Zarządzanie bezpieczeństwem i komfortem w budynkach inteligentnych. Cz. I

JERZY MIKULIK – AGH

Jednym z głównych powodów powstania budynku inteligentnego BI była chęć zwiększenia komfortu i bezpieczeństwa jego użytkowników z równoczesnym obniżeniem kosztów utrzymania obiektu. Określenie „budynek inteligentny" pojawiło się w USA na początku lat 80. XX wieku. Było bardzo modne i miało raczej charakter komercyjny. Zgodnie z tym trendem zaczęto wymagać od wykonawców wyposażania obiektów w nowoczesne systemy infrastruktury technicznej.
Systemy automatycznego sterowania, urządzenia i zarządzanie budynkiem inteligentnym zmieniały się zgodnie z rozwojem systemów elektronicznych, technik i sieci komputerowych.
Szybki rozwój technik informatycznych, elektroniki i systemów automatycznego sterowania umożliwił stworzenie budynku, który reaguje automatycznie na potrzeby człowieka, i minimalizację kosztów utrzymania przy wysokim komforcie użytkowania. Budynek inteligentny, dzięki zaawansowanym technologiom, może szybko i skutecznie reagować na zmieniające się sytuacje w jego wnętrzu i otoczeniu.

Od około 20 lat trwa dyskusja, czym jest budynek inteligentny. Jedno jest pewne – nie jest tylko samą bryłą architektoniczną, jest uważany za połączenie technologii i procesów w celu stworzenia budynku, który będzie bezpieczny i użyteczny dla jego mieszkańców i ekonomicznie skuteczny dla właścicieli. Zastosowanie nowoczesnych technologii i procesów sterowania gwarantuje niskie koszty eksploatacji, a BI w odmianie budynków biurowych wpływają na wzrost wydajności pracy i obniżenie kosztów operacyjnych pomieszczeń. Zastosowanie takich systemów w budynkach biurowych wpływa na wzrost wydajności pracy i obniżenie kosztów operacyjnych pomieszczeń.
Nie ma znormalizowanej definicji BI – jest to trudne. Dla BI najważniejsza jest jego prosta funkcjonalność osiągnięta poprzez integrację wszystkich systemów technicznych, możliwa dzięki zastosowaniu technologii informatycznych. Budynek inteligentny posługuje się inteligencją techniczną. Przez inteligencję techniczną można rozumieć zdolność tych systemów do sterowania informacją w swoich obwodach elektronicznych.

Komfort fizyczny i bezpieczeństwo BI

Przez komfort fizyczny BI można rozumieć komfort cieplny, odpowiednią jakość powietrza wewnątrz BI (czyli jego wilgotność, prędkość, czystość i zawartość CO_2) oraz prawidłowe oświetlenie. Z tych parametrów zdefiniowany jest zgodnie z normą PN-83/B-03430 tylko komfort cieplny jako stan, w którym człowiek jest zadowolony ze swojego termicznego otoczenia, czyli nie odczuwa ani zimna, ani gorąca. Z parametrów komfortu fizycznego bardzo ważne są oświetlenie o odpowiednim natężeniu i dostęp do światła dziennego. Za utrzymanie sprzyjającego klimatu cieplnego wewnątrz BI odpowiadają systemy wentylacji, ogrzewania i klimatyzacji.
Przez bezpieczeństwo rozumie się stan, w którym jednostka lub grupa społeczna czy organizacja nie odczuwają zagrożenia swojego istnienia lub podstawowych interesów. Istnieje wiele rodzajów bezpieczeństwa. Z punktu widzenia BI najważniejsze jest bezpieczeństwo życia i zdrowia ludzi, następnie bezpieczeństwo zgromadzonego mienia oraz bezpieczeństwo technologiczne. Nad utrzymaniem bezpieczeństwa czuwają: system sygnalizacji pożarowej, system oddymiania, system automatycznego gaszenia pożaru, dźwiękowy system ostrzegawczy, system wykrywania gazów trujących, system sygnalizacji włamania i napadu, system kontroli dostępu, system telewizji dozorowej, sys-

