

Вартість заходів щодо усунення загроз

Заходи щодо усунення недоліків	Приблизні фінансові витрати, тис. грн
Регулярне навчання співробітників з питань інформаційної безпеки.	50
Впровадження системи блокування портів передачі даних.	100
Затвердити угоду про дотримання режиму ІБ (яке слід підписувати кожному співробітнику).	100
Розробити процедуру регулярних перевірок ІБ (внутрішні перевірки, зовнішній аудит).	0

Закінчення таблиці 2.9

Розробити перелік інцидентів в області інформаційної безпеки, за якими необхідно проводити розслідування.	0
Розробити процедуру реагування на інциденти в області інформаційної безпеки.	0
Затвердити нормативними документами перелік системних подій, за якими необхідно здійснювати аудит і проводити аналіз лог-файли.	0
Впровадження системи моніторингу конфігурацій робочих станцій і серверів.	45
Система виявлення і запобігання атак	500
Обладнати приміщення для резервного сервера і зберігання архівної інформації на знімних носіях	500
Провести категорування інформаційних ресурсів. Затвердити систему контролю заходів щодо ІБ.	30

Підсумкова вартість витрат на забезпечення інформаційної безпеки становить 1325 тис. грн., що більш ніж в 4 рази менше сумарного ризику, якому піддаються інформаційні ресурси.

2.2. Модель загроз

Для визначення можливих каналів витоку інформації, виявлених на етапі обстеження, необхідно розробити документ Приватна модель загроз безпеки конфіденційної інформації (КІ) при їх обробці для систем.

Цей документ містить перелік загроз безпеки ІС, розрахунок актуальності яких розраховувався виходячи з рівня вихідної захищеності, уразливості, що дозволяють здійснити їх практичну реалізацію, а також методи і способи захисту інформації, що дозволяють знизити актуальність загроз до прийнятного рівня.

Загрози безпеці інформації, оброблюваної в ІС, що містяться в моделі загроз, можуть доповнюватися в міру виявлення нових джерел загроз в ІС.

Так як для комерційної таємниці як такої базової моделі загроз як для систем персональних даних, то модель загроз складається на основі проведеного аналізу імовірнісних загроз інформаційної безпеки.

Приватна модель загроз представлена у вигляді таблиці 2.10.

Таблиця 2.10

Модель загроз інформаційної системи

Загрози	Існуючі заходи захисту	Вразливості	Імовірність реалізації
1.1 Фізичний доступ порушника	Встановлена охоронна сигналізація і елементи фортифікації	–	Низька
1.2. Розголошення конфіденційної інформації, що зберігається на серверах	Трудовий кодекс України, трудовий договір.	Людський фактор (Шантаж, підкуп, погрози, помста, необережність)	Середня
1.3. Руйнування конфіденційної інформації на серверах за допомогою спеціальних програм і вірусів	–	Людський фактор (Шантаж, підкуп, погрози, помста, необережність), а також застарілий антивірусний захист	Середня
1.4. Копіювання конфіденційної інформації з сервера	Розмежування прав доступу користувачів	Користувачі не дотримуються заходів щодо інформаційної безпеки	Середня
1.5. Доступ з мереж загального користування до серверів	Функціонує міжмережевий екран, провайдер забезпечує додатковий захист	Міжмережевий екран із застарілим програмним забезпеченням, застарілий антивірусний захист	Середня

Закінчення таблиці 2.10

2.1. Фізичний доступ порушника до АРМ, копіювання конфіденційної інформації	Встановлено елементи фортифікації, встановлена охоронна сигналізація, розмежування прав доступу користувачів	Користувачі не дотримуються заходів щодо інформаційної безпеки	Середня
2.2. Розголошення конфіденційної інформації, що зберігається на АРМ	Трудовий кодекс, трудовий договір	Людський фактор (шантаж, підкуп, погрози, помста, необережність)	Середня
2.3. Доступ з мереж загального користування до АРМ	Функціонує міжмережевий екран, провайдер забезпечує додаткову захист	Міжмережевий екран із застарілим програмним забезпеченням, застарілий антивірусний захист	Середня
3.1. Фізичний доступ порушника до документів, електронних носіїв	Встановлено елементи фортифікації, встановлена охоронна сигналізація	Користувачі не дотримуються заходів з інформаційної безпеки	Середня
3.2. Розголошення конфіденційної інформації, що зберігається на документах, електронних носіях, винос документів за межі контрольованої зони	Трудовий кодекс трудовий договір	Людський фактор (шантаж, підкуп, погрози, помста, необережність)	Середня
3.3. Несанкціоноване копіювання, друк і розмноження конфіденційних документів	Встановлено елементи фортифікації, встановлена сигналізація	Користувачі не дотримуються заходів по ІБ	Середня

Після складання приватної моделі загроз для ІС були виявлені можливі загрози, ймовірність яких вище, ніж низька. Для розробки політики безпеки вважаємо, що дані загрози є актуальними.

Після того, як складена приватна модель загроз була розроблена, для ІС були виявлені актуальні загрози. В першу чергу це:

– розголошення конфіденційної інформації (КІ), розташованої на сервері;

– знищення або псування КІ на серверах за допомогою спеціальних шкідливих програм, вірусів або черв'яків;

– копіювання КІ з сервера;

– доступ із зовнішньої мережі Інтернет до серверів об’єкта, що охороняється;

– фізичний доступ потенційного порушника до АРМ з подальшим копіюванням КІ;

– розголошення КІ, розташованої на АРМ співробітників;

– знищення або псування КІ за допомогою спеціальних шкідливих програм, вірусів або черв'яків;

– доступ із зовнішньої мережі Інтернет до АРМ;

– фізичний доступ потенційного порушника до документів і електронних носіїв (флешка, жорстких дисків, *CD, DVD)*;

– розголошення КІ, що знаходиться в документах, що виносяться за межі периметра охорони;

– несанкціоноване копіювання, друк або розмноження КІ.

2.3. Побудова моделі порушника

При побудові даної моделі в першу чергу всіх порушників можна розділити на дві основні групи – це зовнішні і внутрішні.

Під зовнішніми порушниками для ІС слідує розуміти в першу чергу конкуруючі організації, а також потенційні кримінальні та терористичні

угруповання, а також потенційні корупційні елементи, що знаходяться в органах влади.

Найчастіше діяльність даних порушників спрямована в першу чергу на будь-які пасивні носії КІ, а також на копіювання, псування або знищення її носіїв.

Також дії зовнішніх порушників можуть бути спрямовані на персонал, і можуть проявлятися у вигляді різних загроз або підкупу, з метою отримання необхідної інформації, яка становить комерційну таємну.

Також дії зовнішніх порушників можуть бути направлені на переманювання співробітників компанії.

Але найбільшу загрозу можуть представляти собою внутрішні порушники, так як вони мають доступ до інформації, який має статус КІ, або, наприклад, знати про існуючі способи захисту даної інформації.

Таким чином, внутрішніми порушниками можуть бути як нечисті на руку керівники організації, рядові співробітники, а також шахраї або аферисти.

Крім цього, варто звернути увагу на те, що співробітники мають високий рівень самооцінки і можуть бути незадоволені або рівнем заробітної плати, або відносинами з керівництвом компанії або рядовими співробітниками.

Таким чином, в таблиці 2.11 модель порушника можна представити таким чином:

Таблиця 2.11

Модель порушника

Порушник	Мотив дії	Потенційні можливості
Керівник	Власна вигода	Мають доступ до обладнання на якому зберігається / обробляється конфіденційна інформація. Мають права доступу до обладнання
Системний адміністратор, адміністратор безпеки	Образа, користь, помста, примус сторонньою організацією	

Закінчення таблиці 2.11

Співробітник	Образа, користь, помста, примус сторонньою організацією	Мають доступ до обладнання на якому зберігається / обробляється конфіденційна інформація. Мають права доступу до обладнання
Підрядник		У деяких випадках мають доступ до обладнання на якому зберігається / обробляється конфіденційна інформація
Колишній співробітник		Мають доступ до обладнання на якому зберігається / обробляється конфіденційна інформація з моменту звільнення до моменту закриття доступу до даних адміністратором.
Терористичні, екстремістські угруповання. Кримінальні структури. Конкуренти. Спеціальні служби іноземних держав	Власна вигода, помста, примус	Примус (залякування, підкуп) співробітників, здійснення хакерських атак (при наявності виходу в мережу)
Розробники, виробники, постачальники програмних, технічних засобів		Здійснення хакерських атак (при наявності виходу в мережу)

На підставі даної таблиці можна зробити наступні висновки. До можливих внутрішніх порушників можна віднести керівника, главу служби безпеки, системного адміністратора, співробітників ІС.

До зовнішніх порушників можна віднести конкурентів, колишніх співробітників, підрядників, розробників і виробників ПЗ, кримінальні угруповання.

Саме впровадження СКУД на основі виявлення загроз і порушників є одним з методів забезпечення безпеки об’єкта, що охороняється.

2.4. Вибір методики проектування СКУД

Інтеграція системи контролю доступу – важливий етап забезпечення інформаційної безпеки організації.

Дане рішення дозволяє пов'язувати облікові записи системи контролю доступу з обліковими записами IT-систем.

Інтегровані системи безпеки на базі відкритих архітектур, забезпечують роботу системи контролю доступу (безконтактної або біометричної) з будь-якою структурою каталогів. Завдяки сумісності рішення зі стандартними серверами, адміністратори інтегрованої системи безпеки можуть вести гнучку політику використання всіх існуючих в компанії баз даних.

Сервер повинен володіти каталогом і надавати можливість клієнтам через мережу працювати з цими каталогами, в т.ч. шукати в них елементи, завантажувати значення їх атрибутів [11,12].

