STANISŁAW TOPOLEWSKI
ORCID: 0000-0001-8268-3754
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Zagrożenia dla bezpieczeństwa informacji

Dlaczego chronimy informacje?

Jedną z charakterystycznych cech współczesnej cywilizacji jest bez wątpienia permanentny wzrost zarówno roli, jak i znaczenia informacji.

Informacja jest jednym z najcenniejszych naszych zasobów i przybiera postać nie tylko danych, ale również wiedzy i umiejętności. Jest nośnikiem najnowszych technologii przemysłowych, pokojowych czy wojskowych. Zasoby informacyjne są nie tylko najbardziej wartościowymi narzędziami na rynkach kapitałowych i inwestycyjnych, lecz także doskonale sprawdzają się w walce na scenie politycznej i służą osiąganiu wpływów politycznych[1].

Współcześnie zdecydowana większość podmiotów i organizacji uzależniona jest od dostępu do informacji, które decydują o ich rozwoju i pozycji na rynku. Bowiem obok zasobów surowcowych i energetycznych, zasoby informacyjne stanowią najistotniejszy czynnik potencjału cywilizacyjnego. Posiadają charakter zasobów strategicznych o istotnej wartości, są czynnikiem rozwoju cywilizacyjnego i gospodarczego oraz sprzyjają powstawaniu nowych branż i nowych profesji. Elementem efektywnej strategii ekonomicznej (gospodarczej) jest przewaga informacyjna na rynkach lokalnych i globalnych[2].

[1] K. Lidel, *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej*, [w:] *Bezpieczeństwo XXI wieku. Asymetryczny świat*, red. K. Liedel, P. Piasecki, T.R. Aleksandrowicz, Difin, Warszawa 2011, s. 27.

[2] P. Sienkiewicz, *Bezpieczeństwo informacji – wspólne dobro dla racji stanu, bezpieczeństwa i obronności kraju, firm i obywateli,* [w:] *Ochrona informacji niejawnych i biznesowych. Materiały IV Kongresu*, KSOIN, UŚ, Katowice 2008, s. 15-16.

Zdecydowana większość obywateli naszego kraju posiada, dysponuje i przetwarza wiadomości, informacje, materiały (dokumenty), które – z różnych względów – nie powinny być powszechnie dostępne. Dotyczy to informacji wynikających z charakteru pracy, jak również szeroko rozumianej sfery prywatnej (korespondencja, banki, urzędy, szkoły, uczelnie, placówki służby zdrowia itd.).

Najogólniej informacje możemy podzielić na wrażliwe i niewrażliwe. Wrażliwymi są te wszystkie informacje, które muszą być chronione, bo tak nakazują przepisy prawa. Zaliczyć do nich możemy informacje niejawne i dane osobowe, a także inne informacje wskazane w organizacji przez kompetentne organy (np. służby ochrony państwa czy wewnętrzne komórki bezpieczeństwa w danej organizacji) jako informacje wrażliwe[3]. Takimi informacjami mogą być też dane, w zasadzie same w sobie niewrażliwe, które w powiązaniu z innymi informacjami pozwalają na wyciągnięcie określonych wniosków. Informacjami wrażliwymi są też informacje dotyczące życia osobistego ważnych przedstawicieli państwa czy przedsiębiorców, których ujawnienie mogłoby posłużyć do nacisków czy też do szantażu określonych osób. Należy również mieć świadomość, że agregacja dokumentów (informacji) jawnych stwarza zagrożenie ich analizy i uzyskania na jej podstawie informacji wrażliwych.

Szczególną troską otacza się te informacje, których ujawnienie może wywrzeć negatywny wpływ na bezpieczeństwo państwa, jego struktury, w tym także określonych instytucji, oraz obywateli. Natomiast szczególnej ochronie podlegają informacje niejawne, czyli te, których „nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania”[4]. Również w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej mocno akcentowane są zagadnienia związane z ochroną i bezpieczeństwem informacji w różnych wymiarach[5].

Dlatego, by zachować stabilność państwa i dawać poczucie bezpieczeństwa obywatelom, najważniejszym zadaniem i obowiązkiem rządu i jego wyspe-

[3] Tamże.

[4] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228).

