PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2013, t. I

Radomír Ščurek, Martin Konečný, Ondřej Stoniš
VŠB – Technical University of Ostrava
ul. Lumírova 13, 700 30 Ostrava – Výškovice, Czechy,
e-mail: radomir.scurek@gmail.com

OCENY RYZYKA BEZPIECZEŃSTWA PUBLICZNYCH UCZELNI W ZAKRESIE OCHRONY FIZYCZNEJ

Streszczenie. Artykuł dotyczy występowania czynów niedozwolonych oraz innych form przestępczości przeciwko środowisku na uczelniach publicznych odnoszących się do funkcjonowania obiektów tego rodzaju. Artykuł koncentruje się również na zastosowaniu wybranych metod analizy ryzyka i oceny wpływu błędu ludzkiego jako czynnika ryzyka w procesie ochrony fizycznej osób i mienia w środowisku uczelni publicznych.

Słowa kluczowe: Zagrożenie bezpieczeństwa, analiza, czynniki ludzkie, ochrona fizyczna.

Wstęp

Celem niniejszego artykułu jest zwrócenie uwagi na potencjalne zagrożenia dotyczące uczelni publicznych, które mogą być analizowane z różnych stanowisk. W zakresie ochrony fizycznej uczelnie publiczne mogą być zaliczone do obiektów, które są narażone na powszechne działania niezgodne z prawem. Chodzi o różnego rodzaju formy przestępczości, takie jak włamania, kradzieże, wandalizm i inne działania w mniejszym stopniu niezgodne z prawem, które są zagrożeniem dla zdrowia i życia ludzkiego.

Oprócz wspomnianych konwencjonalnych działań niezgodnych z prawem, uczelnie publiczne przez swój charakter są potencjalnie bardziej narażone na zagrożenia, mające istotnie negatywny wpływ na zdrowie ludzi i dobra materialne. Do przedstawicieli tej grupy zagrożeń bezpieczeństwa, możemy zakwalifikować ciągle aktualny terroryzm i przestępczość zorganizowaną, dla których uczelnie publiczne są celem częstego ataku, a w przypadku kiedy przebiegnie on pomyślnie, niesie ze sobą druzgocąco negatywne skutki dla społeczeństwa. Nie można ignorować faktu, że w obiektach uczelni publicznych w ciągu dnia porusza się duża liczba osób w ramach konferencji, wykładów, okolicznościo-

wych uroczystości, w których biorą udział wybitni politycy i mężowie stanu, którzy przez swoje pozycje są potencjalnymi celami zagrożeń bezpieczeństwa tego typu.

Obiekty uczelni publicznych są narażone nie tylko na już wspomniane zagrożenia. Podstawowym niebezpieczeństwem jest również indywidualna przemoc i agresja wśród uczniów, czasem nauczycieli, którą ciężko jest wykryć. Jako przykład może posłużyć niedawny atak nożem na nauczycielkę szkoły podstawowej w Hawirzowie, gdzie sprawca zadał liczne cięcia i rany kłute. Dlatego powstaje pytanie, kiedy i z jaką intensywnością incydenty o podobnym charakterze wystąpią na uczelniach publicznych, których jest obecnie 26 i znajdują się prawie w całej Republice Czeskiej.

Istotnym faktem w ochronie fizycznej uczelni publicznych pozostaje poziom bezpieczeństwa poszczególnych uczelni, który nie jest optymalny, istniejące środki bezpieczeństwa są niewystarczające, urządzenia bezpieczeństwa nie odpowiadają wymaganiom detekcji, a potencjalnego sprawcę trudno wykryć. Należy zwrócić uwagę także na znaczenie podstawowych elementów kompleksowego systemu bezpieczeństwa i ochrony fizycznej, który wprowadzają pojedyncze uczelnie publiczne z pomocą straży. W ramach osiągnięcia optymalnego poziomu bezpieczeństwa kwestią jest sama znajomość systemu bezpieczeństwa oraz ochrona fizyczna w przypadku przeprowadzenia interwencji lub odpowiedzi na alarm, a następnie działania przeciwko przestępcom. Ze względu na wysoki koszt zatrudnienia wyspecjalizowanej ochrony fizycznej, często na jej miejsce są zatrudniani pracownicy bez praktycznego doświadczenia i wiedzy teoretycznej, którzy owszem przeszli obowiązkowe badania kwalifikacji zawodowych, ale nie potrafią ich zastosować w praktyce.