Для забезпечення найвищого рівня взаємодії між СКУД і різними IT-додатками в інтегровані системи безпеки закладена можливість створення програм на макромові.

Для цього використовується стандартний інструментарій. До числа найбільш поширених завдань, в яких рішення забезпечує взаємодію інтегрованої системи з іншими IT-додатками відносяться:

– Створення облікового запису користувача в системі контролю доступу на базі відповідних облікових записів користувачів *Windows*;

– Деактивація облікового запису в *Windows* внаслідок деактивації відповідного пропуску (карти доступу, відбитка пальця);

– Створення скриптів для автоматичного переміщення даних між *HR*-системами та службами каталогів;

– Створення додатків, що забезпечують роботу модулів інтегрованої системи безпеки на базі мобільних пристроїв;

– Активація облікових записів для доступу до комп'ютерів з використанням карт доступу в приміщення.

2.5. Висновки до розділу

В межах даного розділу роботи була розроблена модель загроз і моделі порушника для об’єкту, що охороняється. Встановлено, що розробка та впровадження СКУД є актуальним та необхідним напрямком для забезпечення інформаційної безпеки організації. Також було розділено всі джерела загроз безпеці інформації на три основні групи: антропогенні джерела загроз (помилки експлуатації, помилки проектування і розробки компонентів АС, навмисні дії порушників і зловмисників; техногенні джерела загрози (аварії, збої і відмови устаткування (технічних засобів)); обумовлені стихійними джерелами (Стихійні лиха, катаклізми). Встановлено, що політика безпеки будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації. На етапі розробки політики безпеки було виділено підзадачі.

РОЗДІЛ 3
БАЗА ДАНИХ ТА РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1. Обґрунтування вибору складових системи.

На основі визначення моделі загроз і порушника та враховуючи те, що основну інформацію про систему можна отримати з комп'ютера, в межах даного розділу розглянемо побудову системи безпеки з впровадження СКУД на прикладі об'єкта, що охороняється, до якого надходять всі дані.

Для функціонування роботи апаратних пристроїв використовується спеціальне програмне забезпечення, за допомогою якого здійснюється управління контролем доступу.

Оформлення всіх пропусків в офіс здійснюється на пості охорони, розміщеному на вході.

На рис. 3.1 представлена схема організації СКУД.

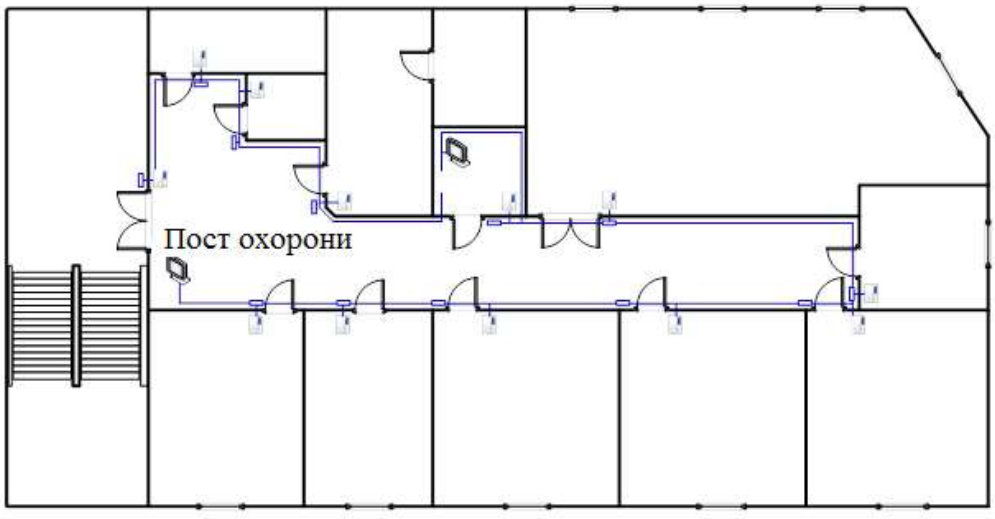

Рис. 3.1. Схема організації СКУД

В якості контролю управління доступу пропонується впровадити систему відеоспостереження, яка дозволить здійснювати контроль. На рис. 3.2 представлений план розміщення камер спостереження, які забезпечують повний контроль на об'єкті захисту.

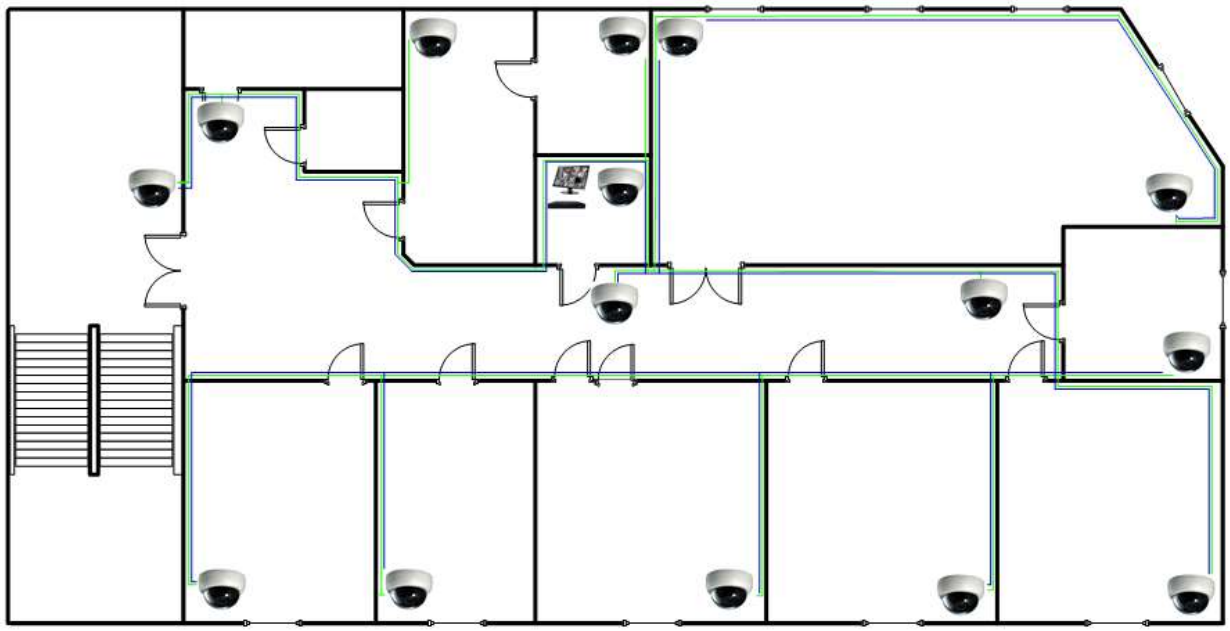

Рис. 3.2. Розроблена система відеоспостереження

Прокладка кабелю буде здійснюватися під підвісною стелею. Спеціальний сервер для відеоспостереження буде розміщуватися в серверному приміщенні на окремій телекомунікаційної стійці. Доступ до даного пристрою здійснюється тільки за допомогою пароля, який є тільки у керівника служби безпеки і системного адміністратора на об'єкті захисту. Монітори відеонагляду розміщуються на пості охорони і дозволяють виробляти спостереження заданих секторів об'єкта.

Запис відеопотоку здійснюється на спеціальне мережеве сховище цілодобово. Впровадження ПІБ має на увазі зміну схеми організації мережі (представлена на рис. 3.3).

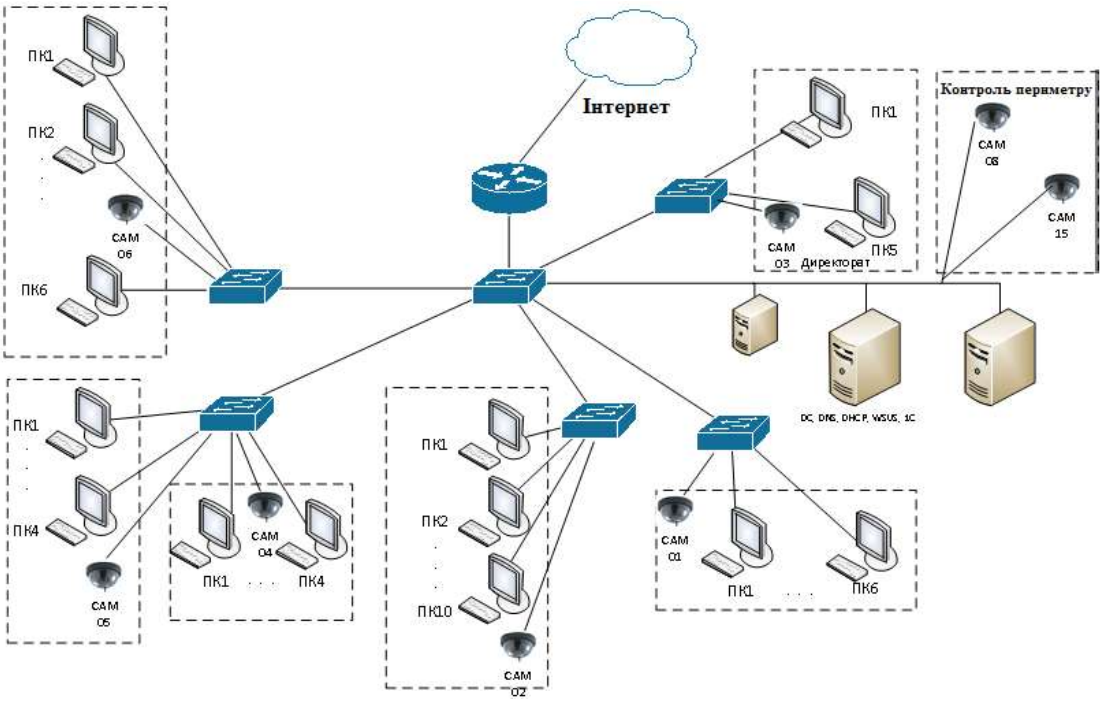

Рис. 3.3. Модернізована схема мережі

Таким чином, в роботі пропонується використовувати 15 камер відеоспостереження купольного типу. Дані камери досить популярні для впровадження на об'єктах малого і середнього бізнесу.

