

IMPLEMENTATION OF A SECURITY SYSTEM FOR THE ART GALLERY IN DOBRICH*

MILEN B. KOLAROV, HRISTO I. PARASKEVOV

ABSTRACT: *This paper presents a structured overview and practical implementation of an intrusion alarm system designed for a public building—the Art Gallery in Dobrich. The article looks at the key parts of modern security systems—like control panels, sensors, extra modules, communication tools, and fire detection devices—and how they work together in a complete system. The process of equipment selection, functional block diagram design, and wiring is described in detail, with particular attention to power consumption estimation and component compatibility. The article emphasizes the need for reliable and scalable security solutions, as well as centralized and remote management through internet and mobile applications. The paper wraps up by highlighting important trends in security system development, such as the use of computers, combining with biometric and video surveillance technologies, and following standards from the telecommunications industry.*

KEYWORDS: *intrusion alarm system, control panel, integration, fire detection, access control*

2020 Math. Subject Classification: 90B25; 94B05

ИЗГРАЖДАНЕ НА ОХРАНИТЕЛНА СИСТЕМА ЗА ХУДОЖЕСТВЕНАТА ГАЛЕРИЯ В ГРАД ДОБРИЧ†

МИЛЕН Б. КОЛАРОВ, ХРИСТО И. ПАРАСКЕВОВ

*This paper is (partially) supported by Scientific Research Grant RD-08-106/05.02.2025 of Konstantin Preslavsky University of Shumen

†Статията е частично финансирана по проект № РД-08-106/05.02.2025

1 Въведение

В условията на нарастващи заплахи за сигурността в обществения и частния сектор, сигнално-охранителните системи (СОС) се превръщат в основен елемент от техническите решения за защита на физически обекти. Те съчетават различни подсистеми – като детектори за движение, системи за видеонаблюдение и контрол на достъп – в интегрирана среда, която позволява превенция, идентификация и реакция при инциденти [1], [2].

Бързото развитие на електронните технологии и комуникационната инфраструктура води до все по-широко разпространение на интелигентни охранителни решения, базирани на цифрова обработка на сигнали, IoT-сензори и дистанционно управление през мобилни или облачни платформи [3]. Съвременните СОС се изграждат по модулен принцип, като се адаптират към конкретните изисквания на обекта, архитектурата на сградата и нивото на риск, като същевременно осигуряват възможности за надграждане и централизирано управление [4] [5].

Класическата архитектура на една сигнално-охранителна система включва основни компоненти като детектори, контролни панели, известителни устройства и комуникационни модули. Основната ѝ задача е да преобразува физическо събитие (напр. движение, отваряне на врата, счупване на стъкло) в електрически сигнал, който чрез шлейфова връзка достига до контролния панел, където се анализира и води до активиране на алармено състояние [6].

Настоящата статия има за цел да представи основните технически и функционални характеристики на съвременните сигнално-охранителни системи, с фокус върху тяхната структура, принцип на действие и възможности за интеграция с видеонаблюдение и системи за контрол на достъп. Особено внимание се отделя на предизвикателствата, свързани с изграждането на комплексни охранителни решения и добрите практики при проектиране на надеждни архитектури.

2 Основни компоненти на съвременните сигнално-охранителни системи

В основата на всяка сигнално-охранителна система стои набор от взаимосвързани модули и устройства, които осигуряват наблюдение, детекция, контрол на достъп и комуникация с външни системи. Модулният принцип на изграждане позволява конфигурируемост, надграждаемост и висока степен на адаптивност според нуждите на конкретния обект [1]. В настоящото изследване се разглеждат ключовите компоненти на охранителна система, изградена с оборудване на фирмата PARADOX, поради доказаната и надеждност, богатата функционалност и широка разпространеност в България [2], [4].

2.1. Контролен панел

Сърцето на системата е контролният панел Digiplex EVO192, поддържащ до 192 зони, до 999 потребителски кода и до 254 разширителни модула. Панелът разполага с памет за 2048 събития, 5 програмируеми PGM изхода (разширяеми до 250), възможности за управление чрез софтуера NEware и WinLoad, както и интегрирани функции за контрол на достъп и комуникация (GSM, IP).