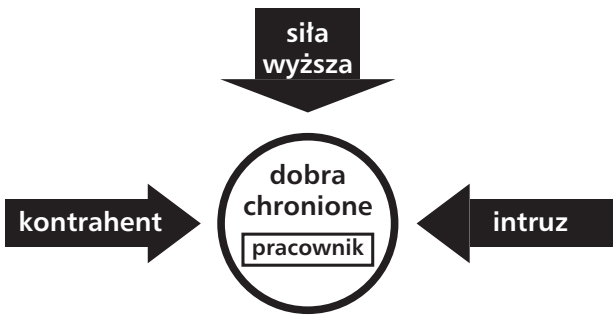
tem sterowania windami, system ochrony zewnętrznej budynku, system kontroli dostępu do parkingów oraz system monitorowania procesów technologicznych.

Zarządzanie bezpieczeństwem BI

Zarządzanie bezpieczeństwem budynków BI dotyczy działań profesjonalnych, tzn. opartych na rzetelnej wiedzy, fachowych umiejętnościach, racjonalnych metodach, sprawnych oraz skutecznych sposobach i technikach postępowania. Istotą jest zarządzanie rozumiane jako dążenie do osiągania celów poprzez planowanie, organizowanie, motywowanie i kontrolowanie ludzi i oddanych im do dyspozycji zasobów.

W obecnych, bardzo skomplikowanych czasach najlepszym rozwiązaniem jest wprowadzenie globalnego systemu zarządzania bezpieczeństwem BI, czyli stworzenie tzw. polityki bezpieczeństwa BI. Polityka ta będzie przemyślanym zbiorem reguł i praw oraz sposobów postępowania w przypadkach pojawienia się zagrożeń. Musi mieć niestety charakter przymusowy i dotyczyć całości działalności w budynku.

W BI typu biurowego, a tych jest zdecydowana większość, główne zagrożenia bezpieczeństwa pochodzą od własnych pracowników, kontrahentów, kooperantów i zwykłych intruzów. Przykładowo na *rys. 1* pokazano czyhające na BI zagrożenia ze strony sił przyrody, na których działanie mamy niestety mały wpływ, oraz zagrożenia ze strony ludzi.

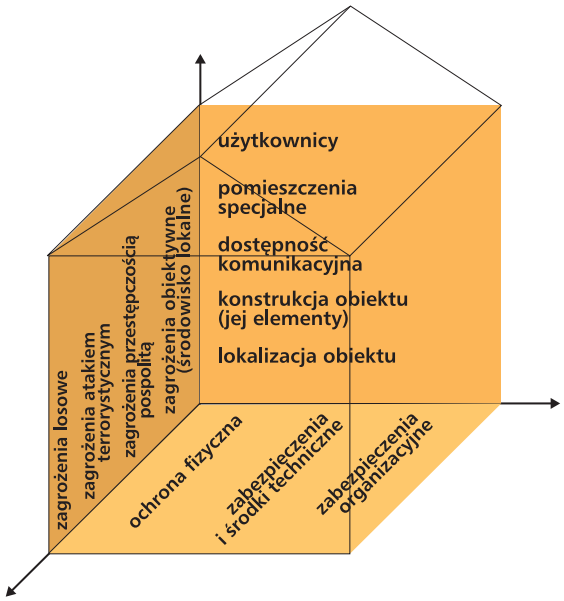


Rys. 1. Podstawowe zagrożenia oddziałujące na dobro chronione typu BI

Oceniając bezpieczeństwo, należy zwrócić szczególną uwagę na wyraźnie wyodrębnione trzy fazy funkcjonowania BI:
– faza nocna (zamknięcie lub stan czuwania),
– faza pośrednia (sprzątanie przed lub po godzinach pracy, przygotowanie do użytkowania),
– faza dzienna (pełne użytkowanie).