У таблиці 3.1 наведені основні виробники даних камер. Перевага віддається камері з 1.3 *Mnc*, так як на сьогоднішній день камери з таким дозволом є досить популярним засобом для організації відеоспостереження. Дані камери мають досить великий кут огляду в базовій комплектації.

Таблиця 3.1

Вибір купольної камери

Марка	Кількість пікселів	Кут огляду	Вартість, грн.
ActiveCam AC-D8111IR2W	1,3 *Mnc*	74,7	2990
AHD MT-DW960IP	1,3 *Mnc*	80	3700
MDC-i8260VTD	1,3 *Mnc*	78	4800

Всі камери спостереження мають веб-сервер для віддаленого доступу. Підключення даних камер здійснюється за допомогою кабелю витої пари.

На підставі таблиці 3.2 робимо вибір на користь виробника *AHD*. Дана камера має максимальний кут огляду, при цьому вартість даної камери середня в порівнянні з конкурентами.

Мініатюрна камера має ІЧ-підсвічування, що дозволить працювати цій камері в темний час доби.

Виробник гарантує ступінь захисту *IP66*. Для збереження відеопотоку з камер спостереження необхідно використовувати *IP*-відеореєстратор. Для виключення можливих колізій при роботі обладнання різних виробників буде використовуватися *IP*-відеореєстратор *MATRIXM-16IPMC*.

Реєстратор підтримує функцію хмарного сховища даних. Також дане обладнання дозволяє проводити спостереження в реальному часі або відтворювати необхідні записи з зовнішніх відеокамер. Підтримка жорсткого диска до 6 *ТБ* дозволяє зберегти відео в форматі 1280 × 960 до 7 діб.

У таблиці 3.2 наведена загальна вартість оснащення системою відео спостереження офісу системи.

Таблиця 3.2

Кошторисна вартість на обладнання

Найменування	Ціна, грн.	кількість	Вартість, грн.
IP-камера	3700	15	55500
Відеореєстратор *MATRIXM-16IPMC*	7050	1	7050
Разом			62550
Невраховані витрати,%	10		6255
Всього			68805

Таким чином, витрати на оснащення комплексом відеоспостереження на об'єкті захисту складають 68 805 грн.

Ґрунтуючись на даному типі топології пропонується використання шлюзу контролю доступу для централізованого управління доступом. Такий підхід дозволяє спростити процес впровадження контекстного контролю доступу, і збігається з підходами, що використовуються в реальних системах.

Процес розбивається на чотири етапи [11,12]:

1. Аналіз мережевої взаємодії. Пристрої взаємодіють один з одним через шлюз контролю доступу, в результаті чого ця задача стає очевидною;

2. Застосування правил контролю доступу. На даному етапі запити між пристроями фільтруються відповідно до правил контролю доступу;

3. Оновлення контексту. Виробляється на основі отриманих раніше запитів і безпосереднього опитування пристроїв. Журнали значень параметрів і виконаних операцій зберігаються як частина контексту, оскільки відображають процес переходу в новий стан;

4. Оновлення правил контролю доступу. На основі оновленого контексту і політики контекстної моделі проводиться оновлення правил контролю доступу та приведення їх у дію.

В якості прикладу розглянемо сценарії, які демонструють алгоритми функціонування системи.

Розглянемо сценарій, який демонструє базові можливості захисту.

Нехай застосовується скомпрометований смартфон, з використанням якого може відкриватися дверний замок. Для обмеження можливостей порушника створено правило, що пропонує підвищення рівня цілісності дверного замку при дотриманні умов за часом, відсутності руху і освітлення. В такому випадку відкриття замку з використанням смартфону може зробити тільки людина.

В ході сценарію задіяні такі правила контекстної моделі:

Constraint (світло == *true*, людина_в_приміщенні, *true*)

Constraint (рух == *true*, людина_в_приміщенні, *true*)

Constraint (людина_в_приміщенні == *false and* (1:00 <= час <= 7:00), двері_закриті == *true*)

Execute (смартфон, двері, відкрити)

Execute (смартфон, освітлення, включити)

Execute (двері, двері, відкрити)

Description (двері, відкрити) –> {двері_закриті: *false*}

Прийняте рішення на основі даних правил отримують таким чином:

1. Оскільки освітлення вимкнене і рух відсутній, в контексті зберігається параметр, який свідчить про відсутність людини в приміщенні;

2. За часом і відсутності людини в приміщенні виводиться обмеження на стан двері. У поточному контексті двері повинні бути закриті;

3. Дія відкриття дверей викликає порушення контексту, оскільки змінює контекст неприпустимим чином. В результаті необхідно розв'язати конфлікт, викликаний можливістю відкриття дверей зі смартфона;

4. Конфлікт може бути дозволений зниженням рівня цілісності смартфона або підвищенням рівня цілісності дверного замка. Оскільки зниження рівня смартфона призведе до заборони виконання інших дій, які не викликають конфліктів, приймається рішення на користь підвищення рівня цілісності замка.

В якості основних програмно-апаратних засобів на об'єктах захисту використовуються спеціальні сервіси, які функціонують в операційних системах на автоматизованих місцях працівників.

Уже багато років на ринку засобів захисту програм від несанкціонованого тиражування присутні так звані апаратні ключі захисту (*Dongles*).

На об'єкті захисту пропонується використовувати спеціальний міжмережевий екран, який робить аналіз проходження через нього потоку трафіку.

Одночасно з цим проводиться реєстрація подій і тривожна сигналізація в разі виявлення загрози. Звичайно екранують системи робляться несиметричними.

Для екранів визначаються поняття "всередині" і "зовні", причому, в завдання екрану входить захист внутрішньої мережі від потенційно ворожого оточення.

Крім того, ММЕ може використовуватися в якості корпоративної відкритої частини мережі, видимої з боку *Internet*.

Так, наприклад, у багатьох організаціях ММЕ використовуються для зберігання даних з відкритим доступом, як, наприклад, інформацію про продукти та послуги, файли з баз *FTP*, повідомлення про помилки і так далі [13,14].

У таблиці 3.3 наведені характеристики основних мережевих екранів.

Таблиця 3.3

Порівняння мережевих екранів

Продукт	Тип	Платформа	Особливості
Solstice Firewall	Комплексний екран	*SunOS, UNIX, Solaris*	Реалізує політику безпеки: всі дані, які не мають явного дозволу – відкидаються. У процесі роботи фільтри пакетів на шлюзах і серверах генерують записи про всі події, які запускають механізми тривоги, що вимагають реакції адміністратора
Black Hole	Екранує шлюз прикладного рівня	Різні апаратні платформи	Не використовує механізм фільтрації пакетів. Принцип дії: то, що явно не дозволено, є забороненим. Реєструє всі дії сервера, попереджає про можливі порушення. Може використовуватися як двонаправлений шлюз
Border Ware FirewallServer	Екранує шлюз прикладного рівня	*UNIX, Windows, DOS*	Програмний засіб захисту, що забезпечує роботу під керуванням ОС. Дозволяє фіксувати адреси, час, спроби, використовуваний протокол
ALF (Application LayerFilter)	Екранує шлюз прикладного рівня	*BSDI*	Може фільтрувати *IP*-пакети по адресам, діапазонам портів, протоколам і інтерфейсам
ANS Inter Lock Service	Екранує шлюз прикладного рівня	*UNIX*	Використовує програми-посередники для служб *Telnet, FTR, HTTR*. Підтримує шифрування з'єднання точка-точка, причому, в якості засобів автентифікації можуть використовуватися апаратні

Продовження таблиці 3.3

Brimstone	Комплексний екран	*SunOS*, *BSDI* на *Intel*, *IRIX* на *INDY* і *Challenge*	Для аналізу використовує час, дату, адресу, порт і т.д. Включає програми-посередники прикладного рівня для служб *Telnet*, *FTR*, *SMTP*, *X11*, *HTTP*, *Gopher* та ін. Підтримує більшість пакетів апаратної автентифікації
Centri	Екранує шлюз прикладного рівня	*SunOS, BSDI, Solaris, HP-UX, AIX*	Закрита мережа бачиться ззовні як єдиний хост. Має програми-посередники для служб: електронної пошти, протоколу *FTR* і ін. Реєструє всі дії сервера, попереджає про порушення
CONNECT	Екранує шлюз прикладного рівня	*UNIX*	Є програмним продуктом, що забезпечує захист інформації від несанкціонованого доступу при з'єднанні закритою і відкритою мережами
Digital Firewallfor UNIX	Комплексний екран	*DigitalAlpha*	Представляє можливості екрануючого фільтра і шлюзу прикладного рівня

Закінчення таблиці 3.3

Firewall IRX Router	Екранує маршрутизатор	*DOS, MS-Windows*	Дозволяє зробити аналіз мережі з метою оптимізації мережевого трафіку, безпечно зв'язати локальну мережу
Firewall-1	Комплексний міжмережевий екран	*Intel x86, SunSparc*	Забезпечує захист від хакерських нападів типу *address-spoofing* (підробка адрес пакетів) і представляє комбінацію засобів захисту мережевого і прикладного рівнів
Firewall-1 / VPN-1	Комплексний міжмережевий екран	*Intel x86, SunSparc*	Являє відкритий інтерфейс програми *OPSEC API.* Забезпечує: виявлення комп'ютерних вірусів; сканування *URL.* блокування *Java* і *ActiveX*; підтримку протоколу *SMTP*; фільтрацію *HTTP*; обробку протоколу *FTP*
Fortinet FG-60E	Міжмережевий екран	Різні апаратні платформи	Простота адміністрування, масштабованість мережі, централізоване управління, поділ повноважень, висока продуктивність

В якості ММЕ обираємо *Fortinet FG-60E*.

