Andrzej Tomczak

Zasady sztuki

przy wykonywaniu systemów zabezpieczeń

Ustawa o swobodzie działalności gospodarczej pozwala praktycznie każdemu na wykonywanie zabezpieczeń systemami alarmowymi, nie żądając zaliczania przedtem kursów specjalistycznych. Trudno się dziwić, że wiele obiektów w Polsce było i jest zabezpieczanych nieprawidłowo. Projektanci i instalatorzy systemów zabezpieczeń w obiektach cywilnych nie mogli również do niedawna znaleźć oparcia w Polskich Normach.

Brak spisanych wymagań powodował, że kryterium najniższej ceny stanowił pretekst do realizacji zabezpieczeń niezgodnie z „zasadami sztuki". Doprowadziło to do degradacji branży w Polsce. Bardzo często inwestorzy udają, że płacą, instalatorzy udają, że zabezpieczają, stacje monitorowania udają, że monitorują itd.

Nasza branża doczekała się wreszcie kilku dokumentów, które (przynajmniej częściowo) określają „zasady sztuki" w projektowaniu, wykonywaniu i eksploatacji elektronicznych systemów zabezpieczeń technicznych. Są to przede wszystkim nowe normy europejskie i polskie, a szczególnie arkusze norm określające tzw. wytyczne stosowania. Do tych dokumentów powinni odwoływać się projektanci i instalatorzy, aby swojej pracy nadać profesjonalny charakter. Takimi dokumentami są:

- opublikowana w języku polskim w 2011 r. specyfikacja techniczna **PKN-CLC/TS 50131-7:2011** ***Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 7: Wytyczne stosowania***,
- Załącznik 1 – ***Wymagania dla elektronicznych systemów zabezpieczeń*** do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 7 września 2010 r. *w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne* (Dz.U. nr 166, poz. 1128);
- Załącznik 2 – ***Metodyka doboru środków bezpieczeństwa fizycznego*** do rozporządzenia Prezesa Rady Ministrów *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych* (projekt po konsultacjach).

Polska Izba Systemów Alarmowych dołożyła starań, aby zasady określone w powyższych dokumentach były zbieżne ze sobą oraz z zapisami norm europejskich i polskich dot. systemów alarmowych:

- PN-EN 50131 (systemy sygnalizacji włamania i napadu),
- PN-EN 50132 (systemy dozorowe CCTV stosowane w zabezpieczeniach),
- PN-EN 50133 (systemy kontroli dostępu stosowane w zabezpieczeniach),
- PN-EN 50136 (systemy i urządzenia transmisji alarmu).

Zgodnie z ustawą z 12 września 2002 r. *o normalizacji* stosowanie norm nie jest obowiązkowe; wprowadzenie do rozporządzeń zapisów równoważnych z zapisami norm powoduje, że stają się obowiązkowe w obiektach, które podlegają danym rozporządzeniom.

Specyfikacja techniczna PKN-CLC/TS 50131-7:2011

Specyfikacja techniczna podaje zalecenia, jak przeprowadzić prawidłowo proces projektowania, wykonania i eksploatacji systemu alarmowego sygnalizacji włamania i napadu. Dokument napisany w formie instrukcji trudno streścić – trzeba się po prostu z nim zapoznać. Można podzielić go na kilka części.

Część pierwsza (wstępna) to m.in. powtórzenie, za arkuszem PN-EN 50131-1, zasad stopniowania zabezpieczenia oraz klasyfikacji klimatycznej urządzeń i systemów alarmowych SWiN. Dla przypomnienia, rozróżniamy cztery stopnie zabezpieczenia od 1 do 4 (stopień 1 jest najniższy) oraz cztery klasy środowiskowe: klasę I – środowisko wewnętrzne, klasę II – środowisko wewnętrzne ogólne, klasę III – środowisko zewnętrzne (zewnętrzne osłonięte lub wewnętrzne przy ekstremalnych warunkach środowiskowych), klasę IV – środowisko zewnętrzne ogólne.