[5] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, Warszawa 2020.

cjalizowanych służb jest ochrona tych informacji. Może ją zapewnić właściwie zorganizowany i sprawnie funkcjonujący system, który będzie gwarantował ograniczenia w dostępie osób zwłaszcza do informacji wrażliwych, właściwe ich przetwarzanie, a także wykorzystanie odpowiednich i wystarczających środków bezpieczeństwa fizycznego i teleinformatycznego. Z tego też względu system ten wymaga na poziome państwa precyzyjnie określonych zasad i norm mających umocowanie w przepisach prawa, określających zasady wytwarzania informacji, sposób ich ochrony oraz sankcje, jakie mogą zostać zastosowane w przypadku niestosowania się do tych reguł.

Zagrożenia – rozumienie pojęcia

W literaturze przedmiotu znajdujemy wiele definicji terminu „zagrożenia" w zależności od przyjętego kryterium, uwarunkowań czy podejścia np. terenu, obiektu, obszaru, środowiska, czasu i wielu innych czynników. Dla przykładu kilka z wielu definicji:

1) „Zagrożenie to możliwość wystąpienia jednego z negatywnie wartościowanych zjawisk"[6].
2) „Zagrożenie to (…) sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia. Przyjmując za podstawę dziedziny, w których może wystąpić zagrożenie, wyróżnia się zagrożenia militarne i niemilitarne. Wśród zagrożeń niemilitarnych można z kolei wyróżnić zagrożenia polityczne, gospodarcze, psychospołeczne, ekologiczne, wewnętrzne i inne"[7].
3) „Zagrożenia – z jednej strony, to pewien stan psychiczny lub świadomościowy wywołany postrzeganiem zjawiska, które subiektywnie ocenia się jako niekorzystne lub niebezpieczne – z drugiej strony, czynniki obiektywne powodujące stany niepewności i obaw"[8].
4) „Zagrożenie to szeroki całokształt zjawisk, które stwarzają bezpośrednią groźbę obniżenia w krótkim czasie jakości życia ludności państwa i

[6] F.X. Kaufmann, *Koncepcja socjologii religii*, ZW Nomos, Kraków 2006.
[7] *Słownik terminów z zakresu bezpieczeństwa narodowego*, Wyd. AON, Warszawa 2008, s. 172.
[8] S. Korycki, *System bezpieczeństwa Polski*, Wyd. AON, Warszawa 1994, s. 54.

stanowią poważne ograniczenia swobody wyboru w polityce lub działaniach podmiotów nierządowych (osób, grup, korupcji)”[9].

5) „Zagrożenie to możliwość powstania sytuacji, w której dane społeczeństwo nie ma zapewnionych warunków bytu i rozwoju lub są one w sposób istotny ograniczone”[10].
6) Zagrożenia to sytuacje, w której naruszone mogą być istotne dla danego podmiotu wartości. Szersza definicja leksykalna podaje, że zagrożenie to sytuacja, w której istnieje zwiększone prawdopodobieństwo utraty życia, zdrowia, wolności albo dóbr materialnych. Zagrożenie wywołuje u człowieka niepokój lub strach o różnym stopniu natężenia, do przerażenia lub obezwładnienia włącznie, bądź odruch lub świadomą chęć przeciwdziałania. Zagrożenie może wynikać z przyczyn naturalnych (np. oddziaływania żywiołów) i spowodowanych przez innego człowieka (np. nieprzyjaciela)[11].

Zagrożenie najogólniej rozumiane jest jako brak bezpieczeństwa, przez co staje się niezmienną, nieuniknioną, a w niektórych wypadkach powszechną rzeczywistością życia ludzkiego. Jednocześnie ma ścisły związek z bezpieczeństwem. Innymi słowy bezpieczeństwo i zagrożenia są to pojęcia, które są ze sobą nierozerwalnie związane, bowiem brak bezpieczeństwa powoduje niepokój i poczucie zagrożenia. Najczęściej zjawisko zagrożenia ujmowane jest dwojako. W ujęciu subiektywnym oznacza pewien stan psychiki i świadomości, wywołany postrzeganiem zjawisk, które oceniane są jako niekorzystne lub niebezpieczne. W drugim, realnym ujęciu – akcent kładzie się na rzeczywiste czynniki powodujące ów stan niepewności i obaw[12].