Пристрої комплексної мережевої безпеки *FortiGate-60E* забезпечують захистом малі офіси, відділення та роздрібні мережі. Основою пристрою є технологія *FortiASIC System on a Chip 3 (SOC3)*, яка забезпечує повний набір всіх захисних функцій для захисту програм і даних.

Проста схема ліцензування за пристрій, вбудована консоль управління, багатий набір інтерфейсів, а так само можливість віддаленого управління значно знизять вартість закупівлі, обслуговування та управління. Можливості та переваги *FortiGate-60E* [15].

Повний функціонал безпеки – міжмережевий екран, система запобігання вторгнень, контроль додатків, *VPN* і веб-фільтрація – включені в ціну єдиної підписки Система ліцензування "за пристрій" гарантує, що кількість користувачів обмежена тільки продуктивністю системи, що дозволяє економити на операційних витратах.

Простота установки і першого запуску пристрою за допомогою *FortiExplorer.* Автоматизоване оновлення підписок в режимі реального часу за допомогою сервісів підписки *FortiGuard*.

Рис. 3.4. Зовнішній вигляд міжмережевого екрану *Fortinet FG-60E*

В рамках даного розділу розглянемо також існуюче антивірусне ПЗ пропоноване для установки в корпоративних мережах.

У таблиці 3.4 наведено аналіз існуючого ПЗ.

Таблиця 3.4

Порівняльний аналіз антивірусного ПЗ

Назва	Термін ліцензії	Можливості	Ціна, грн.
Dr. Web «Універсальний»	1 рік / 40 ПК	Центр управління *Dr.Web* *Desktop Security Suite* *Server Security Suite* *Mail Security Suite* *Gateway Security Suite*	31275
Kaspersky Security	1 рік / 40 ПК	Підтримка платформ *Windowd, Mac, Android*; Захист від шкідливого ПЗ; Захист антифішинга; Резервне копіювання; Захист від спаму.	51282
ESET NOD32 Business Edition	1 рік / 35 ПК	Захист робочих станцій; Захист мобільних пристроїв; Захист файлових серверів.	56151

Дані таблиці дають право для того, щоб віддати перевагу для вибору антивірусного ПЗ – *Dr. Web* «Універсальний».

Даний продукт добре зарекомендував себе на ринку. В пакеті призначеному для бізнесу на 40 персональних комп'ютерів також пропонуються додаткові опції, які роблять даний комплект більш привабливим серед існуючих антивірусних програм.

Ще одним інструментом для забезпечення мережевої безпеки є наявність системи моніторингу. Моніторинг дозволяє системному адміністратору системи розумного міста відстежувати рух пакетів всередині локальної мережі.

На ринку послуг існують безліч продуктів, як платних, так і безкоштовних [16].

Проведемо порівняльний аналіз найбільш популярних продуктів. У таблиці 3.5 наведені основні системи моніторингу. Розглянемо лише безкоштовні продукти моніторингу, так як немає необхідності купувати систему.

Таблиця 3.5

Порівняльний аналіз систем моніторингу

Система моніторингу	Переваги
Zabbix	Відмінна функціональність; можливість масштабування; зручна система оповіщень; можливість намалювати карту мережі; є агенти під *Windows*; можливість підключення скриптів.
Nagios	Стабільна і проста система; великий набір плагінів; моніторить тисячі хостів
Cacti	Зручний, сучасний веб інтерфейс; красиві, інформативні графіки.
Monit	Існування процесу по *PID*; ресурси займані процесом; робота певного порту (*TCP* / *UDP*); відповідь протоколу за певним портом (*SMTP*, *SSH*, *HTTP* ...); обсяг і вільний простір в файловій системі; права доступу до файлу або каталогу. комбінація методів перевірки; сповіщення по *E-mail*; підтримує зовнішні скрипти; має веб-інтерфейс.

Вибір зробимо на користь використання *Zabbix*. З причини простого інтерфейсу і можливості оповіщення за допомогою різних засобів.

Крім цього, система моніторингу має свій *Web*-інтерфейс, що дозволяє здійснювати моніторинг віддалено.

3.2. Організація зв’язку в СКУД

Розглянемо безпосередньо схему організації зв’язку в СКУД [17].

Визначимо структурні елементи, які використовуються при побудові системи на основі існуючого рішення [17]:

– мережеві контролери *Z-R5 net 8000 IronLogic*;
– зчитувачі безконтактних проксіміті карт *Matrix II (EM-Marin 125KHz)*;
– турнікет *FORMA 5.3*;
– дверні електромагнітні замки *YM-180*;
– кнопки відкриття дверей;
– датчики відкриття дверей Страж П-408;
– блоки живлення ІБПС-12-1;
– конвертор інтерфейсів *USB / RS-485, Z-397 Guard IronLogic*;
– комп'ютер з програмним забезпеченням і базою даних;
– безконтактні карти *EM-Marin ISO 125 kHz*;

Структурна схема системи зібрана з перерахованих вище компонентів представлена рис. 3.5.

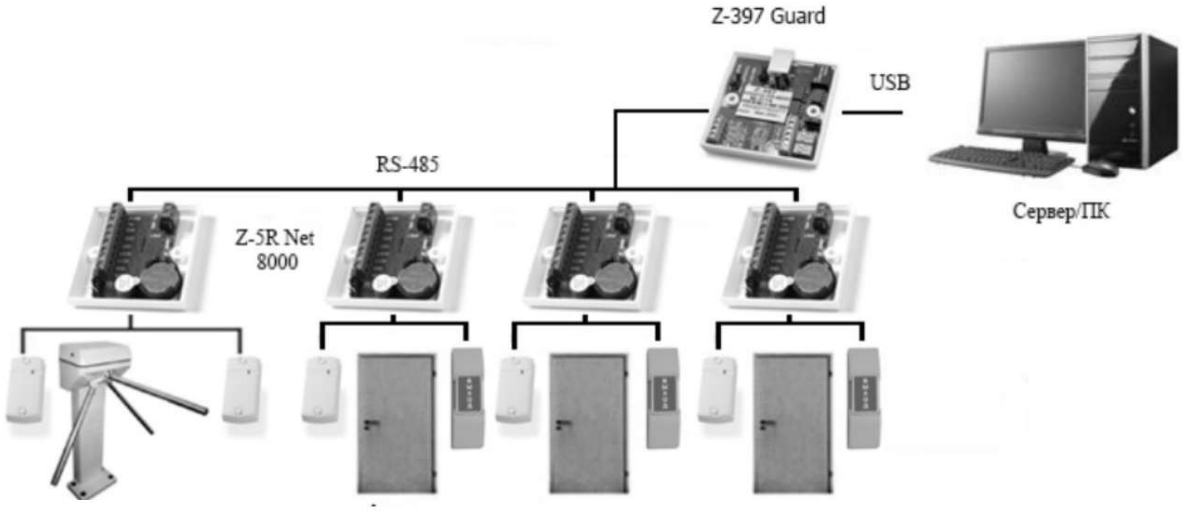

Рис. 3.5. Структурна схема організації зв’язку в СКУД

Контролери об'єднуються в мережу з використанням інтерфейсу *RS-485* і працюють під управлінням комп'ютера. Спеціалізоване ПЗ, дозволяє програмувати контролери, управляти їх роботою.

Схема підключення елементів до контролеру представлена на рис. 3.6.