Nie można porównywać klasy urządzeń A, B, C i S wg normy PN 93/E-08390.14 ze stopniami 1, 2, 3 i 4 wg PN-EN, gdyż klasyfikacja starej normy nie uwzględniała np. różnic we właściwościach wykrywczych urządzeń różnych klas – koncentrowała się głównie na odporności na drgania i impulsy elektromagnetyczne oraz na odporności klimatycznej. Nowa m.in. w tym celu wprowadza odrębną klasyfikację klimatyczną.

Nie można też porównywać systemów starych klas SA1, SA2, SA3 i SA4 do systemów nowych stopni 1, 2, 3 i 4, choćby z tego względu, że wymagania starej normy są zawarte na trzech stronach arkusza normy, natomiast w nowej na 22 stronach. Można jedynie próbować analizować tylko wybrane cechy i poddawać je porównaniu w celu ustalenia, które stopnie czy klasy dla tej konkretnej cechy są bardziej lub mniej wymagające.

W części specyfikacji dotyczącej projektowania i planowania instalacji omawiane są kolejne etapy do zrealizowania. Szeroko opisano temat wizji lokalnej, doboru elementów, lokalizacji urządzeń i procedur związanych z działaniem systemu. W załącznikach można znaleźć bardziej szczegółowe informacje. W kolejnej omówiono procesy: wykonania instalacji, sprawdzania zgodności, badań funkcjonalności i uruchomienia. W ostatniej części określono sposób dokumentowania wykonanego systemu, zasady związane z obsługą, konserwacją i naprawami systemów.

Wymagania dla elektronicznych systemów zabezpieczeń – Załącznik 1 do rozporządzenia MSWiA z 7 września 2010 r.

Rozporządzenie MSWiA dotyczy grupy obiektów, w których są przechowywane wartości pieniężne: krajowe i zagraniczne znaki pieniężne, czeki i weksle (z wyjątkami określonymi w rozporządzeniu), inne dokumenty zastępujące w obrocie gotówkę, złoto, srebro, platynę i inne metale z grupy platynowców oraz wyroby z tych metali, kamienie szlachetne i perły (z wyjątkiem przedmiotów będących muzealiami w rozumieniu ustawy z 21.11.1996 r. o muzeach). A jest tych obiektów, wbrew pozorom, nie tak mało.

Zgodnie z zapisami § 2.1 rozporządzenia omawiane przepisy dotyczą systemów przeznaczonych do ochrony wartości pieniężnych w obiektach podlegających obowiązkowej ochronie z mocy ustawy.

Natomiast § 2.2 rozciąga przepisy na wszystkich przedsiębiorców i jednostki organizacyjne, przechowujących wartości pieniężne przekraczające 0,2 jednostki obliczeniowej (w I kwartale 2012 r. wartość >86 082 zł. Mają oni obowiązek zapewnie-

nia co najmniej zabezpieczenia technicznego tych budynków lub pomieszczeń.

Dotyczy to również małych obiektów bankowych, które nie podlegają obowiązkowej ochronie, ale na ich terenie przechowuje się wartości pieniężne przekraczające 0,2 jednostki obliczeniowej. Dotyczy także sklepów i hurtowni jubilerskich, w których przechowuje się wyroby z metali i kamieni szlachetnych o wartości przekraczającej 0,2 jednostki obliczeniowej. Dotyczy również sklepów, których utarg przekracza 0,2 jednostki obliczeniowej ltd.

Zapisy zawarte w tym dokumencie są zbieżne z polskimi normami. Omówimy tylko najważniejsze z nich. W obu dokumentach opisano konieczność prowadzenia tzw. książki zapisów (nazwanej również książką systemu). W załączniku 1 rozporządzenia podano:

21. Wszelkie zdarzenia utrwalone przez system, czynności konserwacyjne, uszkodzenia, przypadki nieprawidłowego działania systemu oraz naprawy powinny być rejestrowane w Książce Elektronicznego Systemu Zabezpieczeń, przechowywanej w chronionym obiekcie. Zawartość KESZ określono w art. 22.

