Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра інформаційних технологій та систем електронних комунікацій

«Допущено до захисту»
Начальник кафедри інформаційних технологій та систем електронних комунікацій

Олександр ПРИДАТКО
“___” _____20__ року

ДИПЛОМНА РОБОТА МАГІСТРА

на тему **«Проектування локальної мережевої системи санкціонованого доступу на режимний об’єкт з використанням засобів відеоспостереження»**

Виконав:
здобувач VI курсу, групи КН-61м
спеціальності 122 «Комп’ютерні науки»
(шифр і назва спеціальності)
Олександр ПИЛИПИШИН
(прізвище та ініціали)
Керівник Олександр ПРИДАТКО
(прізвище та ініціали)
Рецензент Павло ЛУБ
(прізвище та ініціали)

Львів 2023 рік

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра інформаційних технологій та систем електронних комунікацій
Освітній ступінь_магістр
Спеціальність 122 «Комп'ютерні науки»
Освітня програма Комп'ютерні науки

ЗАТВЕРДЖУЮ
Начальник кафедри інформаційних технологій та систем електронних комунікацій

Олександр ПРИДАТКО

"____" _____20___ року

ЗАВДАННЯ
на дипломну роботу

Здобувачу_____Пилипишину Олександру Руслановичу_____
(прізвище, ім'я, по батькові)
1. Тема: Проєктування локальної мережевої системи санкціонованого доступу на режимний об'єкт з використанням засобів відеоспостереження
керівник роботи_Придатко Олександр Володимирович _____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ЛДУ БЖД від "___" _____ 20_ року №_____
2. Термін подання здобувачем роботи _____
3. Початкові дані до роботи
1. Сорокін К. Застосування біометричних технологій в забезпеченні інформаційної безпеки бізнесу [Текст] / СКУД. Антитероризм-2013, 2013 – С : 46-47с.
2. Uchit Vyas. OpenStack Deployment [Текст]/ Applied OpenStack Design Patterns. - Berkeley, CA: Apress, 2016. - S. 31-50. - ISBN 978-1-4842- 2453-3
3. L. M. Varalakshmi A selective encryption and energy efficient clustering scheme for video streaming in wireless sensor networks [Текст] // G. Florence Sudha, G. Jaikishan / Telecommunication Systems. - 2013-08-31. - Т. 56, no. 3. - S. 357–365.

4. Зміст дипломної роботи (перелік питань, які потрібно розробити)

Розділ 1 Системи безпеки
Розділ 2 Аналіз існуючих систем контролю і управління доступом
Розділ 3 Система контролю і управління доступом до об’єктів
Розділ 4 База даних та реалізація програмного забезпечення

5. Консультанти розділів роботи

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

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Розділ 1 Системи безпеки		
2	Аналіз існуючих систем контролю і управління доступом		
3	Система контролю і управління доступом до об’єктів		
4	База даних та реалізація програмного забезпечення		

Здобувач _____ Олександр Пилипишин
(підпис) (прізвище та ініціали)

Керівник роботи _____ Олександр Придатко
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Пилипишин О.Р. «Проектування локальної мережевої системи санкціонованого доступу на режимний об’єкт з використанням засобів відеоспостереження». Дипломна робота за спеціальністю 122 “Комп’ютерні науки” складається з текстової частини, що містить 4 розділи, 67 с., 24 рис., 10 таблиць, 18 джерел використаної літератури.

Об’єкт дослідження – процес забезпечення інформаційної безпеки та санкціонованого доступу на об’єкт.

Предмет дослідження – система контролю і управління доступом до об’єкта із використанням засобів відеоспостереження.

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

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

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

В роботі представлено покрокову інструкцію організації локальносї системи санкціонованого доступу на ркжимний об’єкт із використанням засобів відоспостереження. Підібрано елеметну базу, запропоновано апартну частину та здійснено вибір програмного забезпечення, яке дозволить організувати систему санкціонованого доступу на будь якому об’єкті.

Ключові слова: санкціонований доступ, локальна мережа, засоби відеоспостереження

ABSTRACT

Pylypyshyn O.R. "Designing a local network system of authorized access to a regime object using video surveillance." The diploma work on specialty 122 "Computer science" consists of a text part containing 4 chapters, 67 pages, 24 figures, 10 tables, 18 sources of used literature.

The research object is the process of ensuring information security and authorized access to the object.

The subject of the study is the system of control and management of access to the object using video surveillance.

The purpose of the thesis is to implement an access control and management system (ACMS) at an object protected with the use of surveillance systems.

The thesis is devoted to the current topic of the implementation of the system of control and management of access to protected objects in order to increase the level of information security.

The developed schematic and structural solutions can be applied at facilities that require protection and information security and the implementation of access control and management systems.

The work presents step-by-step instructions for organizing a local system of authorized access to a security object using surveillance tools. The electronic base was selected, the separate part was proposed, and the software was selected, which will allow organizing an authorized access system at any facility.

Keywords: authorized access, local network, video surveillance

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.

ВИСНОВКИ

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

В результаті написання другого 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 третьому 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, помилкипроектування 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 спеціальнихшкідливих програм, вірусів або черв'яків;

копіювання КІ з сервера;

доступ із зовнішньої мережі Інтернет до серверів об’єкта, щоохороняється;

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 четвертому 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:

Оцінено ризики інформаційної безпеки;

Розроблено модель загроз і модель порушника;

Обрано методики проектування СКУД;

Проведено обґрунтування складових системи;

Розроблено структурну схему зв’язку в СКУД;

Створено базу даних для СКУД.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Не типові функції СКУД [Електронний ресурс].

2. Огляд можливостей СКУД [Електронний ресурс].

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

4. Система контролю доступу на підприємстві. Особливості впровадження Принцип дії [Електронний ресурс]. Режим доступу.

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

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

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

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

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

11. Классификация СКУД [Електронний ресурс]

12. Ворона В.А. Системы контроля и управления доступом / Вор онаВ. А., Тихонов В. А. – М.: 2010. -272 с.

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

14. Іванов І.В. Охоронна периметрів-2 [Текст] — М.: Паритет Граф, 2000, 50-56с.

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

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

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

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