Ekspercka metoda oceny bezpieczeństwa systemów technicznych w inteligentnym budynku

Monika Klaś, Jerzy Mikulik

Streszczenie: W artykule zawarto przegląd systemów technicznych związanych z bezpieczeństwem budynku inteligentnego. W pierwszej części omówiono podstawowe zagadnienia związane z inteligentnym budownictwem oraz przedstawiono powszechnie stosowane metodyki oceny ryzyka systemów technicznych oparte na zmiennych lingwistycznych. Następnie wprowadzono autorską metodę oceny ryzyka opartą na systemie ekspertowym. Szczegółowo opisano ideowe działanie systemu ekspertowego. Zaprezentowano przykładowe parametry wykorzystywane w ocenie ryzyka oraz omówiono plan dalszych badań w zakresie rozwoju systemu.

Słowa kluczowe: budynek inteligentny; systemy techniczne; ryzyko; system ekspertowy

1. Pojęcia podstawowe

Początków określenia 'inteligentny budynek' w literaturze należy upatrywać we wczesnych latach 80. XX wieku. Rozwój nauk inżynieryjnych oraz rosnące wymagania klientów co do jakości i funkcjonalności obiektów sprzyjały ewolucji określenia inteligentnego budynku oraz powstawaniu nowych rozwiązań technicznych w tym zakresie. Początkowo za inteligentne uważano obiekty posiadające jedynie kontrolę instalacji odpowiedzialnych za mikroklimat pomieszczeń, sygnalizację pożarową, zasilanie elektryczne, windy czy system kontroli dostępu. Z czasem pojawiło się centrum sterujące i monitorujące, sprawujące kontrolę nad całą budowlą [2].

Podążając za definicją Inteligent Building Institute w Waszyngtonie USA, można stwierdzić, że za inteligentny uznaje się obiekt architektoniczny, który ma zdolność integracji różnych systemów technicznych, dzięki czemu możliwe jest skoordynowane zarządzanie jego zasobami. Budynki inteligentne pozwalają na maksymalizację oszczędności związanych z ich eksploatacją oraz redukcję kosztów operacyjnych, przy jednoczesnej trosce o jak najlepsze funkcjonowanie użytkowników [2].

Każdy budynek inteligentny wyposażony jest w wyspecjalizowane systemy sterowania i zarządzania budynkiem jako całością, z włączeniem bezpieczeństwa funkcjonowania i użytkowania obiektu [3]. Problematyka oceny ryzyka systemów bezpieczeństwa budynków inteligentnych jest zagadnieniem skomplikowanym i poruszanym w licznych opracowaniach naukowych. Poprzez „ryzyko" należy rozumieć tutaj prawdopodobieństwo wystąpienia zdarzenia niepożądanego. Natomiast sama analiza i ocena poziomu ryzyka sprowadza się do identyfikacji zagrożeń i oceny ich wielkości. Celem tej analizy jest minimalizacja skutków niepewnych zdarzeń, które mogą być przyczyną zmiany jakości pracy, kosztów eksploatacji czy też właściwości technicznych obiektu.

W niniejszej pracy szczególną uwagę zwrócono na funkcjonowanie systemu sterowania bezpieczeństwem obiektu, w skład którego wchodzą [1, 2, 7]:

a) System sygnalizacji pożaru SSP

Podstawowym zadaniem systemu SSP jest szybkie i bezbłędne wykrycie powstającego pożaru, zanim dojdzie do jego rozprzestrzenienia. Jest to system automatycznego wykrywania pożaru, ogłaszania alarmu i transmisji sygnału alarmu do jednostek straży pożarnej. Jego sprawne działanie umożliwia skuteczną ewakuację ludzi z miejsca zagrożenia oraz minimalizację strat materialnych.

b) System oddymiania SO

System oddymiania służy do usuwania dymów i gorących gazów pożarowych z obiektu (a w szczególności z dróg ewakuacyjnych). System ten zapewnia lepszą widoczność, poprzez ograniczenie zadymienia. Ułatwia to ewakuację ludzi ze stref zagrożenia oraz przeprowadzenie skutecznej akcji gaśniczej.

c) System gaszenia pożaru SG

System gaszenia pożaru to zbiór specjalnie dobranych urządzeń, których zadaniem jest zgaszenie powstałego pożaru. System zapewnia ochronę budynku przed całkowitym spłonięciem, jak również przed zalaniem wodą gaśniczą pozostałej jego części. Wyróżnia się 4 główne rodzaje systemów gaszenia pożaru w zależności od zastosowanego środka gaśniczego, którym może być: woda, mgła wodna, piana lub gaz.