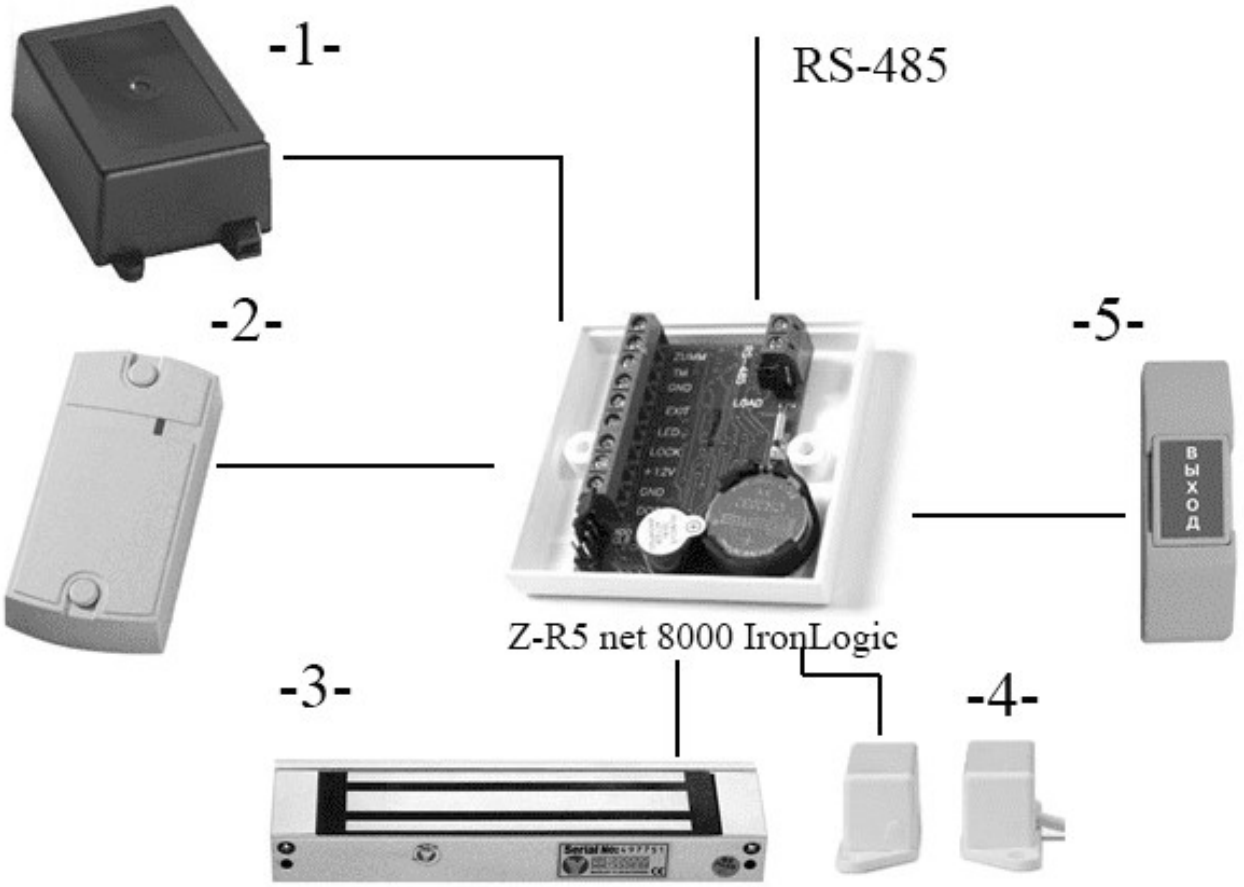

Рис. 3.6. Схема підключення елементів до контролеру

Детальніше розглянемо обраний мережевий контролер (рис. 3.7).

Рис. 3.7. Мережевий контролер СКУД

Технічні характеристики:

– Кількість ключів: 8168 *шт*.;
– Кількість подій, які запам'ятовуються: 8192 *шт*.;
– Типи записуваних ключів: простий, майстер, який блокує;
– Інтерфейс зв'язку зі зчитувачем: *Dallas TM (iButton), Wiegand* 26;
– Наявність перемички для вибору типу замка: є;
– Світлова та звукова індикація режимів роботи: є;
– Установка тривалості відкривання замку: від 0 до 25,5 *с;*
– Вихід: транзистор 1 *шт*.;
– Інтерфейс зв'язку: *RS-485;*
– Відстань контролера по *RS-485*: до 1200 *м*.;
– Напруга живлення: 8–18*V DC;*
– Струм споживання: 30*мА;*
– Струм комутації: 5*А;*
– Захист від неправильного включення: є;
– Робоча температура: –30 + 40 ° *С;*
– Габаритні розміри (*мм*): 65×55×12.

Режими роботи:

Повернення до нормального режиму – забезпечує прохід по простим і блокуючим ключам.

Режим *ACCEPT* – дозволяє відновити базу даних ключів. У режимі *ACCEPT* контролер дозволяє доступ усім ключам і при цьому заносить їх *ID* в свою пам'ять. Тим самим, пропрацювавши кілька днів в режимі *ACCEPT*, контролер формує нову базу даних ключів.

Режим *TRIGGER* – управління роботою замку. Один дотик ключа – замок закритий; друге торкання ключа – замок відкритий. Режим *TRIGGER* зручний у випадках, де необхідно відкривати або блокувати двері на певний період (робочий день, перерва і т.д.).

Режим Блокування – відкритий прохід по блокуючим ключам, простим ключам прохід закритий.

Режим Вільний прохід – замок завжди знеструмлений.

В якості модернізації існуючого рішення пропонується інтеграція СКУД з *LDAP*-сервером.

Тут важливо виділити переваги даного сервера [18]:

1. *LDAP* надає стандартизовані як віддалений, так і локальний методи доступу до даних. Таким чином, цілком реально замінити одну реалізацію *LDAP* на іншу, абсолютно не впливаючи на зовнішній інтерфейс доступу до даних.

2. Оскільки в *LDAP* використовуються стандартизовані методи доступу до даних, клієнти і сервери *LDAP* можуть розроблятися окремо або бути отримані з різних джерел.

3. *LDAP* надає метод, за допомогою якого дані можуть бути переміщені (делеговані) в кілька місць, не зачіпаючи при цьому зовнішнього доступу до цих даних. Використовуючи метод відсилань *LDAP*, дані можуть бути переміщені на альтернативні *LDAP*-сервери шляхом тільки зміни операційних параметрів. Таким чином, можна побудувати розподілені системи, можливо, з даними, які надходять з окремих автономних організацій, забезпечуючи при цьому для своїх користувачів єдине, послідовне уявлення цих даних.

Інформаційна модель *LDAP* представлена на рис. 3.8.

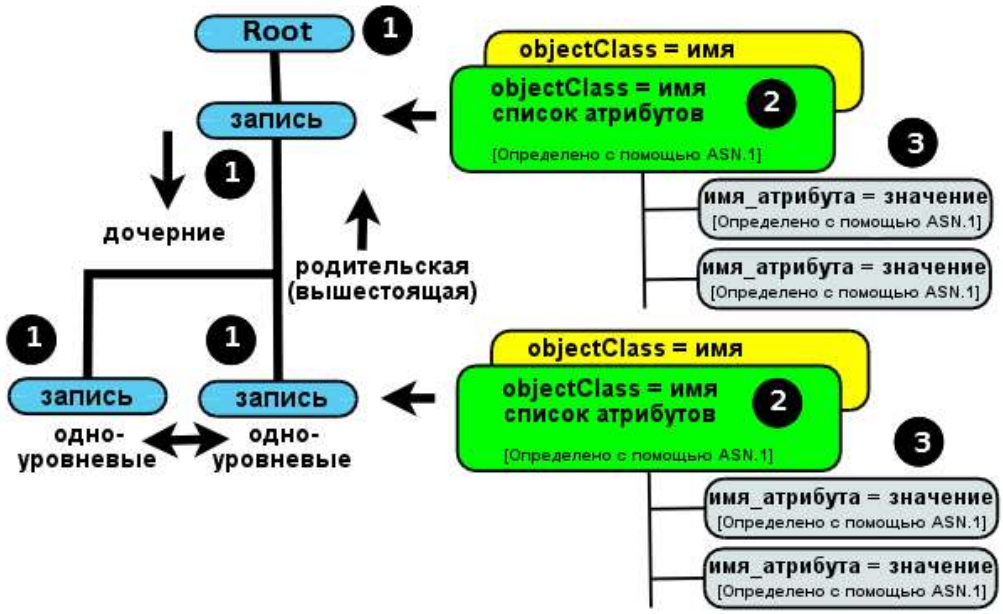

Рис. 3.8. Інформаційна модель *LDAP* [19]

Системи *LDAP* можуть бути налаштовані на реплікацію даних на один або кілька серверів *LDAP* або одному або декільком додаткам тільки за рахунок операційних параметрів, без необхідності додати ще трохи коду або зміни зовнішнього доступу до даних.

3.3. Структура бази даних СКУД

На першому етапі збирають і оптимізують дані: збір даних системою КУД, їх фільтрація і агрегування [18].

На етапі збору даних СКУД реєструє всі події, що надходять від контролерів системи, і інциденти відвідувачів контролю. Отримані набори даних не піддаються аналізу без попередньої їх обробки, тому вони надходять на етап фільтрації, де зайві і некоректні дані відсіваються. Дані, отримані від СКУД і минулі етапи фільтрації, надходять на етап агрегування і приймають формат атрибутів (таблиця 3.6).

Таблиця 3.6

Вхідні дані системи виявлення загроз

Атрибут	Опис
X1={0|1|X}	Ознака робочого часу
X2={0|1|X}	Перше відвідування об'єкта
X3={0:n|X}	Рівень доступу карти
X4={0:n|X}	Рівень доступу об'єкта
X5={0|1|X}	Спроба доступу до забороненого об'єкта
X6={0:n|X;Obj;L}	Кількість спроб доступу; об'єкт; рівень доступу об'єкта
X7={0|1|X;Obj;L}	Ознака відмови обладнання; об'єкт; рівень доступу об'єкта
X8={0:n|X}	Множинний вхід в різні об'єкти без виходу
X9={0|1|X;Obj;L}	Відключення електроживлення; об'єкт; рівень доступу
X10={0|1|X;Obj;L}	Відкриття дверей, без події проходу; об'єкт; рівень доступу об'єкта
X11={0|1|X;Obj;L}	Не замкнені двері; об'єкт; рівень доступу об'єкта
X12={0|1|X}	Доступ всередині об'єкту, що охороняється, без проходу на територію підприємства

Примітка:

0 – критерій не встановлений;

1 – критерій встановлений;

X – критерій не визначено;

0:n – цілочисельне значення;

Obj – об'єкт, під ним розуміється приміщення або вся будівля об'єкту, що охороняється в цілому;

L – рівень доступу об'єкта.

На другому етапі вибирають методи для вирішення завдання [18].

Спочатку складається логічна модель, яка враховує модель представлення даних без прив'язки до конкретної СУБД (рис. 3.9).