Fazy funkcjonowania obiektu wpływają na zmiany profilu występujących zagrożeń oraz na zakres i charakter wybranego zagrożenia. Dlatego zapewnienie bezpieczeństwa BI w każdej z faz wymaga odrębnej analizy ryzyka i oceny możliwości wystąpienia potencjalnych zagrożeń. Analiza powiązań pomiędzy zagrożeniami, parametrami obiektu i zastosowanymi zabezpieczeniami wymaga traktowania budynku BI jako obiektu o systemowej analizie bezpieczeństwa, co pokazano na *rys. 2.*

Bezpieczeństwo BI opracowuje się i wdraża, stosując odpowiednie algorytmy projektowania systemów ochrony, które obejmują kategorie chronionych obiektów, poszukują słabych miejsc, w których mogą wystąpić zagrożenia, określają środki neutralizacji zagrożeń i dokonują czasowej

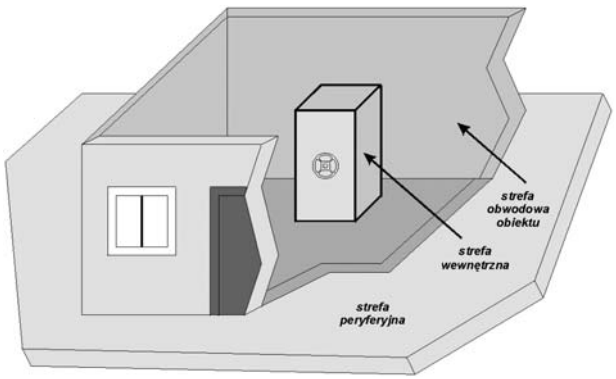


Rys. 2. Systemowa analiza bezpieczeństwa inteligentnego budynku [5]

analizy skuteczności ochrony, co pokazano na *rys. 3.* Czasowa analiza skuteczności jest najważniejsza, ponieważ określa, czy czas potrzebny na fizyczną interwencję i ujęcie sprawcy jest mniejszy od czasu zmaterializowania się zagrożenia.

Aby ułatwić organizację i rozmieszczenie systemów zabezpieczeń, wprowadza się w chronionym obiekcie tzw. strefy bezpieczeństwa. W najbardziej ogólnej analizie wyróżnia się trzy podstawowe strefy bezpieczeństwa: peryferyjną, obwodową i wewnętrzną *(rys. 4).* Ich rozległość i odległość od najbardziej chronionego pomieszczenia czy przedmiotu zależy od konkretnego rodzaju obiektu. Najdalej od chronionego miejsca znajduje się strefa peryferyjna, którą jest przeważnie bezpośrednie otoczenie obiektu. Strefa obwodowa oddziela strefę peryferyjną od strefy wewnętrznej. Tworzą ją (przeważnie) mury budynku wraz z otworami okiennymi i drzwiami. Strefa bezpośrednio przyległa do chronionego pomieszczenia to tzw. strefa wewnętrzna z głównym chronionym dobrem.

Rys. 3. Algorytm projektowania systemu ochrony



Rys. 4. Strefy bezpieczeństwa w chronionym obiekcie

Stosowana obecnie struktura zarządzania bezpieczeństwem budynku za pomocą systemów: SMS *(Security Management System),* DMS *(Danger Management System)* lub też tradycyjnie jeszcze BMS *(Building Management System)* to przede wszystkim systemy techniczne, których działanie oparto na technologiach informatycznych. Wyróżnić można dwie główne grupy tych systemów:
– systemy zabezpieczające ludzi i mienie przed skutkami zagrożeń losowych,
– systemy zabezpieczające ludzi i mienie przed skutkami zagrożeń wynikających ze świadomej działalności człowieka.
Największym zagrożeniem losowym dla budynku jest zawsze pożar, dlatego też do grupy pierwszej należą głównie systemy pożarowe: SSP, system automatycznego gaszenia, system oddymiania i dźwiękowy system ostrzegawczy DSO. Inne zagrożenia losowe to burze, wichury, powodzie, trzęsienia ziemi.
Podstawowym zadaniem systemu SSP jest szybkie wykrycie pożaru w jego początkowym stadium, zanim ogień osiągnie rozmiary trudne do opanowania. W razie wykrycia i potwierdzenia zagrożenia centrala SSP podejmuje decyzję o zainicjowaniu alarmu pożarowego odpowiedniego stopnia oraz koordynuje działania praktycznie wszystkich elementów ochrony przeciwpożarowej w danym obiekcie.
Systemy automatycznego gaszenia mają za zadanie rozpoczęcie gaszenia ognia, by stłumić pożar w początkowej fazie i zapobiec jego rozprzestrzenieniu się. W zależności od rodzaju i przeznaczenia pomieszczeń są wyposażone w różne środki gaśnicze (woda czy specjalne gazy).
Powstający w czasie pożaru dym rozprzestrzenia się w krótkim czasie, powodując dezorientację ludzi. Składniki chemiczne dymu stanowią groźbę utraty przytomności bądź nawet uduszenia. Rola systemu oddymiania polega na usuwaniu dymu oraz ciepła ze strefy pożaru, co umożliwia przeprowadzenie sprawnej ewakuacji.
Do sprawnego przeprowadzenia ewakuacji ludzi z zagrożonej strefy służy system DSO. System ten powiadamia ludzi o niebezpieczeństwie i kieruje ich na odpowiednie ciągi ewakuacyjne. Obecnie stosuje się systemy z informacją głosową, gdyż ostrzeganie w postaci syren lub buczków wywoływało przeważnie panikę lub było lekceważone. Ponadto informacja głosowa jest zrozumiała dla wszystkich użytkowników obiektu.