Biorąc pod uwagę przedstawione fakty, nie da się w przyszłości zapobiec atakom o podobnym charakterze na uczelniach publicznych. Z tego powodu istotne jest poświęcenie większej uwagi tej problematyce, należy podjąć wszelkie możliwe środki ostrożności i być odpowiednio przygotowanym na możliwość wystąpienia niepożądanych sytuacji.

Stosowanie środków zapobiegawczych w zakresie ochrony fizycznej uczelni publicznych

Kwestia ochrony osób i mienia na uczelniach publicznych powinna być przedmiotem zainteresowania i prowadzić do zastosowania odpowiednich elementów ochrony technicznej, przy użyciu wybranych procedur i metod analizy ryzyka, prowadzących do optymalizacji zidentyfikowanych zagrożeń bezpieczeństwa. Dlatego konieczne jest poszukiwanie możliwości zastosowania elementów technologicznych w dziedzinie technologii zabezpieczeń, gdzie rozwój jest skierowany na wprowadzenie innowacyjnych systemów dostępu, umożli-

wiających identyfikację, ewentualnie lokalizację ludzi w danym obiekcie (np. technologia RFID).

W celu prewencji należy rozważyć zastosowanie technologii typowania i profilowania potencjalnych przestępców, odpowiednio ich zamiarów dotyczących przeprowadzenia ataku w oparciu o rejestrację niewerbalnych zachowań ciała, które są niewykrywalne dla ludzkiego oka (temperatura ciała, tętno itp.). W przypadku kiedy czujniki zidentyfikują nieprawidłowości w badanych parametrach, system zaalarmuje ochronę, która spacyfikuje przestępcę.

Z punktu widzenia kosztów odpowiednia jest również już wspomniana technologia RFID, działająca na zasadzie identyfikacji osób na postawie częstotliwości radiowej, za pomocą której organizacja uzyska bezkontaktowo element identyfikacji osób i mienia, ewentualnie ich lokalizacji w obrębie obiektu w czasie rzeczywistym. Zasięg promieni RFID jest obszerny i we współpracy z optymalnymi ustawieniami środków bezpieczeństwa, jest bardzo skutecznym systemem zabezpieczeń, który umożliwia monitorowanie przemieszczania się pracowników, studentów i turystów w obrębie uczelni publicznych.

Aby zapewnić pełne bezpieczeństwo uczelni publicznych, konieczne jest zapewnienie wzajemnej współpracy różnych elementów systemów bezpieczeństwa i dostosowanie ich działania do ochrony obiektów uczelni publicznych. W przypadku, gdy jeden składnik nie będzie optymalny, nie można go skutecznie zastąpić innym, a system uważać za bezpieczny i niezawodny. W związku z tym konieczne jest zwrócenie uwagi na inny istotny element w zakresie ochrony fizycznej, czyli na zarządzanie ryzykiem, które przy odpowiednio dobranej strategii i określeniu skutecznych środków bezpieczeństwa, prowadzi do optymalizacji ryzyka i strat wynikającychz niekorzystnych zdarzeń [4].