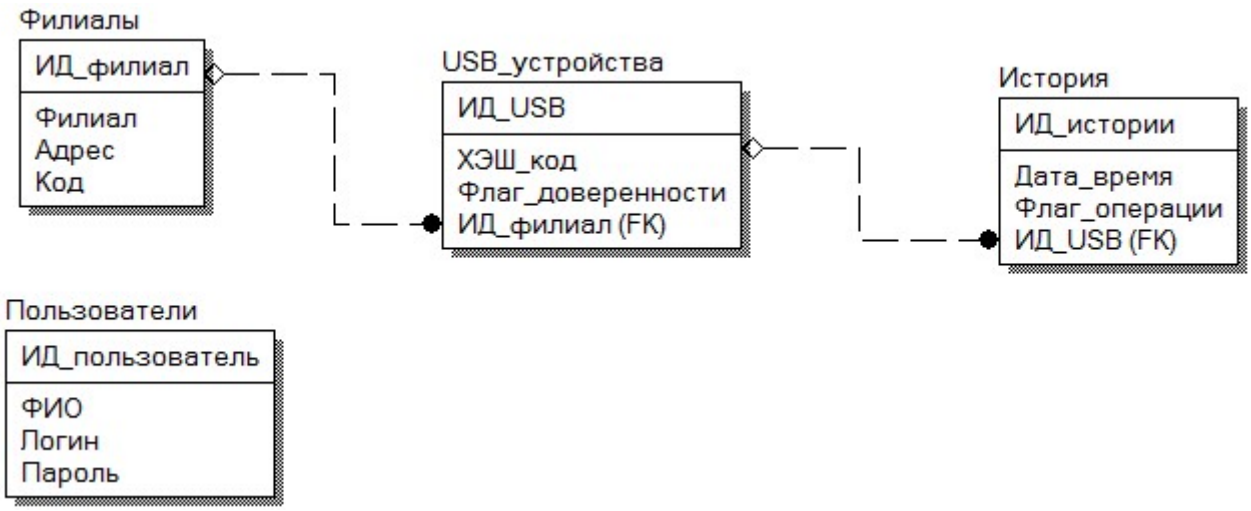

Рис. 3.9. Логічна модель БД

Проектування бази даних може проводитися в засобі проектування – *ERWin Data Modeler*, в якості прикладу розглянемо саме цей засіб [19,20].

Логічна модель складена російською мовою, так як українська мова в даному засобі відсутня.

Перехід до фізичної моделі дуже простий. Для цього треба просто змінити тип в настройках (рис. 3.10).

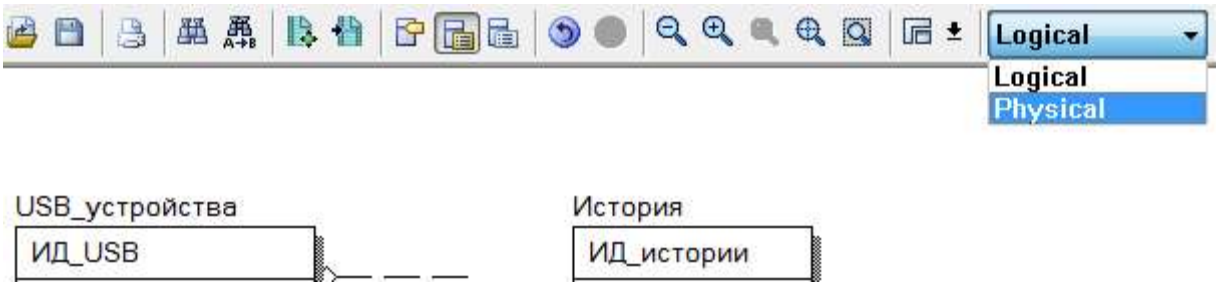

Рис. 3.10. Зміна типу моделі на фізичну

Після зміна можна в налаштуваннях моделі задати відображення типів даних (рис. 3.11).

Фізична модель представлена на рис. 3.12.

Фізичну модель бажано перевести на латинський алфавіт, щоб не було проблем з кодуваннями.

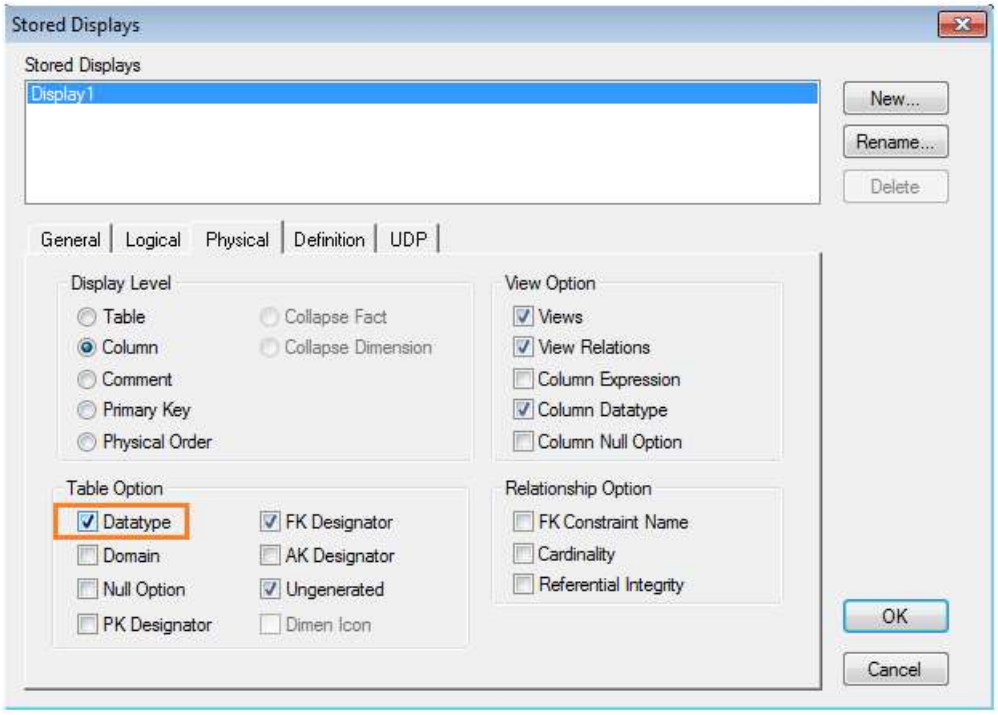

Рис. 3.11. Вибір відображення типів даних

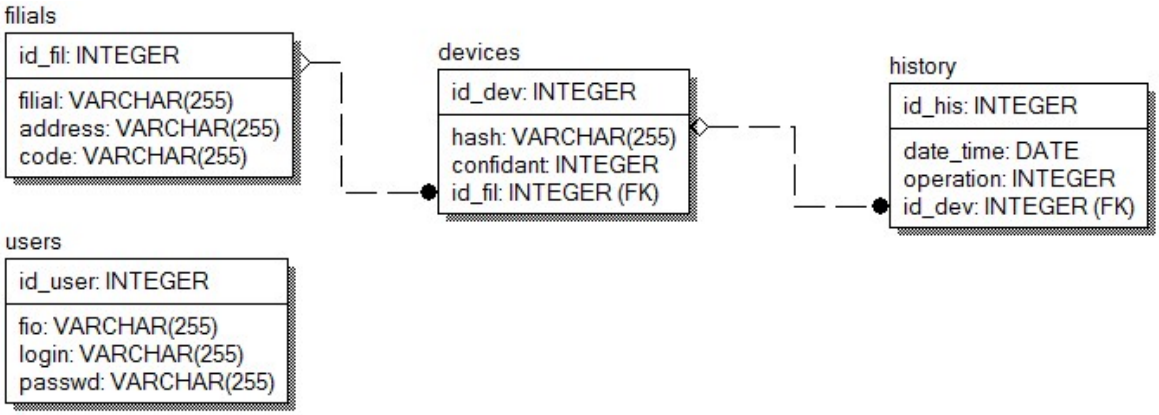

Рис. 3.12. Фізична модель

Після проектування фізичної моделі можна створити базу даних в *MySQL*. Робиться це за допомогою *phpmyadmin* (рис. 3.13).

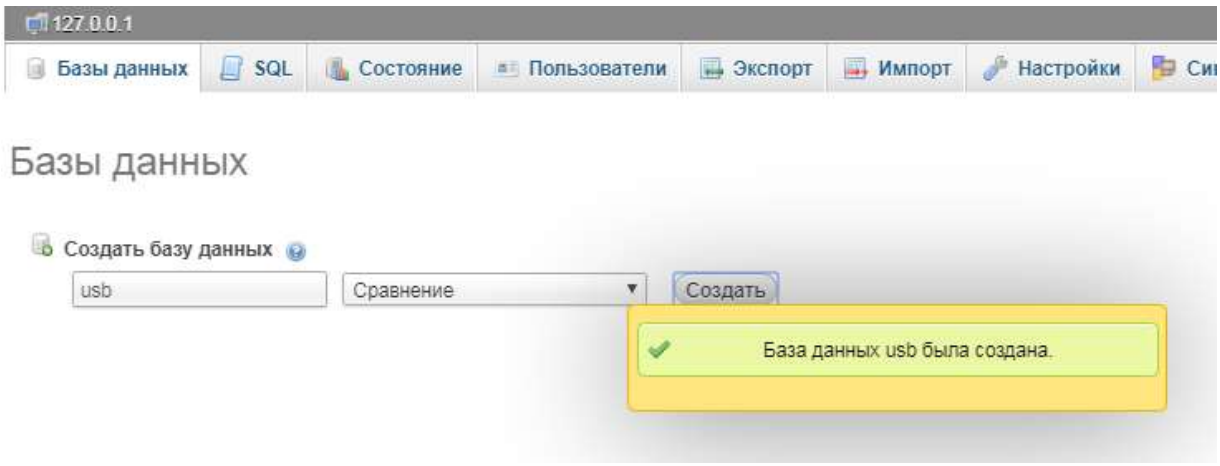

Рис. 3.13. Створення бази даних в *phpadmin*

Тепер можна скористатися інструментом експорту фізичної моделі з *ERWin* в СУБД *MySQL* (рис. 3.14).