Po wejściu w życie rozporządzenia (7 września 2010 r.) Książkę Systemu należało zaprowadzić dla każdego systemu zabezpieczeń chroniącego obiekt, który podlega wymogom rozporządzenia.

Załącznik 1 do arkusza 7 normy 50131 podaje przykład Książki Zapisów (Książki Systemu), która może być wykorzystywana do zapisu zdarzeń. „Zdarzenie" należy rozumieć jako epizod mający duże znaczenie dla bezpieczeństwa obiektu chronionego, np. alarm faktyczny czy fałszywy, natomiast nie chodzi o sytuacje normalne, jak włączenie czy wyłączenie systemu. Przykładowe przyczyny wpisów podawane w Załączniku 1: niepożądane stany alarmowe, badania, wizyty konserwacyjne, czasowe braki połączeń, uszkodzenia oraz wizyty naprawcze.

Oba dokumenty mają również zbieżne zapisy dotyczące konserwacji systemów. W rozdziale 13 wytycznych stosowania stwierdza się, że to klient odpowiada za zapewnienie właściwej konserwacji (rozumianej jako przeglądy i serwisowanie), a gdy zajdzie taka potrzeba – naprawy systemu. Dokument zaleca również, aby ustalenie harmonogramu konserwacji nastąpiło natychmiast po ukończeniu instalacji. Odpowiednie punkty rozporządzenia brzmią następująco:

19. Stopień zabezpieczenia uzyskany przez system może być utrzymany pod warunkiem wykonywania systematycznej konserwacji oraz dokonywania niezbędnych napraw. Konserwacja powinna odbywać się w okresach przewidzianych właściwymi dla danego systemu normami technicznymi, a gdy nie ustalono takich norm – nie rzadziej niż raz na 6 miesięcy.

20. Przedsiębiorca lub kierownik jednostki organizacyjnej, w której są przechowywane wartości pieniężne, jest odpowiedzialny za wdrożenie konserwacji, o której mowa w pkt 19, niezwłocznie po zainstalowaniu systemu.

Zapisy rozporządzenia nie pozostawiają cienia wątpliwości, co się stanie, jeżeli system nie będzie systematycznie konserwowany i naprawiany. **System utraci stopień zabezpieczenia.**

Metodyka doboru środków bezpieczeństwa fizycznego – Załącznik 2 do rozporządzenia Prezesa RM *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych*

To kolejny dokument określający m.in. „zasady sztuki". Opisano w nim środki bezpieczeństwa fizycznego stosowane do zabezpieczania informacji niejawnych, do których w grupie elektronicznych środków pomocniczych zaliczono: systemy KD, SSWiN oraz CCTV. W Załączniku 2 opisano metodykę doboru środków bezpieczeństwa fizycznego w zależności od poziomu zagrożeń (odpowiednio dla danej klauzuli tajności określa się poziom zagrożeń jako niski, średni i wysoki, korzystając z Załącznika 1 do rozporządzenia *Podstawowe kryteria i sposób określania poziomu zagrożeń*).

Poszczególnym środkom bezpieczeństwa fizycznego przydziela się punkty, a po ich zsumowaniu sprawdza się, czy zastosowane wielopoziomowe środki bezpieczeństwa fizycznego są wystarczające do ochrony informacji niejawnych dla określonej klauzuli tajności i uzyskanego poziomu zagrożeń.

Szczegółowe omówienie tego dokumentu przekracza ramy artykułu, skoncentrujemy się na wykazaniu podobieństw zapisów w obu rozporządzeniach oraz normach europejskich i polskich. We wszystkich dokumentach występuje określenie „poświadczenie zgodności".