Z zagrożeniem bardzo często jest utożsamiane ryzyko, które najczęściej wiąże się z możliwością pojawienia się strat, szkód w wyniku zdarzeń niepożądanych. Dlatego tak ważne jest, na każdym etapie tworzenia i modyfikacji systemu oraz przetwarzania informacji, jego szacowanie (ocena, analiza).

[9] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Wyd. AON, Warszawa 2013, s. 12.
[10] R. Wróblewski, *Wybrane problemy diagnozy bezpieczeństwa narodowego*, „Zeszyty Naukowe AON” 1991, nr 3/4, s. 69.
[11] *Leksykon wiedzy wojskowej*, red. Marian Laprus, Wyd. MON, Warszawa 1979, s. 510.
[12] K. Lidel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wyd. A. Marszałek, Toruń 2008, s. 6.

Wraz z rozwojem życia społecznego modyfikacji ulegało również rozumienie zjawiska zagrożenia. Stwierdzono, że ludzie negatywnie wartościują zarówno zjawiska godzące w przetrwanie, jak i te stanowiące wyzwanie do podjęcia określonych działań i wymagające sformułowania odpowiedzi.

Identyfikacja zagrożeń i wiedza o nich stają się zatem podstawowym warunkiem do wszczęcia działań zapobiegawczych oraz organizacji obrony. Szwajcarski politolog D. Freia, analizując subiektywne i obiektywne aspekty zagrożeń, sformułował cztery możliwe oceny stanu bezpieczeństwa:

1) stan braku bezpieczeństwa – gdy występuje rzeczywiste i istotne zagrożenie zewnętrzne, którego postrzeganie jest adekwatne;
2) stan obsesji bezpieczeństwa – gdy mało istotne zagrożenie postrzegane jest jako duże;
3) stan fałszywego bezpieczeństwa – gdy istotne zagrożenie postrzegane jest jako niewielkie;
4) stan bezpieczeństwa – gdy zagrożenie zewnętrzne jest niewielkie, a jego postrzeganie jest prawidłowe[13].

Klasyfikacje zagrożeń dla bezpieczeństwa informacji

Podobnie jak w przypadku definicji, w literaturze istnieje szereg różnego rodzaju klasyfikacji zagrożeń dla bezpieczeństwa informacji (informacyjnego). Najogólniejszy to podział ze względu na umiejscowienie źródła zagrożenia, które można podzielić na zewnętrzne i wewnętrzne.

Zewnętrzne źródła zagrożenia dzielimy na:

- wynikające z sytuacji w regionie geograficznym, położenia państwa, sojuszy, zaangażowania politycznego, militarnego i gospodarczego – zagrożenia strategiczne;
- wynikające z sytuacji w otoczeniu danej jednostki organizacyjnej.

Natomiast wewnętrzne – to w szczególności wynikające ze znaczenia jednostki organizacyjnej dla bezpieczeństwa państwa i sytuacji wewnątrz jednostki (instytucji).

[13] R. Zięba, *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych,* [*w:*] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. B. Bobrow, E. Halizak, R. Zięba, Scholar, Warszawa 1997, s. 4-5.

- Przejawy zagrożeń zewnętrznych to:
  - możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne działające w sposób profesjonalny, przemyślany i zorganizowany;
  - możliwość napadu przez pojedynczych przestępców, przypadkowe osoby wykorzystujące sprzyjające okoliczności, np. na skutek niedostatecznej ochrony;
  - klęski żywiołowe mogące uszkodzić infrastrukturę instytucji;
  - akty wandalizmu polegające na niszczeniu systemów zabezpieczeń instytucji;
  - katastrofy budowlane lub inne, które mogą uszkodzić infrastrukturę instytucji;
  - długotrwałe przerwy w dostawie elektryczności.
- Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do obiektów to:
  - wzmożone zainteresowanie osób postronnych daną instytucją, pomieszczeniami, objawiające się m.in. podejmowaniem prób uzyskania informacji o obiektach, pomieszczeniach podczas rozmów z pracownikami;
  - nawiązywanie rozmów przez osoby postronne z pracownikami na temat danej instytucji;
  - podszywanie się pod byłych pracowników instytucji i przejawianie zainteresowania tym, co się po latach zmieniło;
  - interesowanie się osobami sprawującymi określone funkcje oraz sposobem wykonywania przez nie obowiązków służbowych;
  - obserwacja sposobu funkcjonowania systemu ochronnego, sekretariatu, firm dostawczych czy usługowych (np. sprzątaczek itp.);
  - rozpoznawanie systemu zabezpieczeń, w tym stosowanych urządzeń technicznie wspomagających ochronę;
  - celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.;
  - próby pozyskania do grup przestępczych pracowników danej instytucji.
- Przejawy zagrożeń wewnętrznych to:
  - próby pozyskania dokumentów lub materiałów przez pracowników instytucji;