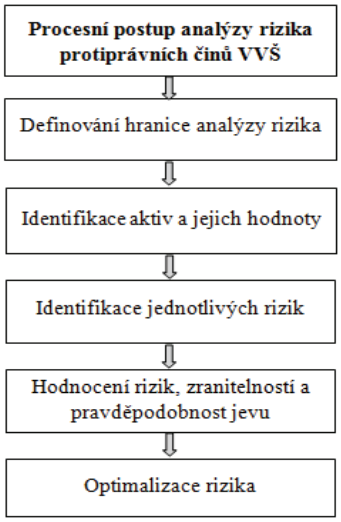
Faktem jest, że pomimo wszystkich środków ostrożności, które wprowadziła dana organizacja zajmującą się zarządzaniem ryzykiem, nie można wykluczyć szeregu negatywnych zjawisk, które mogą prowadzić do poważnego zagrożenia zdrowia osób i innych aktywów uczelni publicznej. Dotyczy to niezwykłych sytuacji, które są sztucznie wywołane, przypadkowe, nieoczekiwane i niebezpieczne dla społeczeństwa, a to ze względu na znaczący wpływ na zdrowie ludzkie, dobra materialne i środowisko. Do tej grupy można zakwalifikować np. wybuch bomby lub pożar. Sprawców tych przestępstw można podzielić na napastników zewnętrznych i wewnętrznych, ewentualnie połączenia obu tych typów, które są bardzo skuteczne, jeśli chodzi o udaną realizację ataku. Przykładem może być student lub pracownik posiadający niezbędną wiedzę na ten temat i dostęp do niej, który współpracuje z przestępcą (np. w przypadku przyniesienia i umiejscowienia bomby).

Faktem pozostaje, że uczelnie publiczne, ze względu na swoje otwarcie dla wszystkich odwiedzających, są łatwym celem ataków terrorystycznych oraz innych form przestępczości, gdzie przy dużej liczbie poruszających się osób na

tych obszarach, nie można na bieżąco określić, kto i w jakim celu wchodzi do budynku. Dlatego konieczna jest prewencja w tym zakresie, czy to w formie analizy ryzyka czy innowacyjnych środków ochrony technicznej, poprawy monitoringu, identyfikacji i ewentualnej lokalizacji ludzi w budynkach tego rodzaju.

Zastosowanie analizy ryzyka na uczelniach publicznych

Analiza ryzyka jest procedurą, która pomaga rozwijać naszą percepcję i zrozumienie tego problemu, jak również przedstawia skuteczne narzędzia wstępne w ramach oceny ryzyka, co prowadzi do decyzji, w jaki właściwy sposób uniknąć ryzyka i zoptymalizować jego potencjalnie negatywny wpływ na zdrowie i życie, zniszczenie mienia lub środowiska. Ogólnie proces analizy ryzyka można graficznie zilustrować przy pomocy schematu blokowego, który jest przedstawiony poniżej.



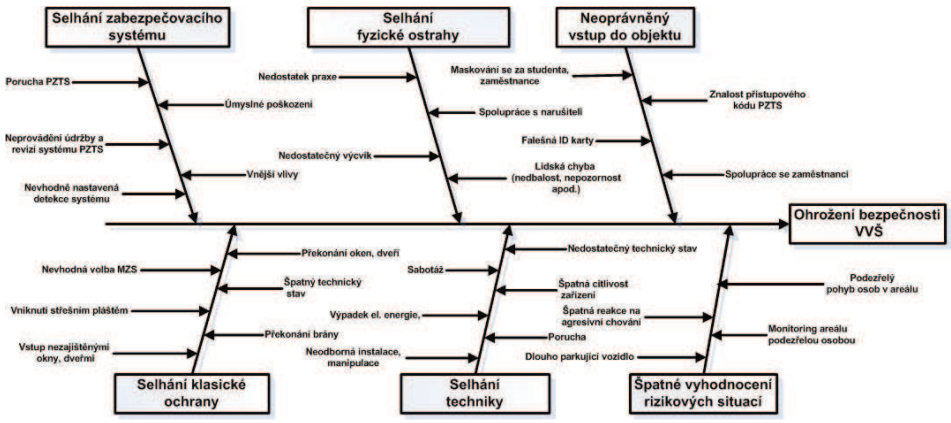
Rys. 1. Schemat blokowy procesu analizy ryzyka

Zasadniczym punktem tej ogólnej procedury jest przedział analizy ryzyka będący granicą ustalania aktywów, które zostaną włączone do analizy lub nie. Fakt ten jest ściśle związany z wyżej wymienioną optymalizacją ryzyka, która jest konieczna w przypadku zminimalizowania ryzyka do poziomu, w którym koszty na jego obniżenie nie będą nieproporcjonalne w porównaniu z odpowiednim ograniczeniem ryzyka (zasada ALARA). Z ekonomicznego punktu widzenia wydatki na optymalizację systemu powinny wynosić około 10% jego aktywów, w wyjątkowych przypadkach mogą wynosić 15%. Dopiero po tych

ustaleniach następuje identyfikacja pojedynczych zagrożeń z określeniem ich stopnia i negatywnego wpływu na wybrane aktywa. Później następuje ustalenie propozycji rozwiązania oraz środków zapobiegawczych, prowadzących do jej optymalizacji.