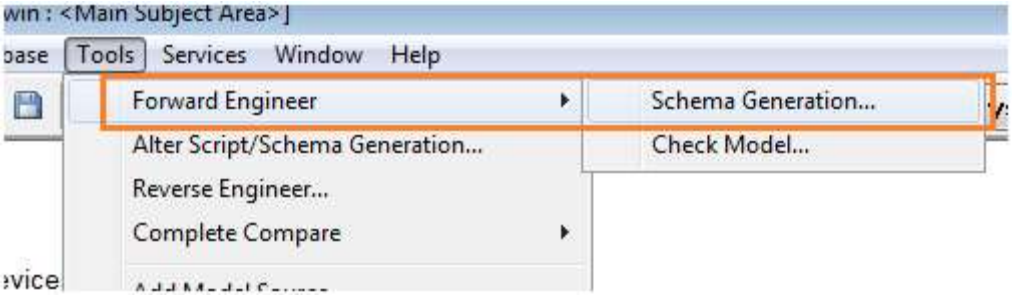

Рис. 3.14. Інструмент експорту фізичної моделі з *ERWin* в СУБД *MySQL*

Інструмент запропонує вибрати драйвер зв'язку з СУБД. Тестування з'єднання з БД пройшло успішно (рис. 3.15).

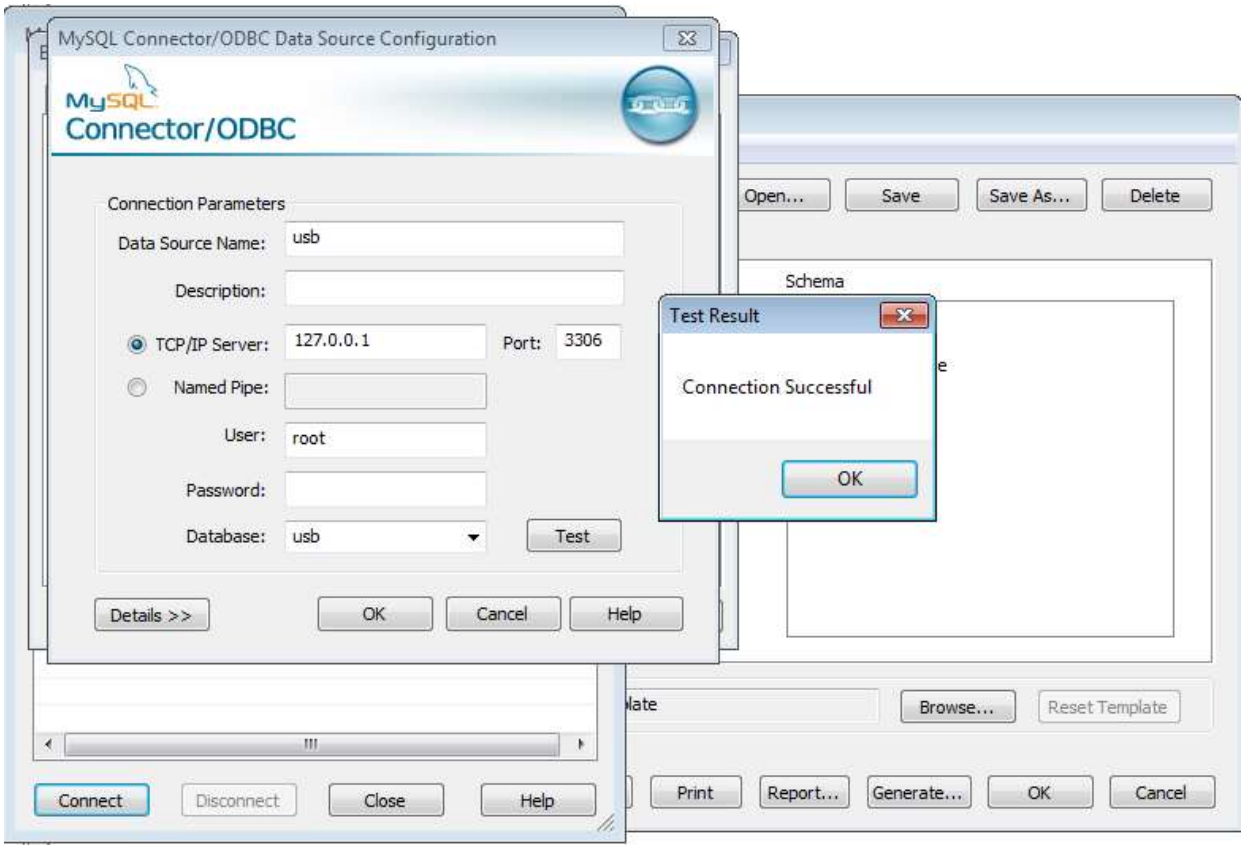

Рис. 3.15. Тестування зв'язку з СУБД

Після цього *ERWin* автоматично експортує БД в СУБД (рис. 3.16).

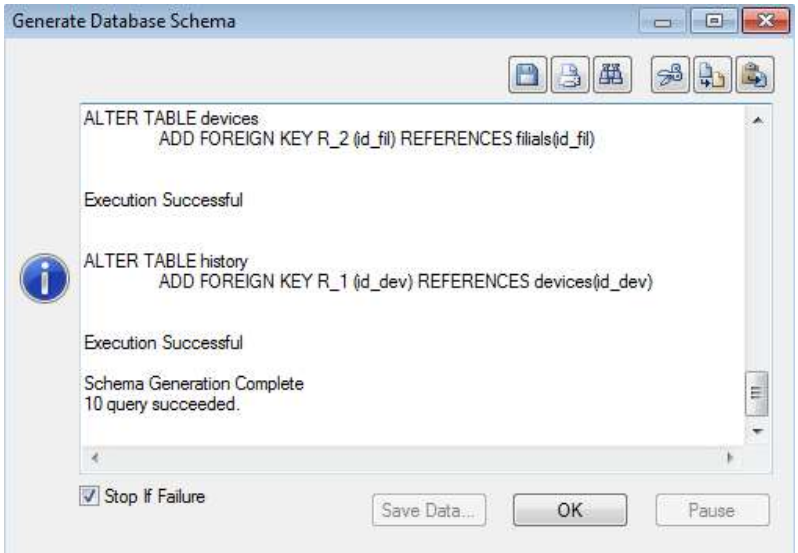

Рис. 3.17. Успішний експорт фізичної моделі в СУБД

Створена база даних в СУБД представлена на рис. 3.18.

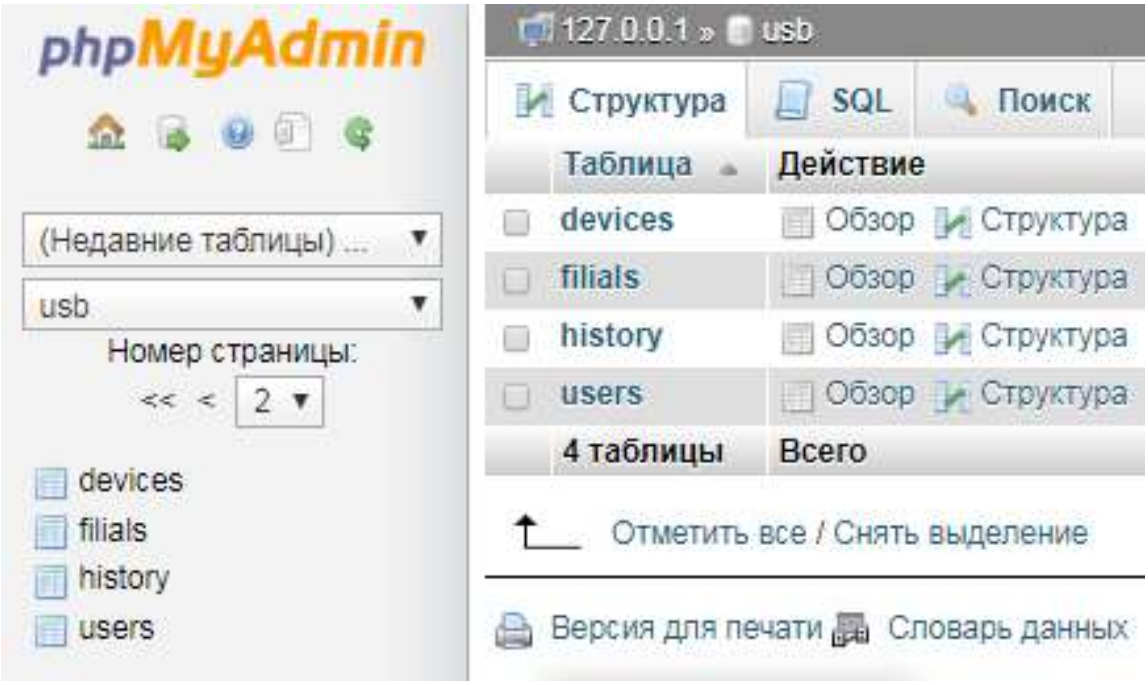

Рис. 3.18. Створена БД в СУБД *MySQL*

Цю БД можна переглянути на діаграмі (рис. 3.19).