§ 12.3 rozporządzenia MSWiA mówi: *Urządzenia stosowane w elektronicznym*

systemie zabezpieczeń, dla których jest wymagana klasyfikacja, powinny posiadać odpowiednie do wymaganej klasyfikacji certyfikaty lub deklaracje zgodności w rozumieniu przepisów o systemie oceny zgodności, zaś elektroniczny system zabezpieczeń powinien posiadać wydane przez dostawcę poświadczenie zgodności z wymogami określonymi w niniejszym rozporządzeniu.

W § 4.6 Rozporządzenia RM dotyczącego środków bezpieczeństwa fizycznego stwierdza się: *Elektroniczny system pomocniczy wspomagający ochronę informacji niejawnych powinien posiadać wydane przez dostawcę, z uwzględnieniem przepisów o systemie oceny zgodności, poświadczenie zgodności z wymogami określonymi w rozporządzeniu.*

Dla porównania arkusz 7 normy 50131 zaleca, aby firma instalacyjna dostarczyła klientowi poświadczenie zgodności stwierdzające, że system alarmowy SWiN został zainstalowany zgodnie z dokumentacją powykonawczą, uzupełnione o potwierdzenie spełniania wymagań prawa, przepisów, specyfikacji krajowych lub europejskich. Poświadczenie zgodności z wymogami rozporządzenia wypełnia drugą część zaleceń normatywnych dla poświadczenia zgodności (pierwsza to oczywiście poświadczenie wykonania systemu zgodnie z przekazaną dokumentacją powykonawczą).

W przypadku systemów telewizji dozorowej oba rozporządzenia wymagają rejestracji wizji o rozdzielczości min. 400 TVL. Jest to zgodne z zapisami normy PN-EN 50132-7:2003 określającej wytyczne stosowania dla systemów CCTV. W kryteriach projektowych systemów zakłada się, że aby skorzystać z wytycznych dotyczących rozmiarów osób na potrzeby identyfikacji, rozpoznania, detekcji intruza i kontroli tłumu, rozdzielczość zainstalowanego systemu CCTV musi przewyższać 400 TVL.

Norma nie określa czasu rejestracji zapisu wizyjnego. W tym przypadku rozporządzenia wyręczają normę. I tak dla systemów używanych do zabezpieczania wartości pieniężnych minimalny czas rejestracji to 14 dni, zaś w systemach wspomagających zabezpieczanie informacji niejawnych 30 dni.

Oba rozporządzenia przewidują 3 lata na dostosowanie systemów CCTV do wymogów rozporządzenia (okres dostosowawczy wynikający z rozporządzenia MSWiA kończy się we wrześniu 2013 r.).

W zakresie systemów SWiN oba rozporządzenia określają poziomy nadzoru dla poszczególnych stopni zabezpieczenia w sposób zgodny z tabelą F.1 w wytycznych stosowania PKN-CLC/TS 50131-7:2011. Jest to jeden z ważniejszych zapisów, który wskazuje minimalne wymagania w zakresie nadzoru dla systemów poszczególnych stopni.

Przykładowo, rozporządzenie MSWiA definiuje takie wymagania następująco:

5. Określa się następujące rodzaje czynności, jakie powinien wykrywać system sygnalizacji włamania i napadu w zależności od stopnia zabezpieczenia: (...)

5.4. Stopień 4:

- otwarcie drzwi, okien i innych zamknięć chronionego obszaru,

- penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania,

- penetrację ścian, sufitów i podłóg,

- poruszanie się w chronionym obszarze (pułapkowo),

- atak na urządzenia i miejsca szczególnie zagrożone.

Natomiast załącznik 2 do rozporządzenia RM definiuje poziomy nadzoru następująco:

Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania;

Typ 4 (...)