- próby, nielegalnego (nieuprawnionego) kopiowania oraz wglądu w dokumenty instytucji;
- nieostrożność w życiu towarzyskim, nieumiejętność dotrzymania tajemnicy – nadmierne „gadulstwo";
- byli pracownicy instytucji zwolnieni dyscyplinarnie.

P. Potejko[14] w publikacji *Bezpieczeństwo informacyjne* dokonuje klasyfikacji zagrożeń, które dzieli na: ogólne, wynikające z aspektów psychologicznych, środowiskowe i kryminalne, wynikające z nieuczciwej konkurencji i tradycyjne zagrożenia informacyjne.

Ogólne to: kradzież zasobów, niewłaściwe wykorzystywanie zasobów, bezprawne ujawnianie informacji osobom nieupoważnionym, podsłuchiwanie rozmów, projektowanie wadliwej infrastruktury informacji.

Wynikające z aspektów psychologicznych to: ludzkie błędy i pomyłki, nieuczciwi pracownicy, działania niezadowolonych pracowników, działalność intruzów komputerowych.

Środowiskowe i kryminalne: kataklizmy – ogień, woda, przestępczość – włamania, napady, wymuszanie itd.

Wynikające z nieuczciwej konkurencji: wywiadownie gospodarcze, opinie branży, weryfikacja dokumentów.

Następnie wskazuje na rodzaje i typowe przejawy zagrożeń:

- tradycyjne zagrożenia informacyjne: szpiegostwo, dezinformacja prowadzona przez obce służby w zakresie technologiczno-informatycznym, przestępstwa komputerowe, cyberterroryzm, walka informacyjna;
- zagrożenia technologiczno-informatyczne;
- zagrożenia odnoszące się do praw obywatelskich: przekazywanie informacji nieuprawnionym podmiotom, sprzedaż informacji, naruszanie przez władzę prywatności, bezprawne ingerowanie służb specjalnych, ograniczenie jawności życia publicznego;
- zagrożenia wynikające z błędnych, niewystarczających rozwiązań organizacyjnych czy strukturalnych: podjęte błędne decyzje, planowanie wadliwej infrastruktury, patologie, działania korupcyjne[15].

[14] P. Potejko, *Bezpieczeństwo informacyjne*, [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Aspra, Warszawa 2000, s. 196-197.
[15] Tamże, s. 197-198.

Natomiast P. Bączek[16] zagrożenia informacyjne dzieli na dwie grupy.

Do pierwszej zalicza: przestępstwa komputerowe, brak informacji, chaos informacyjny, cyberterroryzm, walkę informacyjną, działalność grup świadomie manipulujących przekazem informacyjnym.

Drugą grupę stanowią: niekontrolowany rozwój nowoczesnych technologii bioinformatycznnych; zagrożenia asymetryczne; szpiegostwo; nieuprawnione ujawnienie informacji (tzw. wyciek lub przeciek: pomyłkowy, polityczny, komercyjny); asymetria w międzynarodowej wymianie informacji: systemowa, w wyniku zaniedbań w polityce zagranicznej; naruszenie przez władze praw obywatelskich: ograniczenie jawności życia publicznego, wdzieranie się w życie prywatne, bezprawne ingerowanie służb specjalnych.

Według S. Kozieja zagrożenie to pośrednie lub bezpośrednie destrukcyjne oddziaływanie na podmiot. Wyróżnia on następujące typy zagrożeń: potencjalne lub realne, subiektywne i obiektywne, zewnętrzne i wewnętrzne, militarne i niemilitarne[17]. Ponadto umiejscawia zagrożenia informacyjne w grupie zagrożeń niemilitarnych wraz z zagrożeniami politycznymi, ekonomicznymi, społecznymi, ekologicznymi[18].