Obecnie istnieje wiele narzędzi do analizy ryzyka, ale zawsze jest konieczne zdefiniowanie ciągu „niebezpieczeństwo – zagrożenie – uszkodzenia – szkoda", a dopiero potem wybranie odpowiedniej metody, zgodnie z którą ryzyko zostanie ocenione. Do odpowiednich metod analizy ryzyka w środowisku uczelni publicznych można zaliczyć metody prawdopodobieństwa, opinię inżynierów, analogię oraz model [2].

Można powiedzieć, że proces identyfikacji i oceny ryzyka powinien obejmować wykonanie dwóch etapów. W początkowym etapie celem jest uzyskanie kompleksowego przeglądu i wstępnych informacji, które są użytecznym narzędziem dla przybliżonej analizy, do czego odpowiednim przyrządem jest tzw. analiza orientacyjna, która często korzysta z jakościowej formy oceny ryzyka, np. z modelowania ryzyka diagramem Ishikawy. Ogólnie można stwierdzić, że taka analiza orientacyjna może zapewnić przegląd oceniających, dotyczący możliwych przyczyn, które doprowadziły do interesującego ich negatywnego zjawiska, z dostateczną wiedzą i informacjami o jego pochodzeniu. Praktyczny przykład zastosowania metody przy pomocy diagramu Ishikawy przedstawia następujący schemat.



Rys. 2. Analiza ryzyka za pomocą diagramu Ishikawy

Następną orientacyjną analizą ryzyka, którą można w tym celu zastosować, jest metoda podejścia naukowego, czyli analiza przy pomocy drzewa błędów (FTA). Metoda ta jest bardzo systematyczna i pozwala na analizę różnych czynników, wliczając w nie zjawiska fizyczne i interakcję człowieka. Idąc "z góry na dół", uwaga jest skupiona na konsekwencjach błędów, które są bezpośrednio związane ze szczytowym zdarzeniem, takim jak np. eksplozja bomby [1].

Drugim etapem oceny ryzyka powinna być szczegółowa analiza, którą może być już wspomniana orientacyjna analiza jakościowa, ale w celu identyfikacji ryzyk na uczelniach publicznych preferowane są metody ilościowe. Do tej kategorii należy również analiza rodzajów i skutków możliwych błędów (FMEA), która opiera się na rozbiorze rodzajów błędów i ich skutków, co prowadzi do identyfikacji skutków i przyczyn poprzez systematyczne budowanie struktury przeprowadzanych błędów. Metoda ta służy zarówno do kontroli pojedynczych elementów systemu, jak i jego funkcjonowania, która identyfikuje podstawowe błędy. Podczas stosowania metody FMEA ryzyko jest oceniane z punktu widzenia procesu (spowodowane przez czynnik ludzki) i struktury, gdzie przyczyną powstania błędów jest przede wszystkim wada techniczna lub strukturalna. Praktycznym przykładem oceny ryzyka na uczelniach publicznych z punktu widzenia struktury jest incydent w polu widzenia, na powierzchni bocznej, czy w obszarze zainteresowania (np. awaria systemu kamer). Z punktu widzenia procesu chodzi o ryzyko powstałe w procesie specyficznym dla danej uczelni publicznej (np. współpraca niezadowolonego pracownika z przestępcą).