d) System sygnalizacji włamania i napadu SSWN

Do podstawowych funkcji systemu SSWN należy: wykrywanie włamania lub próby włamania, obsługa systemu (włączanie/wyłączanie systemu), przetwarzanie sygnałów i komunikatów powstałych w wyniku wykrycia intruzów, próby sabotażu oraz monitorowanie systemu, dostarczenie użytkownikowi

informacji o stanie systemu, zabezpieczenie sabotażowe i sygnalizacja sabotażu (ochrona przed celowym lub przymusowym zniszczeniem systemu).

e) System kontroli dostępu SKD

Za pomocą systemu SKD monitoruje się i steruje przemieszczaniem ludzi lub pojazdów w dozorowanych strefach. System pozwala na identyfikację, weryfikację i udzielenie zezwolenia na dostęp do chronionego pomieszczenia oraz na kontrolę stanu obiektu i archiwizację danych.

f) System telewizji dozorowej STVD

System STVD dzięki wizualizacji stanu obiektu (w czasie rzeczywistym) umożliwia wczesną i prawidłową reakcję służb ochrony lub personelu technicznego budynku na zagrożenie. System ten bardzo często współpracuje z SSP i SKD.

g) System nagłośnienia ewakuacyjnego DSO

DSO służy usprawnieniu procesu ewakuacji ludzi ze strefy zagrożenia zdrowia lub życia. Po aktywacji systemu w strefie niebezpieczeństwa nadawane są automatyczne komunikaty alarmowe.

Cechą, która odróżnia inteligentne budynki od zwyczajnych budynków wyposażonych w systemy automatycznego sterowania, jest zintegrowane zarządzanie systemami i podsystemami sterowania. Integracja systemów bezpieczeństwa może dokonywać się na następujących płaszczyznach: sprzętu, środków transmisji sygnału lub oprogramowania. Pozwala to służbom nadzoru technicznego i ochrony danego obiektu na uzyskiwanie kompleksowej informacji o stanie chronionego budynku.

2. Jakościowa ocena ryzyka

W większości prac związanych z oceną stopnia zabezpieczenia oraz ryzyka systemów technicznych w budynku inteligentnym stosuje się metody jakościowe. Sprowadzają się one do wyboru właściwych kryteriów i oceny ich jakości za pomocą zmiennych lingwistycznych. Zmiennym lingwistycznym przypisane są wagi. Zazwyczaj stosuje się następujące wartościowanie stopnia zabezpieczenia:

- maksymalny;
- wysoki;
- średni;
- niski/nie dotyczy.

Wybór zmiennych lingwistycznych można dostosowywać do przyjętych warunków oceny. Wartościowanie kryteriów może być różne, z uwzględnieniem założenia, że najwyższy stopień zabezpieczenia ma wagę najwyższą – np. 4 – a dla stopni niższych przyjmuje się w kolejności niższe oznaczenia – np. 3, 2, 1 [5].

Zmienne lingwistyczne są stosowane w analizach o charakterze typowo jakościowym i mogą być wykorzystywane do oceny ryzyka wystąpienia zdarzenia niepożądanego w budynku inteligentnym w sposób:

a) Bezpośredni

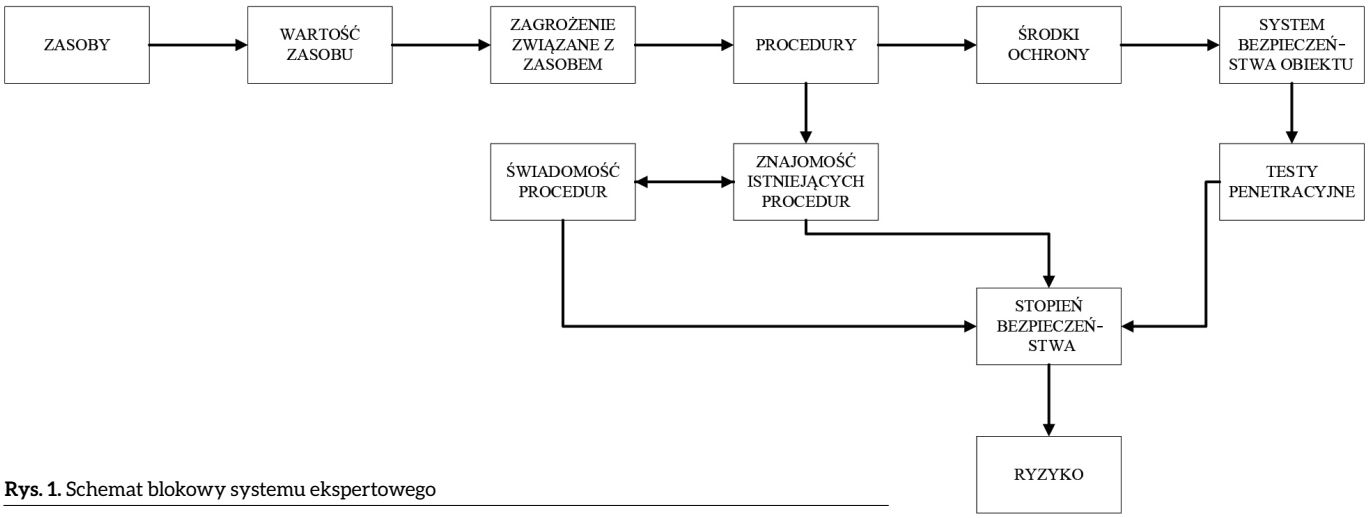
Zmienne lingwistyczne stosuje się do określenia stopnia zabezpieczenia budynku inteligentnego (SZBI) przed zagrożeniem. Przedstawia się go symbolicznie za pomocą funkcji *SZBI*, określonej na zbiorze zmiennych lingwistycznych {*P, O, G, W, K, C, D*} [5]:

$$SZBI = min\{P, O, G, W, K, C, D\} \quad (1)$$

Jako kryteria decyzyjne w równaniu (1) stosowane są wartości parametrów:

- *P* – stopień zabezpieczenia systemu sygnalizacji pożaru;
- *O* – stopień zabezpieczenia systemu oddymiania;
- *G* – stopień zabezpieczenia systemu gaszenia pożaru;
- *W* – stopień zabezpieczenia systemu sygnalizacji włamania i napadu;
- *K* – stopień zabezpieczenia systemu kontroli dostępu;
- *C* – stopień zabezpieczenia systemu telewizji dozorowej;
- *D* – stopień zabezpieczenia systemu nagłośnienia ewakuacyjnego.

Dodatkowo należy zaznaczyć, że w równaniu (1) można również uwzględnić współczynniki wagowe {*p, o, g, w, k, c, d*}, oznaczające udział/znaczenie danego systemu w zarządzaniu bezpieczeństwem analizowanego budynku. Jak wynika z równania (1), stopień zabezpieczenia inteligentnego budynku przyjmuje wartość najniższą ze zbioru {*P, O, G, W, K, C, D*} – minimalna wartość jednego parametru determinuje stopień zabezpieczenia obiektu.



Rys. 1. Schemat blokowy systemu ekspertowego

b) Pośredni

Zmienne lingwistyczne stosowane są do określania ryzyka związanego z wystąpieniem poszczególnych zagrożeń w analizowanym obiekcie. W tym celu stosuje się metody parametryczne, które mogą stanowić namiastkę analizy ilościowej. W zależności od dostępności informacji oraz stopnia szczegółowości oceny w metodach parametrycznych można uwzględniać różne czynniki. Przykładem może być czteroparametryczna formuła do analizy i ilościowej oceny możliwych do wystąpienia zdarzeń niepożądanych [6]:

$$R = \frac{P \times C \times N}{O} \qquad (2)$$

W równaniu (2) R oznacza szacowane ryzyko zależne od zmiennych lingwistycznych, którym przypisano wagi punktowe z uwagi na parametry:

- P – prawdopodobieństwa wystąpienia danego reprezentatywnego zdarzenia niepożądanego;
- C – wielkości strat związanych z wystąpieniem danego reprezentatywnego zdarzenia niepożądanego;
- N – liczby zagrożonych osób;
- O – ochrony inteligentnego budynku przed zjawiskami niepożądanymi (należy zauważyć, że im bardziej rozbudowany jest system barier ochronnych, tym mniejsze jest ryzyko wystąpienia zagrożenia).