System charakteryzuje się następującymi cechami:

1) spełnia wymagania systemu stopnia 4 określone w normie PN-EN 50131-1;

2) obejmuje ochroną cały obszar, w tym szafy służące do przechowywania informacji niejawnych i sygnalizuje co najmniej:

a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru,

b) penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania,

c) penetrację ścian, sufitów i podłóg,

d) poruszanie się w chronionym obszarze (pułapkowo – nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia),

e) atak na szafy służące do przechowywania informacji niejawnych; (…)

Jeśli chodzi o dostosowanie systemów SWiN do sytuacji po wejściu w życie nowych przepisów, każde z rozporządzeń potraktowało to inaczej. Rozporządzenie MSWiA akceptuje systemy wykonane przed wejściem w życie rozporządzenia w klasie minimum SA3 (z zastrzeżeniami dotyczącymi przebudowy systemu). Rozporządzenie RM ten problem traktuje odmiennie. Jeżeli chcemy dalej eksploatować system wykonany przed wejściem w życie rozporządzenia wykonany w klasie minimum SA3, do punktacji otrzymywanej za taki system podchodzimy następująco: jeżeli system spełnia wymagania w zakresie ochrony i nadzoru określone dla stopnia 1 (czujka otwarcia drzwi i czujki przestrzenne) – za taki system dostajemy 0 punktów, jeżeli system spełnia wymagania w zakresie ochrony i nadzoru określone dla stopnia 2 (czujka otwarcia drzwi, czujki otwarcia okien i czujki przestrzenne) – dostajemy 1 punkt itd.

Czyli system wykonany przed wejściem w życie rozporządzenia RM nie będzie mógł być klasyfikowany, jeżeli nie obejmie nadzorem przynajmniej otwarcia drzwi, okien i innych zamknięć chronionego obszaru oraz poruszania się w chronionym obszarze (wykrywanie pułapkowe). Chcąc uzyskać odpowiednią liczbę punktów, w ciągu 3 lat należy taki system odpowiednio dozbroić (możemy uzyskać w ten sposób nawet 3 punkty za system spełniający wymagania ochrony i nadzoru określonych dla stopnia 4).

Wreszcie przepisy prawa są ze sobą spójne oraz zgodne z normami europejskimi i polskimi.

A co z pozostałymi obiektami? Skoro w omawianych dokumentach normatywnych i prawnych „zasady sztuki" określono, warto je stosować nie tylko w obiektach, w których z mocy ustaw lub rozporządzeń taki obowiązek występuje. Jeżeli wokół wykonania systemu zabezpieczeń rozgorzeje spór, który trafi na wokandę, trzeba będzie w trakcie postępowania sądowego wykazać, że pracę wykonało się prawidłowo – czyli zgodnie z zasadami sztuki czy dobrą praktyką. A wykazanie tego bez oparcia się na wiarygodnych dokumentach (a takimi są bez wątpienia normy czy przepisy prawa) może okazać się bardzo trudne.

Nie wszystkie zapisy znalazły się w obu omawianych rozporządzeniach. Ale nie musiały. Jeżeli system wykonany w kancelarii tajnej uzyskał stopień 2 a nie jest konserwowany czy naprawiany, traci go – ponieważ taką zasadę opisano w normie i rozporządzeniu MSWiA. Zasada ogólna nie musi być powtarzana w każdym kolejnym rozporządzeniu. Innym przykładem jest Książka Elektronicznego Systemu Zabezpieczeń (KESZ), opisana w normie i rozporządzeniu MSWiA. System w kancelarii tajnej może nie mieć takiego dokumentu, gdyż w zakresie ochrony informacji niejawnych nie ma takiego obowiązku, co nie znaczy, że nie trzeba dokumentować zdarzeń tam zapisywanych (np. naprawy, konserwacje). A jeśli tak, to może lepiej nie mieć kłopotu i zaprowadzić KESZ?