2.2. Интерфейсни устройства (клавиатури)

За управление на системата се използват LCD клавиатури K641R с вграден четец за достъп и TM50 Touch с 5-инчов цветен дисплей и иконичен интерфейс. Клавиатурите поддържат едновременно работа с няколко зони, управление на PGM изходи, конфигуриране чрез SD карта, визуализация на събития и персонализация чрез цветови панели.

2.3. Разширителни модули

Системата позволява добавяне на нови зони чрез разширители като ZX4 (4 адресируеми зони), като всяка зона може да бъде независимо конфигурирана, включително с допълнителни ключове за защита от саботаж.

2.4. Сензори и детектори

2.4.1. Магнитни контакти

Използван е адресируемый магнитен контакт ZC1 за мониторинг на отваряне на врати и прозорци.

2.4.2. Пасивни инфрачервени (PIR) датчици

PIR датчиците DM50 и DG55+ използват патентована цифрова обработка на сигнали (алгоритъм Digital SHIELD), двоен праг за активиране, автоматична температурна компенсация и защита от електромагнитни смущения. Те покриват ъгъл до 110° и разстояние до 12 м, като отговарят на стандарта EN 50131-2-2 за пасивни инфрачервени детектори [7].

2.4.3. Акустични датчици за стъкло

DG457 осигурява детекция чрез анализ на ултразвукови и звукови честоти, с цифрова филтрация и регулируема чувствителност (до 9 м).

2.5. Комуникационни модули

Интеграцията на комуникационни и контролни модули изисква внимателно отчитане на архитектурните и кибер-физическите уязвимости в рамките на интелигентни обекти [8].

2.5.1. IP модул

IP150 предоставя отдалечен достъп до системата чрез LAN/WAN, с възможности за известяване по e-mail, SSL/HTTPS криптиране и съвместимост със софтуер WinLoad, NEware и Babyware.

2.5.2. GSM/GPRS модул

PCS250 поддържа текстови и гласови известия, възможност за дистанционно активиране/деактивиране чрез SMS, криптиране (AES-256) и поддръжка на до 8 телефонни номера за известяване.

2.6. Модули за контрол на достъп

Модулът ACM12 позволява управление на една врата чрез четец, бутон за излизане, магнитен контакт и електромагнитен заключващ механизъм. Съвместим е с четци R915, които поддържат работа с карта, ПИН код или комбинация от двете, с устойчива на външни условия конструкция.

2.7. Пожароизвестители

2.7.1. Автоматичен пожароизвестител

ACC-EN комбинира оптичен и термичен елемент, с възможност за програмиране на чувствителност и импулсен/неимпулсен режим.

2.7.2. Ръчен пожароизвестител

HCP-E е аналогов адресируем ръчен модул, съвместим с ESP протокол, с LED индикация и монтажни опции.

2.8. Сирени

HPA702L е външна сирена с лампа, алуминиев корпус, акустичен изход 103 dB @ 3 м, 16 програмируеми звукови модуляции, защита срещу саботаж и работа в широк температурен диапазон (-25°C до +75°C).

2.9. Захранване и аварийно обезпечаване

Основното захранване се реализира чрез блок AMS-G13803-P (13.8V DC, 3A, IP65 корпус), а за аварийно обезпечаване се използва акумулаторна батерия 12V/7Ah, осигуряваща автономна работа при отпадане на мрежово **захранване**. Изборът на подходящи захранващи и резервиращи модули следва да се съобрази с топологията на системата и нейната критичност [9].

3 Проектиране на охранителна система

3.1. Архитектура и изходни параметри на обекта

Проектираната система за сигурност е предназначена за охрана на обекта „Художествена галерия гр. Добрич“. Архитектурният план (фиг. 3.1.1) очертава охраняемите зони и точките за контрол на достъпа. Системата следва да отговаря на следните изисквания:

- захранване: AC 220V/50Hz, DC 12V;
- реализация на пожароизвестяване и контрол на достъп;
- комуникация чрез TCP/IP и радиоканал;
- покритие на множество независими зони.