Metody oceny ryzyka budynku inteligentnego oparte bezpośrednio na zmiennych lingwistycznych prowadzą do utraty wielu cennych informacji dotyczących analizowanego obiektu. Uwaga skupiona jest tylko na jednym, głównym czynniku warunkującym końcową ocenę. Z kolei metody parametryczne opierają się przeważnie na sztywnym skategoryzowaniu ryzyka, przypisaniu z góry narzuconych wag oraz ilościowym określeniu prawdopodobieństwa wystąpienia i skutków zaistniałego ryzyka. Ponadto prowadzą zazwyczaj do rozbudowanych tabel decyzyjnych, które każdorazowo należy adaptować do konkretnych warunków oceny. Zastosowanie systemu ekspertowego do oceny ryzyka w budynku inteligentnym pozwala na wyeliminowanie problemów związanych z modelami opartymi na zmiennych lingwistycznych.

3. Ekspercka ocena ryzyka

Systemy ekspertowe są to programy komputerowe, wykorzystujące zgromadzoną wcześniej wiedzę oraz wypracowane reguły rozumowania do wspomagania procesu podejmowania decyzji i rozstrzygania złożonych problemów, w których wymagane jest korzystanie z wiedzy eksperta w danej dziedzinie. Systemy ekspertowe w odróżnieniu od zwyczajnych programów komputerowych nie realizują prostego algorytmu, ale przy rozwiązywaniu złożonych procesów decyzyjnych korzystają z bazy wiedzy ekspertów. Baza wiedzy stanowi zbiór wiadomości i doświadczenia specjalistów oraz wszelkich niezbędnych informacji związanych z problematyką, której dotyczy system ekspertowy [4].

Autorzy niniejszego artykułu za punkt wyjścia przyjęli stworzenie koncepcji modelu systemu ekspertowego, służącego do oceny ryzyka systemów technicznych w budynku inteligentnym. Przyjęto założenie, że każdy z omówionych w niniejszym artykule systemów bezpieczeństwa budynku tworzą następujące zasoby:

- ludzie;
- procedury;
- rozwiązania techniczne.

Ponieważ każdy z powyższych zasobów systemu bezpieczeństwa charakteryzuje się innymi właściwościami, należy stosować odrębne sposoby ich pomiaru. Schemat modelowy autorskiego systemu ekspertowego został przedstawiony na rysunku 1.

Jak wynika z rysunku 1, w proponowanym przez autorów podejściu do oceny ryzyka systemów technicznych bezpieczeństwa w budynku inteligentnym w pierwszej kolejności określane są zasoby danego obiektu. Poprzez zasoby należy rozumieć pracowników oraz zgromadzone mienie. Następnie sprawdzane

Tabela 1. Przykładowe procedury związane z zarządzaniem bezpieczeństwem budynku inteligentnego

Lp.	Procedury
1	Procedura ewakuacji w razie pożaru
2	Procedura postępowania w przypadku braku zasilania
3	Procedura postępowania w przypadku włamania/napadu
4	Procedura zabezpieczania pomieszczeń w budynku
5	Procedura postępowania z kluczami
6	Zasady postępowania w przypadku zagrożenia środkami chemicznymi/biologicznymi
7	Zasady prowadzenia prac remontowych i aranżacyjnych wewnątrz budynku
8	Zasady postępowania w razie alarmu
9	Regulamin użytkowania pomieszczeń w budynku
10	Regulamin budynku
11	Plan ochrony budynku
12	Instrukcja bezpieczeństwa pożarowego
13	Harmonogram przeglądów systemów technicznych i okablowania
14	Zasady archiwizacji dokumentów
15	Procedura wynajmu powierzchni w budynku
16	Procedura dostępu do budynku (wejścia/wyjścia)
17	Procedura realizacji dostaw na terenie budynku
18	Zasady wnoszenia i wynoszenia wyposażenia
19	Procedura zgłaszania awarii oraz usterek
20	Zasady korzystania z powierzchni wspólnych
21	Zasady oznakowania pomieszczeń
22	Zasady dostępu ekip technicznych do pomieszczeń w budynku
23	Zasady odbioru poczty i korespondencji
24	Przepisy przeciwpożarowe
25	Książka obiektu budowlanego
...	...