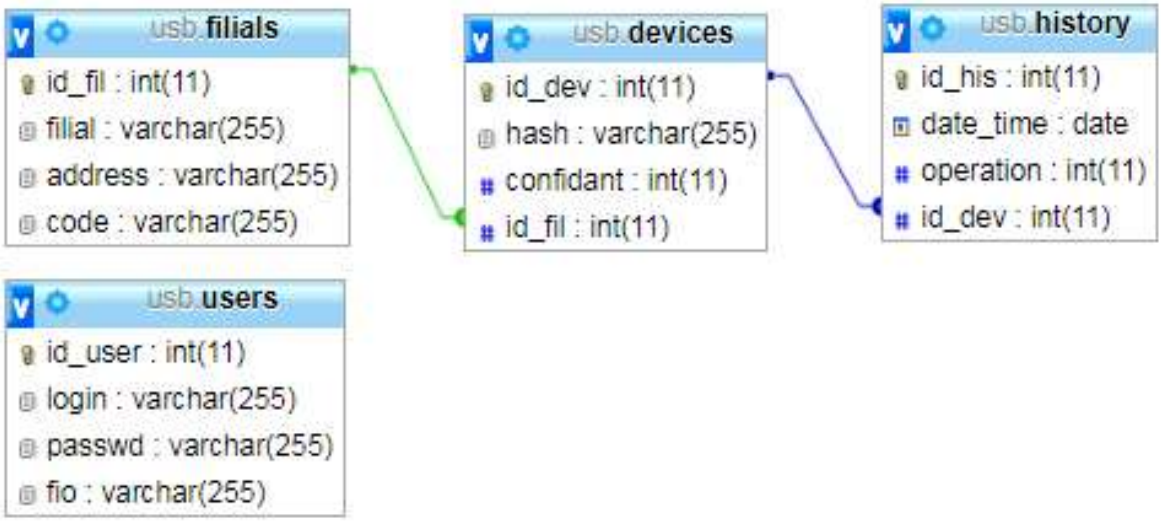

Рис. 3.19. Діаграма БД

Для даної системи видача інформації про підключення несанкціонованого пристрою чи доступу повинна надходити від джерела відразу по пригоді.

3.4. Висновки до розділу

В результаті написання даного розділу дипломної роботи було розглянуто вибір обладнання для забезпечення інформаційної безпеки об’єкта, що охороняється. Наведено основні складові частини структурної схеми відомої СКУД, для якої запропоноване рішення модернізації, яке полягає в інтеграції системи з *LDAP*-сервером. Наведена структура бази даних для СКУД.

ВИСНОВКИ

В результаті написання дипломної роботи було розглянуто впровадження та модернізація існуючого рішення системи КУД на об’єкт, що охороняється.

В результаті написання першого розділу дипломної роботи встановлено, що системи контролю доступу виконують ідентифікаційну аутентифікацію і авторизацію користувачів і об'єктів, оцінюючи необхідні облікові дані для входу, які можуть включати паролі, особисті ідентифікаційні номери (*PIN*-коди), біометричне сканування, токени безпеки або інші чинники аутентифікації. Багатофакторна аутентифікація, яка потребує двох або більше факторів аутентифікації, часто є важливою частиною багаторівневого захисту для захисту систем контролю доступу.

Ці заходи безпеки працюють, ідентифікуючи людину або об'єкт, перевіряючи, що ця особа або додаток є тим, ким або чим воно себе називає.

Мета контролю доступу – мінімізувати ризик несанкціонованого доступу до фізичних і логічних систем. Контроль доступу – це фундаментальний компонент програм забезпечення відповідності вимогам безпеки, що забезпечує наявність технологій безпеки і політик контролю доступу для захисту конфіденційної інформації, наприклад даних клієнтів. Більшість організацій мають інфраструктуру і процедури, що обмежують доступ до мереж, комп'ютерних систем, додатків, файлів і конфіденційних даних, таких як особиста інформація та інтелектуальна власність.

Існує багато типів програмного забезпечення і технологій для контролю доступу, і часто кілька компонентів використовуються разом для підтримки контролю доступу. Програмні інструменти можуть бути локальними, в хмарі або їх гібридом. Вони можуть зосередитися в першу чергу на управлінні внутрішнім доступом компанії або можуть зосередитися зовні на управлінні доступом для клієнтів.

Деякі з типів програмних інструментів управління доступом включають наступне:

– додатки для звітності і моніторингу;

– інструменти управління паролями;

– інструменти забезпечення;

– репозиторії особистості;

– інструменти застосування політики безпеки.

В другому розділі роботи було розглянуто розробку моделі загроз та порушника.

При аналізі та класифікації джерел загроз інформації, виходили з припущення, що для однієї і тієї ж загрози методи відображення для зовнішніх і внутрішніх джерел можуть бути різними.

Особливу групу внутрішніх джерел становлять спеціально впроваджені і завербовані агенти з числа допоміжного, основного, технічного персоналу і представників відділу інформаційної безпеки.

Було вирішено розділити всі джерела загроз безпеки інформації на три основні групи:

– антропогенні джерела загроз (помилки експлуатації, помилки проектування і розробки компонентів АС, навмисні дії порушників і зловмисників;

– техногенні джерела загрози (аварії, збої і відмови устаткування (технічних засобів));

– обумовлені стихійними джерелами (стихійні лиха, катаклізми).

Основні загрози, які визначені в другому розділі:

В першу чергу це:

– розголошення конфіденційної інформації (КІ), розташованої на сервері;

– знищення або псування КІ на серверах за допомогою спеціальних шкідливих програм, вірусів або черв'яків;

– копіювання КІ з сервера;

– доступ із зовнішньої мережі Інтернет до серверів об’єкта, що охороняється;

– фізичний доступ потенційного порушника до АРМ з подальшим копіюванням КІ;

– розголошення КІ, розташованої на АРМ співробітників;

знищення або псування КІ за допомогою спеціальних шкідливих програм, вірусів або черв'яків;

– доступ із зовнішньої мережі Інтернет до АРМ;

– фізичний доступ потенційного порушника до документів і електронних носіїв (флешка, жорстких дисків, *CD*, *DVD*);

– розголошення КІ, що знаходиться в документах, що виносяться за межі периметра охорони;

– несанкціоноване копіювання, друк або розмноження КІ.

До можливих внутрішніх порушників можна віднести керівника, главу служби безпеки, системного адміністратора, співробітників ІС.

До зовнішніх порушників можна віднести конкурентів, колишніх співробітників, підрядників, розробників і виробників ПЗ, кримінальні угруповання.

Саме впровадження СКУД на основі виявлення загроз і порушників є одним з методів забезпечення безпеки об’єкта, що охороняється.

В третьому розділі розроблено СКУД та обрано додаткові апаратні засоби для забезпечення інформаційної безпеки об’єкта, що охороняється.

Прокладка кабелю буде здійснюватися під підвісною стелею. Спеціальний сервер для відеоспостереження буде розміщуватися в серверному приміщенні на окремій телекомунікаційної стійці. Доступ до даного пристрою здійснюється тільки за допомогою пароля, який є тільки у керівника служби безпеки і системного адміністратора на об'єкті захисту. Монітори відеонагляду розміщуються на пості охорони і дозволяють виробляти спостереження заданих секторів об'єкта.

Наведено основні складові частини структурної схеми відомої СКУД, для якої запропоноване рішення модернізації, яке полягає в інтеграції системи з *LDAP*-сервером. Наведена структура бази даних для СКУД.

Таким чином, в результаті написання дипломної роботи було виконане наступне:

1) Оцінено ризики інформаційної безпеки;

2) Розроблено модель загроз і модель порушника;

3) Обрано методики проектування СКУД;

4) Проведено обґрунтування складових системи;

5) Розроблено структурну схему зв’язку в СКУД;

6) Створено базу даних для СКУД.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андерсон Криста Локальные сети / Криста Андерсон, М.: МИФИ, 2011. – 238 с.

2. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации/В.Л. Бройдо, Спб.: Питер, 2011. – 560 с.

3. Васильев Ю.В. Самоучитель создания локальной сети/Ю.В. Васильев, М.: Триумф, 2011. – 185 с.

4. Васильков А.В. Информационные системы и их безопасность/А.В. Васильков, М.: Форум, 2015. – 565 с.

5. Юдін О. Критеріальний аналіз сучасних операційних систем у задачах захисту інформаційних ресурсів / О. Юдін, О. Весельська // Наукоємні технології. — 2012. — Т. 14. — №. 2. — С. 74–79.

6. Ворона В.А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. — М.: Горячая линия–Телеком. — 2010. — Т. 272.

7. Колбин Р.В. Глобальные и локальные сети. Создание, настройка и использование (+ CD)/Р.В. Колбин, М.: Бином, 2012 – 278 с.

8. Максимов Н.В. Технические средства информатизации/Н.В. Максимов, М.: Форум, 2013 – 608 с.

9. Ярочкин В.И. Информационная безопасность: учебник для студентов вузов. – М.: Академический проект; Гаудеамус, 2009. – 216 с.

10. Домарев В. В. Безопасность информационных технологий. Системный подход – К.: ООО ТИД Диа Софт, 2004. – 992 с.

11. Поляк–Брагинский А.В. Локальная сеть. Самое необходимое/А.В. Поляк–Брагинский, Спб.: БВХ–Петербург, 2011 – 576.

12. Поляк–Брагинский А.В. Локальные сети. Модернизация и поиск неисправностей/А. Поляк–Брагинский, Спб.: БВХ–Петербург, 2015 – 832 с.

13. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных

системах предприятий/ В.А. Сердюк, М.: Высшая Школа Экономики (Государственный Университет), 2013 – 576 с.

14. Шаньгин, В.Ф. Комплексная информация в корпоративных системах: учеб. пособие. – М.: ИД «Форум», «ИНФРА– М», 2010 – 592 с.

15. Олифер, В.Г. Основы сетей передачи данных Интернет–университет информационных технологий / В. Г. Олифер, Н. А. Олифер, 2016 –960 с.

16. Барсуков В.С. Современные технологии безопасности // В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2011. – 496 с.

17. Тихонов В.А., Райх В.В., Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты // Гелиос АРВ, 2006. – 528 с.

18. Зырянова Т.Ю. Модель системы управления информационной безопасностью в условиях неопределенности воздействия дестабилизирующих факторов: автореф. дис. канд. техн. наук. – Томск, 2008. – 25 с.

19. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008.

20. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009.

21. ГОСТ 2.106-96.

22. ДСТУ 3008-95.

23. Бойченко С.В., Іванченко О.В. Положення про дипломні роботи (проекти) випускників Національного Авіаційного Університету. НАУ, 2017 р.