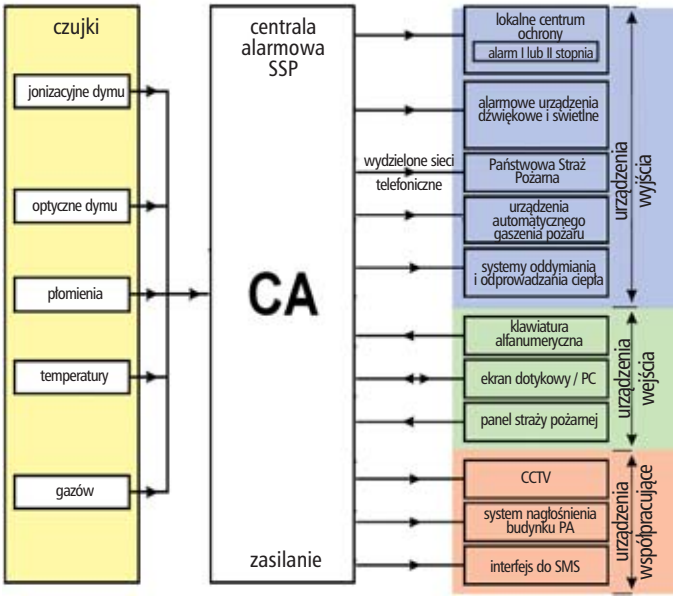
Do drugiej grupy systemów należą: system sygnalizacji włamania i napadu (SSWiN), system kontroli dostępu (SKD), system telewizji dozorowej (STVD). W grupie tej znajdują się również zagrożenia atakami terrorystycznymi.

System SSWN pełni dwojaką rolę w obiekcie: sygnalizuje wystąpienie napadu – funkcja aktywna w czasie normalnej pracy oraz sygnalizuje wystąpienie włamania – funkcja aktywna w czasie, gdy obiekt jest zamknięty. W przypadku automatycznego wykrycia włamania lub próby włamania do chronionego obiektu system sygnalizuje alarm w sposób dźwiękowy lub świetlny oraz przesyła informację do centrum monitorowania. W razie napadu istnieje możliwość ręcznego uruchomienia systemu. W przypadku napadu, ze względu na nieprzewidzianą reakcję napastnika, alarm nie powinien być sygnalizowany ani akustycznie, ani dźwiękowo.

Podstawowe zadanie systemu SKD polega na monitorowaniu oraz porządkowaniu przemieszczania się ludzi, jak również pojazdów, w dozorowanych strefach. W ten sposób system zabezpiecza obiekt przed dostępem osób niepowołanych oraz ogranicza poruszanie się osób nieuprawnionych po wydzielonych strefach, pozostawiając jednocześnie swobodę przemieszczania osobom uprawnionym. System STVD umożliwia ciągłą i kompleksową obserwację wielu obszarów chronionego obiektu z jednego lub kilku stanowisk monitorowania oraz archiwizację zapisu wizji. System ten wspomaga pozostałe systemy odpowiedzialne za bezpieczeństwo obiektu poprzez umożliwienie bieżącej weryfikacji zaistniałych zdarzeń oraz możliwość odtworzenia zdarzeń z materiałów archiwalnych, tworząc w ten sposób materiał dowodowy.