Tabela 2. Przykładowe możliwe do wystąpienia zagrożenia w obrębie systemu technicznego

Lp.	Zagrożenie	System, którego dotyczy zagrożenie
1	Awaria urządzenia do sygnalizacji ewakuacji	DSO
2	Katastrofy naturalne	
3	Dostęp do informacji poufnych	SKD
4	Sabotaż urządzenia	
5	Złamanie kodu dostępu do pomieszczeń	
6	Kradzież identyfikatora dostępu do budynku	
7	Odblokowanie przejścia	
8	Szpiegostwo przemysłowe	
9	Blokada pomieszczeń	
10	Sabotaż	SKD + SSWN
11	Atak terrorystyczny	
12	Kradzież cennych zasobów	
13	Włamanie	
14	Napad	
15	Kradzież cennych zasobów	
16	Kradzież danych	
17	Akty wandalizmu	
18	Awaria urządzenia do sygnalizacji pożaru	SSP
19	Pożar	SSP + SO + SG + DSO
20	Awaria centrali sterującej	SSP + SO + SG + SSWN + SKD + STVD + DSO
21	Brak zasilania	
22	Penetracja sygnalizatora dźwiękowego	
23	Utrata sygnałów/kopii bezpieczeństwa	
24	Błędy w realizacji programów (dotyczy interfejsów sterowanych programowo)	
25	Awaria urządzenia do sygnalizacji napadu	SSWN
26	Penetracja centrali/klawiatury/systemu transmisji alarmu	
27	Awaria zasilania elektrycznego	**SSWN + SKD + STVD**
28	Zanik sygnału wideo	STVD
29	Celowe zasłonięcie lub przysłonięcie kamery	
30	Podstawienie danych wideo w źródle obrazu	
...	...	...

jest, czy dla każdego z posiadanych zasobów została określona jego wartość wraz z podaniem jej nominału. Po zidentyfikowaniu i zwartościowaniu istniejących zasobów określane są możliwe do wystąpienia zagrożenia związane z każdym zasobem. W kolejnym kroku sprawdzane jest istnienie procedur zdefiniowanych dla istniejących, potencjalnych zagrożeń oraz środki ochrony dla poszczególnych procedur. Ocena ryzyka dokonywana jest w dwóch etapach: w pierwszej kolejności za pomocą metod arkuszowych określane jest istnienie procedur i poziom ich znajomości, następnie za pomocą testów penetracyjnych sprawdzany jest system bezpieczeństwa obiektu. W każdym z tych etapów uczestniczy zespół ekspertów z różnych dziedzin związanych z inteligentnym budownictwem, którzy:

- pomagają budować arkusz służący do sprawdzania znajomości procedur;
- oceniają istotność istniejących procedur;
- oceniają istniejące rozwiązania techniczne zastosowane w badanym obiekcie.

Na podstawie wyników oceny dokonanej przez zaangażowanych ekspertów uzyskiwana jest informacja, czy analizowany budynek inteligentny ma spójny system bezpieczeństwa i jakie jest ryzyko wystąpienia poszczególnych zagrożeń w obiekcie.

Szczegółowy proces oceny ryzyka związanego z wystąpieniem zagrożenia w obrębie systemów bezpieczeństwa budynku inteligentnego w odniesieniu do głównych filarów systemu jest następujący:

a) Procedury

W obrębie tego zasobu sprawdzane jest:

- istnienie procedur związanych z zarządzaniem bezpieczeństwem obiektu;

- występowanie zidentyfikowanego zbioru zagrożeń związanych z funkcjonowaniem obiektu;
- istnienie procedur postępowania w przypadku wystąpienia zidentyfikowanego zagrożenia.

Przykładowe procedury związane z zarządzaniem bezpieczeństwem obiektu oraz możliwe do wystąpienia zagrożenia w odniesieniu do konkretnych systemów technicznych zamieszczono w tabeli 1 i 2.

Zarówno rodzaje stosowanych procedur, jak i możliwe do wystąpienia zagrożenia są charakterystyczne dla badanego budynku inteligentnego. Docelowo autorzy mają zamiar stworzyć bazę ogólnych procedur i zagrożeń, którą użytkownik systemu będzie mógł modyfikować w celu adaptacji do istniejących warunków oceny.

b) Ludzie

W ramach tego zasobu sprawdzana jest znajomość procedur i przepisów związanych z eksploatacją inteligentnego budynku przez jego codziennych użytkowników. Sprawdzany jest poziom znajomości systemów technicznych i określana jest świadomość użytkowników związana z reakcją na wystąpienie danego zagrożenia. Ocena odbywa się na podstawie wyniku testu rozwiązywanego przez użytkowników obiektu. Test jest układany przez ekspertów odrębnie dla każdego budynku inteligentnego na podstawie treści obowiązujących w nim procedur.