Ze względu na możliwe warianty, ryzyka zostały zidentyfikowane i zakwalifikowane do już wspomnianych kategorii procesu i struktury, gdzie następnie oceniono pojedyncze ryzyko, wiedząc, że ze względu na zagrożenie ryzyko z punktu widzenia procesu jest większe niż ryzyko strukturalne. Wynikiem tej analizy jest zobrazowanie w postaci tabeli, w tym ocena ryzyka przy pomocy tzw. metody Pareto. Graficznym wynikiem tego procesu jest krzywa Lorenza, która przejrzyście unaocznia sytuacje ryzykowne, w których należy zastosować środki bezpieczeństwa. Można powiedzieć, że ryzyka konstrukcyjne mogą być indeksowane z określoną dokładnością (np. przy pomocy wyłomowej bezpieczeństwa), ale wartości indeksów dla procesu nie możemy zastosować, ponieważ nie można dokładnie poznać umysłu niezadowolonego pracownika, który chce wnieść na uczelnię publiczną bombę. Ryzyko błędu ludzkiego i inne zagrożenia o podobnym charakterze można jednak przewidzieć na podstawie danych statystycznych lub praktyki, a następnie przeliczyć na podstawie wybranych metod i narzędzi [4].

Analizy definiowania błędu ludzkiego w zakresie ochrony fizycznej na uczelniach publicznych

Czynnik ludzki, odpowiednio błąd ludzki, jest trudny do wykrycia i z punktu widzenia ochrony fizycznej uczelni publicznych jest bardzo istotnym zagrożeniem, któremu należy w ramach prewencji poświęcić większą uwagę. Na ludzkie działanie i zachowanie w każdej sferze życia mają wpływ obawy o własne zdrowie, życie bliskich czy poczucie zagrożenia i uszkodzenia mienia. Chociaż procesy związane z ludzkim zachowaniem nie można precyzyjnie określić, są poszukiwane innowacyjne metody i narzędzia przeznaczone chociaż do częściowego ustalenia i zdefiniowania procesów związanych z czynnikiem ludzkim. Błąd ludzki jest zasadniczo działaniem lub próbą działania, przez które przekraczane są graniczne wartości parametrów systemowych, które mogą pojawić się w skutek błędu lub chwilowego braku uwagi człowieka. Wynik ten może być spowodowany wieloma przyczynami, od zaniedbania fizycznej lub psychicznej sprawności, po niewłaściwe szkolenie i brak podstawowych informacji (wymagania dla pilnowania kluczy, kontroli ludzi, itp.).

Jak już wspomniano, kwantyfikację powstawania błędu ludzkiego można przeprowadzać w oparciu o ogólne dane statystyczne, ewentualnie na podstawie eksperymentu. Do metod kwantyfikacji błędu ludzkiego należą np. analiza statystyczna subiektywnych szacunków, porównania par, TESEO, metoda diagramów zależności IDA, HEART, THERP, ASEP, baza danych kwantyfikowanej charakterystyki ludzkiej ingerencji NUCLARR i inne. Z przedstawionych metod, na podstawie praktyki, można polecić metodę TESEO, która określa wiarygodność czynnika ludzkiego na podstawie pięciu kryteriów, które są wzajemnie połączone (współczynnik typu aktywności, warunków i czasu, cechy osobiste, niepokój, zmęczenie, stres oraz ergonomiczne czynniki). Uzyskaną wartość indeksu można odczytać z tabel przy pomocy iloczynu indeksu, również odczytanego z tabel dla poszczególnych kryteriów. Jeśli iloczyn wszystkich pięciu wyników osiągnie większą wartość liczbową niż 1, zakłada się, że wystąpi błąd ludzki. Jeśli wynik jest w zakresie od 0,7 do 0,9, istnieje prawdopodobieństwo wystąpienia błędu ludzkiego, a jeżeli wynik jest w zakresie od 0 do 0,6, nie ma zagrożenia wystąpienia błędu ludzkiego. Na wystąpienie błędu ludzkiego ma również wpływ środowisko i wzajemna interakcja z obiektami (chroniony obiekt jest położony w pobliżu cmentarza, luksusowych will, itp.), które w danej osobie mogą wzbudzić negatywne uczucia, prowadzące do tego błędu.