3.2. Блокова схема и взаимодействие на подсистемите

Функционалната архитектура на системата включва три основни подсистеми:

- сигнално-охранителна система;
- система за контрол на достъп и работно време;
- пожароизвестителна система.

Всяка подсистема изпълнява автономни задачи, но е интегрирана с останалите чрез централен контролен панел, комуникационни интерфейси и обща логика за алармиране и управление [9]. Системата позволява централизирано управление, локализиране на инциденти, както и автоматизирана реакция при установяване на заплаха.

3.3. Функционален анализ на основните блокове

3.3.1. Контролен панел

Контролният панел служи за централизирано управление и координация на свързаните устройства. Основни характеристики включват:

- управление чрез клавиатура, дистанционно или ключ;
- възможност за програмиране на зони и режими на охрана;
- задействане на аларма при нерегламентиран достъп;
- автоматично известяване на до четири телефонни номера;
- възможност за частично активиране (байпасване) на зони.

3.3.2. Детектори

Съществуват различни типове детектори в зависимост от целите и средата на използване:

- инфрачервени обемни детектори (аналогови и цифрови);
- магнитни контактори за врати и прозорци;
- акустични детектори за счупено стъкло;

Цифровите детектори осигуряват по-висока точност и по-ниска чувствителност към смущения [7].

3.3.3. Клавиатури

Клавиатурите осигуряват интерфейс между потребителя и системата. Те се монтират на стратегически места и предлагат:

- LCD или LED дисплей с индикация за състоянието на системата;

- вграден зумер и бутони за управление;
- поддръжка на информационни съобщения и запаметяване на събития;
- паралелно свързване към централата чрез 4-жична шина.

3.3.4. Контактори и сирени

Контакторите се използват за отчитане на отваряния/затваряния на отвори, а сирените служат за звукова сигнализация при алармени събития. По-сложните сирени могат да диференцират алармения сигнал според типа на задействане.

3.3.5. Система за контрол на достъп и работно време

Системата включва сървър, контролери, четци за безконтактни карти, електромагнитни насрещници и софтуер. Основните функции са:

- управление на достъпа чрез идентификация (карти, ПИН, биометрия);
- заключване и освобождаване на врати чрез електромагнити;
- логване на събития, ограничаване на достъпа по график;
- интеграция със CCTV и други системи чрез LAN или сухи контакти [8], [9].

4 Реализация на охранителна система

4.1. Монтаж и опроводяване на контролния панел

Контролният панел EVO 192 се монтира в метална кутия с пет монтажни пина, защитени с тампер, свързан в режим на 24-часова охрана. Кутията допуска и монтаж на разширителни модули. Опроводяването включва свързване на сирени, зоновы входове, програмируеми и релейни изходи, телефонна линия, тампери и комуникационна шина COMBUS. Максималната дължина на проводниците не трябва да превишава 914 m, като при отдалечени модули се препоръчва допълнително захранване. Изходът за сирена поддържа 12V DC за една 30W или две 20W сирени при ток до 2A.

4.2. Изчисляване на енергийна консумация и оразмеряване на линии

Методиката за оразмеряване на захранването изисква изчисляване на общата консумация на всеки клон. При превишаване на 700 mA се предвижда използване на външно захранване. Консумацията се изчислява въз основа на номиналната стойност за всеки модул, като при превишаване на допустимата дължина на кабела се предвижда разклоняване чрез допълнително захранване.

4.3. Свързване на входни зони към контролния панел

Контролният панел EVO 192 разполага с осем адресируеми входни терминала, към които могат да се свържат еднозонови и двузонови детектори, магнитни контакти и други сензори, използвайки N.O./N.C. конфигурации и EOL резистори.