c) Rozwiązania techniczne

Ocena przeprowadzana w ramach rozwiązań technicznych zastosowanych w budynku pozwala określić, czy dla istniejących procedur i zagrożeń zastosowano właściwe środki ochrony. Proces analizy działania poszczególnych systemów technicznych przeprowadzany jest za pomocą testów penetracyjnych. Grupa ekspertów dokonuje praktycznej weryfikacji rozwiązań stosowanych w obiekcie – sprawdzane są poszczególne elementy systemu bezpieczeństwa. Pozwala to na określenie prawdopodobieństwa wystąpienia poszczególnych zdarzeń niepożądanych, (czyli stopnia ryzyka związanego z zagrożeniem). Prawdopodobieństwo wystąpienia danego zagrożenia rozumiane jest jako iloczyn niżej wymienionych czynników:

- prawdopodobieństwo materializacji zdarzenia niepożądanego;
- prawdopodobieństwo wystąpienia skutków związanych z zagrożeniem (skutki są zależne od wartości zasobu, którego dotyczy analizowane zagrożenie);
- prawdopodobieństwo detekcji zdarzenia (zależne od sprawności systemu technicznego, z którym bezpośrednio związane jest analizowane zagrożenie).

Na podstawie wyników oceny na szczeblu strategicznym (w obrębie filarów: ludzie, procedury) oraz weryfikacji sprawności poszczególnych systemów technicznych bezpieczeństwa obiektu określane jest ryzyko związane z funkcjonowaniem budynku inteligentnego. Zależy ono w bezpośredni sposób od stopnia znajomości istniejących w obiekcie procedur, od zakresu tychże procedur oraz od zastosowanych rozwiązań technicznych i ich jakości. Dzięki temu uzyskiwana jest informacja, czy analizowany obiekt posiada spójny system bezpieczeństwa.

Zakończenie

W niniejszym artykule przedstawiono nowe podejście do sposobu oceny ryzyka zagrożeń dla systemów technicznych stosowanych w budynku inteligentnym. Artykuł stanowi wstęp do dalszych działań w zakresie rozwoju idei systemu ekspertowego. W kolejnym kroku autorzy dokonają weryfikacji poprawności działania stworzonego modelu systemu ekspertowego na podstawie analizy oceny ryzyka materializacji zagrożeń w przykładowym budynku inteligentnym.

Należy zaznaczyć, że ocena ryzyka w budynku inteligentnym powinna stać się fundamentalnym elementem procesu zintegrowanego zarządzania obiektem. Jednak, aby możliwe stało się ciągłe monitorowanie poziomu ryzyka, stopnia narażenia na zagrożenie i jakości ochrony przed zagrożeniem, konieczne jest stosowanie metod wspomagających proces decyzyjny. Jedną z opcji jest wykorzystanie przedstawionego w niniejszym artykule modelu systemu ekspertowego. Jak powszechnie wiadomo, zagrożeń nie da się w całości wyeliminować, ale ich wczesna identyfikacja pozwala na wstępne podjęcie działań w obszarach krytycznych.

Literatura

[1] Anderson R.: *Security Engineering: A guide to building dependable Distributed Systems, second edition*. Wiley 2008.

[2] Niezabitowska E. (red.): *Budynek inteligentny. T. 1.* Wydawnictwo Politechniki Śląskiej, Gliwice 2010.

[3] Mikulik J.: *Podstawowe systemy bezpieczeństwa w budynkach inteligentnych.* [w:] Niezabitowska E. (red.): *Budynek inteligentny. T. 2.* Wydawnictwo Politechniki Śląskiej, Gliwice 2014.

[4] Mulawka J.: *Systemy ekspertowe*, WNT, Warszawa 1997.

[5] Ryczer A.: *Metoda oceny stopnia zabezpieczenia inteligentnego budynku* [w:] *Inteligentne budynki. Teoria i praktyka*, Oficyna Wydawnicza Text, Kraków 2010.

[6] Ryczer A.: *Problemy zarządzania ryzykiem w planowaniu i projektowaniu systemów alarmowych inteligentnego budynku.* [w:] *Inteligentne budynki. Nowe możliwości działania*. LIBRON, Kraków 2014.

[7] Wang S.: *Intelligent Buildings and building automation*, Routledge 2009.

Monika Klaś, Jerzy Mikulik – AGH Akademia Górniczo-Hutnicza w Krakowie; Wydział Zarządzania