Zagrożenia można również podzielić z uwagi na lokalizację ich źródeł, jak dokonują tego A. Żebrowski i M. Kwiatkowski. I wówczas będą to: zagrożenia wewnętrzne, zewnętrzne i fizyczne.

Zagrożenia wewnętrzne, które powstają wewnątrz organizacji i obejmują zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu: błędu, przypadku bądź celowego działania nieuczciwych użytkowników.

Zagrożenia zewnętrzne, które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe lub przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemu.

Zagrożenia fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi występuje z powodu wypadku, awarii, katastrof lub innego

[16] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wyd. A. Marszałek, Toruń 2006, s. 177.
[17] S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011, s. 269.
[18] Tamże.

nieprzewidzianego zdarzenia wpływającego na system informacyjny bądź urządzenie sieciowe[19].

Uzupełnieniem powyższych rozważań jest stanowisko A. Żebrowskiego[20], który wskazuje, że największe zagrożenie bezpieczeństwa informacyjnego stanowi działalność człowieka. Celowe zagrożenie dla systemu bezpieczeństwa informacyjnego jest wynikiem kumulacji trzech elementów: motywu, środka realizacji włamania do owego systemu oraz okazji, czyli uzyskania dostępu do dysku komputerowego lub sieci. Człowiek może wykorzystywać różnorakie sposoby włamań do systemów informatycznych, jak np.:

- zmowę kilku sprawców;
- celowe inicjowanie awarii;
- wywoływanie fałszywych alarmów (uśpienie czujności);
- szantaż, korupcję;
- rozsyłanie do firm ankiet, zapytań, propozycji;
- rozkodowywanie hasła dostępu;
- atak słownikowy;
- podsłuch sieciowy;
- wirusy, bakterie, robaki, konie trojańskie, bomby logiczne oraz inne groźne aplikacje destabilizujące sprawność systemu;
- wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej lub serwisu informacyjnego;
- techniki obchodzenia zabezpieczeń, np. programy wykorzystujące błędy zabezpieczeń w systemach operacyjnych i oprogramowaniu użytkowym;
- przechwytywanie otwartych połączeń sieciowych.

K. Liderman z kolei podaje następujące źródła zagrożeń bezpieczeństwa informacyjnego:

- siły natury (pożary, powódzie, huragany, trzęsienia ziemi, epidemie),
- błędy ludzi i ich działania według błędnych lub niewłaściwych procedur (celowe szkodliwe działanie ludzi, awarie sprzętu komputerowego,

[19] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, OW Abrys, Kraków 2000, s. 65.
[20] Tamże, s. 63-64, 70.

oprogramowania, infrastruktury usługowej – zasilania, klimatyzacji, wody, ogrzewania)[21].

M. Pańkowska[22] odnosi się zwłaszcza do zagrożeń dla bezpieczeństwa zasobów informatycznych i dzieli te zagrożenia na zdarzenia (pożary) i przyczyny zdarzeń (np. skopiowanie informacji) powodujące straty finansowe podczas budowy i eksploatacji systemu informacyjnego. W zależności od czynnika, który je powoduje, oraz sposobu oddziaływania (bezpośredni lub pośredni), rozróżnia zagrożenia: losowe zewnętrzne, losowe wewnętrzne i intencjonalne.

- Do losowych zewnętrznych zalicza: temperaturę, wilgotność, wyładowania atmosferyczne, zanieczyszczenia powietrza, awarie systemu zasilania, klimatyzacji, instalacji wodociągowej, katastrofy budowlane, kataklizmy (trzęsienia ziemi, powodzie, pożary), zamieszki zbrojne.
- Do losowych wewnętrznych należą: błędy użytkowników, przypadkowe zagubienie lub niszczenie danych spowodowane lekkomyślnością lub przeciążeniem pracą personelu, błędy administratora bazy danych lub administratora systemu operacyjnego, wadliwa konfiguracja systemu, defekty sprzętu i oprogramowania.
- Intencjonalne dzieli na pasywne i aktywne.
  Pasywne to:
  - monitorowanie sieci dla przejęcia haseł, danych finansowych, prywatnych wiadomości;
  - podgląd (obserwacja, monitorowanie pola elektromagnetycznego, fal radiowych dla odtworzenia wizualnego informacji, które dają wgląd w przebiegające procesy i w przetwarzane dane);
  - analiza ruchu w sieci (wielkość, częstość, źródło i miejsce przeznaczenia przesyłanej informacji).