Każdy z systemów zabezpieczeń ma podobną strukturę funkcjonalną. Głównym elementem jest centrala albo sterownik, do którego podłączone są różnego rodzaju czujki. Dobór czujek zależy od przewidywanego sposobu materializacji zagrożeń. Z centralą lub sterownikiem musi być zapewniona komunikacja za pomocą urządzeń wejściowych, centrala musi mieć także możliwość przesyłania poprzez urządzenia wyjściowe sygnału alarmu do określonego miejsca lub centrum monitorowania. Centrale współpracują z innymi systemami w ramach integracji. Przykładowo schemat funkcjonalny systemu sygnalizacji pożarowej (SSP) pokazano na *rys. 5.* Czujnikami są w tym przypadku urządzenia reagujące na parametry pożarowe, takie jak temperatura, płomień lub dym (czujki pożarowe).

Bardzo istotnym zagadnieniem jest metoda integracji systemów. Ze względu na pewność i niezawodność działania integracja profesjonalnych systemów zabezpieczeń jest przeważnie dokonywana na poziomie oprogramowania w programach integrujących na stacjach operatorskich. Jest to jednak najwolniejszy sposób integrowania systemów z powodu długich czasów przetwarzania informacji, szczególnie w dużych rozbudowanych systemach. Wyjątkowo w obiektach, które nie podlegają obowiązkowi ochrony systemami sygnalizacji pożaru, np. w małych biurach czy domach jednorodzinnych, popularne są zintegro-



Rys. 5. Schemat funkcjonalny systemu sygnalizacji pożarowej

wane centrale obejmujące np. ochronę pożarową budynku i zabezpieczenie przed napadem i włamaniem. Jest to sposób integracji wykonany na bazie sprzętu.

***

BI kryje w swych wnętrzach systemy automatycznego sterowania używane do zarządzania bezpieczeństwem, komfortem i komunikacją. Współczesne systemy sterowania budowane są na bazie urządzeń i sieci komputerowych. Należy zawsze pamiętać, że podstawowym zagrożeniem dla systemów zarządzających inteligentnym budynkiem jest nieautoryzowane wtargnięcie do systemu poprzez sieć komputerową. Dlatego sieć ta wymaga szczególnie starannego zarządzania bezpieczeństwem, zwłaszcza z coraz powszechniejszym otwieraniem się sieci komputerowych na dostęp do Internetu. Z powodu coraz szerszego zastosowania sieci Ethernet z protokołem TCP/IP do komunikacji pomiędzy urządzeniami poszczególnych systemów poprzez sieć obiektową sieć ta powinna podlegać takim samym procedurom zarządzania ruchem i bezpieczeństwem jak sieć komputerowa. Znaczenie zarządzania bezpieczeństwem sieci obiektowej często jest niedoceniane, co może spowodować, iż pewnego dnia jakiś zmęczony haker włamie się do systemu zarządzania IB zamiast do innego komputera. Resztę scenariusza dopisać można sobie samemu.

Literatura

[1] Clements-Croome D. – *2nd International Congress on Intelligent Building Systems,* Cracow 2002

[2] Niezabitowska E. – *Budynek inteligentny,* Politechnika Śląska, Gliwice 2005,

[3] Ehrlich P.P. – *What is an intelligent building,* AutomatedBuilding.com, August 2005,

[4] Mikulik J. – *Budynek inteligentny, tom II: Podstawowe systemy bezpieczeństwa w budynkach inteligentnych,* Wydawnictwo Politechniki Śląskiej, Gliwice 2005,

[5] Blim M, Mikulik J. – *Security management of office facilities in the situation of contemporary threats, proc. of 4th International Congress on Intelligent Building Systems,* InBuS 2006, AGH Cracow, 2006,

[6] www.ciat.pl

[7] www.honeywell.com