Odpowiedzialność karna

Odpowiedzialności karnej poświęcono już odrębny artykuł (*Czy to już kres „wolnej amerykanki"? O odpowiedzialności prawnej zamawiającego, wystawcy deklaracji zgodności i dostawcy (instalatora) elektronicznych systemów zabezpieczeń technicznych – SA 2/2011)*. Warto jednak

przypomnieć: *Kto, wbrew obowiązkowi, nie zapewnia fizycznej lub technicznej ochrony obszaru, obiektu, urządzeń lub transportu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

Jeśli nierzetelny polski producent lub upoważniony na piśmie polski przedstawicieli producenta wystawią niezgodnie z prawdą deklarację zgodności urządzeń wykorzystywanych do zabezpieczenia obiektów podlegających obowiązkowej ochronie, albo instalator, który wbrew stanowi faktycznemu podpisze poświadczenie zgodności wykonania sytemu w obiekcie podlegającym obowiązkowej ochronie, wówczas mamy do czynienia z **art. 271 §1 kk**, a właściwie jego kwalifikowaną postacią opisywaną w § 3, zagrożoną pozbawieniem wolności od 6 miesięcy do 8 lat.

(Art. 271 § 1. Funkcjonariusz publiczny lub inna osoba uprawniona do wystawienia dokumentu, która poświadcza w nim nieprawdę co do okoliczności mającej znaczenie prawne, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. (…)

§ 3. Jeżeli sprawca dopuszcza się czynu określonego w § 1 w celu osiągnięcia korzyści majątkowej lub osobistej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.)

Tyle gwoli przypomnienia. Natomiast nie zamyka to kręgu odpowiedzialności karnej. Coraz częściej słyszy się, że inwestorzy nakłaniają instalatorów do wystawiania poświadczeń zgodności niezgodnie z prawdą.

Szanowni Instalatorzy, jeżeli wystawicie w takiej sytuacji nieprawdziwe poświadczenie zgodności, to fakt wpływu Inwestora nie zmniejszy Waszej odpowiedzialności, chociaż będziecie mieć satysfakcję, że (w razie czego) nie pójdziecie do więzienia sami. Otóż ten, kto was namawiał do popełnienia przestępstwa, może zostać ukarany za tzw. podżeganie. (**art. 18 § 2 kk** – *Odpowiada za podżeganie, kto chcąc, aby inna osoba dokonała czynu zabronionego, nakłania ją do tego)*. Zgodnie z **art. 19 kk** sąd wymierzy za podżeganie karę w granicach zagrożenia przewidzianego za sprawstwo – od 6 miesięcy do 8 lat.

Ale to nie wszystko. Jeżeli do podpisania deklaracji zgodności czy poświadczenia niezgodnego z prawdą zmusza was np. przełożony, na niego również znajdzie się paragraf. **art. 18 § 1 kk** mówi bowiem: *Odpowiada za sprawstwo nie tylko ten, kto wykonuje czyn zabroniony sam albo wspólnie i w porozumieniu z inną osobą, ale także ten, kto kieruje wykonaniem czynu zabronionego przez inną osobę lub, wykorzystując uzależnienie innej osoby od siebie, poleca jej wykonanie takiego czynu.*

Widzimy zatem, że branża zabezpieczeń powinna wreszcie zacząć się zmieniać. Bo jak powiadają prawnicy: Temida nierychliwa, ale sprawiedliwa.

Uwagi końcowe

Po raz pierwszy w branży zabezpieczeń zasady sztuki opisane w normie znalazły odzwierciedlenie w polskim prawie. Kosztowało to przedstawicieli PISA ponad 3 lata wytężonej, społecznej pracy. Pracowaliśmy w zespole dwuosobowym – ja jako ekspert PISA z Henrykiem Dąbrowskim, przedstawicielem PISA – korzystając ze wsparcia merytorycznego Maksymiliana Majerskiego, eksperta PISA.

Normy oraz omawiane rozporządzenia powinny się stać podstawowymi dokumentami wykorzystywanymi do szkolenia branży, a także zamawiania oraz wykonywania systemów zabezpieczeń. □