  Natomiast do aktywnych zalicza:
  - bezprawną modyfikację, ujawnienie i usuwanie informacji gospodarczej, modyfikację programów i informacji przy pomocy bomby logicznej, konia trojańskiego, wirusa i robaka komputerowego, wprowadzanie nieautoryzowanego komunikatu do sieci lokalnej lub rozległej,

[21] K. Liderman, *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012, s. 155.
[22] M. Pańkowska, *Zarządzanie zasobami informatycznymi*, Wyd. Dyfin, Warszawa 2001.

zmianę kierunku przepływu informacji, przetwarzanie maskaradę, czyli udawanie innej stacji sieci telekomunikacyjnej, nieautoryzowane pośrednictwo;

- oszustwa bankowe, fałszowanie urządzeń wejścia lub wyjścia (np. kart magnetycznych lub mikroprocesowych), oszustwa przez podawanie fałszywych danych identyfikacyjnych, oszustwa w systemach sprzedaży (np. w kasach fiskalnych);
- powielanie programów komputerowych, przechowywanie zabronionych prawem zbiorów;
- zakup i dystrybucja nielegalnymi kanałami sprzętu i oprogramowania;
- wymuszanie przerw w pracy systemu (poprzez uszkodzenie aplikacji, systemu operacyjnego, sprzętu komputerowego), przeszkodzenie innym w użyciu jakiejś szczególnej usługi, destabilizacja serwera bądź urządzeń zabezpieczających sieć;
- wykorzystywanie służbowego sprzętu do celów prywatnych, nieraz komercyjnych, kradzież komputerów i wyposażenia.

Podsumowując, występujące obecnie zagrożenia dla bezpieczeństwa informacji możemy podzielić na zagrożenia wynikające z:

1. Celowego działania, a w tym:
   - działalności służb specjalnych państw obcych[23];
   - terroryzmu;
   - nieuprawnionego i przestępczego działania ludzi, (np. kradzieży);
   - podsłuchów;
   - działania hackerów;
   - nieuprawnionego działania personelu organizacji (korupcja, szantaż, wyłudzenie);
2. Przypadkowego (lub nieświadomego) działania jednostek/struktur wynikającego z:
   - nieświadomości zagrożenia;

[23] Zob. B. Jakubus, M. Ryszkowski, *Ochrona informacji niejawnych*, Wyd. Projekt, Warszawa 2001, s. 11-23.

- nieostrożności w życiu towarzyskim (gadulstwo, alkohol, substancje odurzające);
- nierzetelnego wykonywania powierzonych obowiązków;
- nadawania uprawnień nieadekwatnych do zajmowanego stanowiska lub wykonywanych czynności;
- niedostatecznej znajomości, procedur, systemów, programów;
- nieodpowiedniego zabezpieczenia sieci i systemów teleinformatycznych;
- niewłaściwego zabezpieczenia stanowisk pracy.

3. Zagrożeń losowych:
   - katastrof naturalnych (kataklizmów, pożarów, zalań, huraganów, trzęsień ziemi itp.);
   - wypadków, np. podczas przewożenia materiałów wrażliwych, nagłej choroby (omdlenia, zasłabnięcia itp.).
4. Innych:
   - powoływania na odpowiedzialne stanowiska osób bez należytej wiedzy i doświadczenia;
   - naruszania przez organy władzy i administracji publicznej zasad prywatności;
   - słabej znajomości obowiązujących przepisów, norm, zasad, reguł;
   - niespójności (małej precyzyjności, wieloznaczności interpretacyjnej) prawa;
   - zemsty pracowników powodowanej różnymi pobudkami.