Do oceny tych wpływów można stosować metodę SHELL, gdzie symbol S oznacza oprogramowanie (instrukcje postępowania itp.), H – sprzęt (np. scentralizowana ochrona), E – otoczenie (środowisko wykonywania zawodu), pierwsza litera L oznacza użytkownika (jednostka w centrum zainteresowania),

druga L – resztę osób, z którymi ma kontakt jednostka. W analizie SHELL ocenia się skutki poszczególnych czynników (oznaczonych literami) na człowieka [4]. Na przykład wpływ klienta na ochronę fizyczną (L-L), wpływ systemu kamer na człowieka (L-H) lub wpływ dyrektyw organizacji, do których stosuje się ochrona (L-S). Czynników, które wpływają na ludzkie zachowania i działania, jest bardzo dużo. W chwili obecnej istnieje jednak szerokie spektrum metod radzenia sobie z ich oceną, które powinny być przez organizację zastosowane w celu działań prewencyjnych oraz zwiększenia poziomu bezpieczeństwa.

Zakończenie

Artykuł dotyczył omówienia oceny i identyfikacji zagrożeń bezpieczeństwa w środowisku uczelni publicznych. W zakresie ochrony fizycznej można stwierdzić, że w tej dziedzinie istnieje szeroka skala potencjalnych zagrożeń, gdzie niektóre mogą wydawać się nieistotne, a przy sporadycznej analizie trudne do zidentyfikowania. Przykładem takiego niebezpieczeństwa jest ryzyko wystąpienia błędu ludzkiego, który w przypadku pojawienia się może mieć negatywny wpływ na bezpieczeństwo i ochronę osób lub mienia.

Przedmiotem artykułu było wskazanie na możliwości zastosowania odpowiednich środków ochrony technicznej, a zwłaszcza wybranych narzędzi i metod analizy ryzyka, które powinny być podstawą do zarządzania ryzykiem w każdej organizacji oraz środkiem prowadzącym do optymalizacji poziomu bezpieczeństwa w środowisku uczelni publicznych.

Nawiązania do projektu

Powyższy artykuł jest publikowany w tym samym celu co projekt pod nazwą „Ocena i standaryzacja ochrony fizycznej obiektów uczelni publicznych” w ramach programu badań nad bezpieczeństwem w Republice Czeskiej w latach 2010–2015 pod numerem dotacji VG20102013036.

Literatura

[1] Bernatík Aleš, Prevence závažných havárií I., Sdružení požárního a bezpečnostního inženýrství v Ostravě, 2006, ISBN: 80-86634-89-2.
[2] Loveček Tomáš, Veľas Andrej (2010). Technické zabezpečenie ochrany poštových prevádzok. Trilobit, Zlín, 2010, roč. 10, č. 1, s. 1–5, ISSN 1804-1795.
[3] Reitšpis Josef a kol. (2004). Manažérstvo bezpečnostných rizík. 1. vyd. Žilina: Žilinská universita, 2004. 296 s. ISBN 80-8070-328-0.

[4] Ščurek Radomír, Konečný Martin (2011). Aplikace analýzy rizik v oblasti fyzické ochrany veřejných vysokých škol. In: Sborník vědeckých prací Vysoké školy báňské – Technické univerzity Ostrava: řada bezpečnostní inženýrství. 1. vyd. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2011, s. 27–32. ISSN 1801-1764 [cit. 2012-06-10]. Dostupné z: http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/cs/sys/resource/pdf/veda-a-vyzkum/sbornik/2011-1-sbornik.pdf

Radomír Ščurek, Martin Konečný, Ondřej Stoniš
VŠB – Technical University of Ostrava

ASSESSMENT OF SECURITY RISKS OF PUBLIC UNIVERSITIES IN TERMS OF PHYSICAL PROTECTION

Abstract

The article deals with the occurrence of illegal acts and other forms of crime in the environment of public universities (referred to as PU) relating to the operation of objects of this nature. The paper is also focused on the application of selected methods of risk analysis and the evaluation of the impact of human error as a risk factor in the complex process of physical protection of persons and property in the environment of public universities.

Keywords: security risk, public universities, analysis, human factor, physical protection.