4.4. Интеграция на пожароизвестителни детектори

Пожароизвестителните детектори се свързват към контролния панел и се програмират като Fire Zones. PGM1 може да бъде дефиниран като двупроводен вход за димен детектор. В случай на късо съединение се активира аларма, а при прекъсване – се отчита техническа неизправност.

4.5. Свързване на телефонна линия

Контролният панел позволява свързване към телефонна линия за автоматично известяване при алармени събития.

4.6. Конфигурация на модули за контрол на достъпа

Модулите за контрол на достъп се конфигурират съгласно архитектурата на системата и изискванията на обекта. Връзките се осъществяват чрез четирижична шина, като се използват контролери, четци и електромагнитни насрещници.

4.7. Връзка към Интернет чрез комуникационен модул

Модулът IP150 осигурява отдалечен контрол и мониторинг на охранителната система чрез уеб-браузър. Осигурява се съвместимост с HTTPS протокол, криптиране на данни и възможност за известяване по електронна поща.

5 Заключение

Настоящата статия представи етапите по избор, проектиране и реализация на сигнално-охранителна система за обект от обществено значение – „Художествена галерия гр. Добрич“. Анализирани бяха компонентите и технологиите, използвани за изграждане на система с висока степен на надеждност и възможности за интеграция.

Беше извършен преглед на съвременните решения и тенденции в областта на охранителните системи – включително контрол на достъп, пожароизвестяване и комуникационни модули. Представената архитектура показва приложението на модулен подход, адаптивност към изискванията на обекта и възможности за надграждане. Проектираната конфигурация включваше блокова схема на взаимодействие между подсистеми, функционален анализ и оразмеряване на енергийни и комуникационни линии.

Въз основа на извършеното проучване могат да се очертаят следните тенденции в развитието на системите за сигурност:

Преход към компютризирани системи със стандартен хардуер и съвместим софтуер;

Все по-широка интеграция на охранителни, пожаро-известителни и биометрични системи;

Усвояване на технологии и стандарти от телекомуникационния сектор;

Централизирано и дистанционно управление чрез интернет свързаност и мобилни приложения;

Развитие на мрежовите и безжични комуникационни решения;

Възможност за наблюдение от разстояние чрез стационарни и мобилни устройства.

Системите за сигурност се утвърждават като неотменна част от архитектурата на обществени и частни обекти. Тяхната ефективност зависи както от техническите решения, така и от правилното им проектиране и интеграция.

ЛИТЕРАТУРА:

- [1] Smith, J., & Brown, A. (2019). Modern Security Systems: Architecture and Integration. Springer.
- [2] Попов, Д. (2020). Сигнално-охранителни системи и приложението им в жилищни сгради. Техника и технологии, 12(3), 45–52.
- [3] Zhao, X., et al. (2021). IoT-enabled Intrusion Detection Systems: A Review. IEEE Access, 9, 112345–112360.
- [4] Тодоров, И. (2018). Основи на електронната охрана. София: Академично издателство.
- [5] Ivanov, G. & Petrova, N. (2022). Control and Access Systems in Smart Environments. International Journal of Security Technology, 11(2), 79–88.
- [6] Христов, В. (2017). Сигурност и контрол: Теоретични и практически аспекти. Русе: Русенски университет.
- [7] European Committee for Standardization. (2008). EN 50131-2-2: Alarm systems - Passive infrared detectors. CENELEC.
- [8] Kotenko, I., & Stepashkin, M. (2020). Cyber-Physical Security of Smart Buildings: Architectural Models and Threat Analysis. Security and Communication Networks, vol. 2020, Article ID 8743056.
- [9] Стоянов, П. (2019). Интегрирани алармени и контролни системи за сигурност. Електроника и автоматика, 61(4), 22–27.

Милен Коларов

Сектор Пътна Полиция към ОД на МВР гр. Добрич
e-mail: milen_kolarov@abv.bg

Христо Параскевов

Факултет по математика и информатика
Шуменски университет „Епископ К. Преславски“
E-mail: h.paraskevov@shu.bg