Zagrożenia asymetryczne to rodzaj zagrożeń obejmujący swoim zakresem prowadzenie walk informacyjnych i informatycznych. Manipulowanie informacją przez zorganizowane grupy przestępcze lub terrorystyczne, walka informacyjna (zdobywanie informacji przeciwnika – ochrona własnych), inflacja informacji (zbyt duży napływ niepotrzebnych informacji, z których nie można odróżnić prawdziwych od fałszywych) czy globalizacja informacji, to największe zagrożenia dla społeczeństwa. W znacznej mierze powiązane są one z władzą publiczną, polityką, biznesem oraz światem finansowym, zagrażając stabilności i pozycji międzynarodowej państwa.

Siły zbrojne zazwyczaj przodują w organizacji i wykorzystaniu technik informacyjnych. Szybki i precyzyjny dostęp do informacji pozwalają uzyskać systemy teleinformatyczne, które pozwalają również na jej przetwarzanie. Systemy

i sieci teleinformatyczne stały się zatem kolejnym polem prowadzenia działań i operacji militarnych[24].

W kontekście sił zbrojnych pojawił się nowy termin, mianowicie: wojna informacyjna. Departament Obrony USA definiuje ją jako „całokształt działań zmierzających do uzyskania przewagi informacyjnej poprzez oddziaływanie na zasób informacyjny przeciwnika, jego systemy informatyczne, przepływ i przetwarzanie informacji oraz obronę własnych zasobów i infrastruktury informacyjnej"[25].

Kolejny obszar szczególnie wrażliwy na zagrożenia informacyjne to gospodarka, która w znacznej części opiera się na informacji. Również administracja publiczna w Polsce w coraz większym stopniu wykorzystuje systemy przetwarzające informacje. Charakterystyczną cechą zagrożeń informacyjnych jest ich interdyscyplinarność[26]. Nie odnoszą się one tylko do pola walki militarnej, ale mogą dotknąć każdego mieszkańca kraju czy instytucji.

Skuteczne zabezpieczenia są kosztowne, dlatego też winny być dobrane adekwatnie do zagrożeń oraz do wartości szkód w przypadku braku ich zastosowania.

Jednym z najistotniejszych potencjalnych źródeł zagrożeń dla bezpieczeństwa organizacji jest naruszanie przepisów ochraniających te organizacje przez osoby posiadające dostęp do informacji, w tym również nieprzestrzeganie przepisów ustaw i innych regulacji w tym zakresie.

Należy podkreślić, że przedstawione powyżej klasyfikacje różnych zagrożeń nie stanowią katalogu zamkniętego. Ich liczba i różnorodność będzie ulegała rozszerzeniu o nowe, będzie się zmieniała również skala ich występowania. W związku z tym ważnym zadaniem każdej organizacji jest ciągłe monitorowanie zagrożeń zarówno wewnątrz, jak i w jej otoczeniu oraz dostosowywanie systemu zabezpieczeń do nowych wyzwań.

[24] K. Adamczyk, D. Sawicka-Nagańska, *Operacje informacyjne, wybór terminów, główne założenia*, „Myśl Wojskowa", nr 6(641), listopad–grudzień 2005, s. 47.
[25] S.A. Hildreth, *Cyberwarfare. CRS Report for Congress*, Washington 2001, s. 16.
[26] K. Baniak, *Analiza zagrożeń telekomunikacyjnych sektora publicznego*, [w:] *Bezpieczeństwo w telekomunikacji i teleinformatyce*, red. J. Strzelczyk, BBN, Warszawa 2007, s. 33.

Wybrane obszary zagrożeń. Przetwarzanie informacji w systemach i sieciach teleinformatycznych

Rozwój teleinformatyki powoduje, że systemy informatyczne organizacji mogą być zagrożone praktycznie ze strony każdego, kto posiada wystarczający zasób wiedzy i umiejętności.

Bezpieczeństwo systemu teleinformatycznego to najogólniej taki stan systemu, w którym ryzyko urzeczywistnienia się zagrożeń związanych z jego funkcjonowaniem jest ograniczone do akceptowalnego poziomu. Zapewnia się je, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności. I, co ważne, zapewnia się je przed rozpoczęciem oraz w trakcie przetwarzania informacji w systemie lub sieci teleinformatycznej.

Bezpieczeństwo systemów i sieci teleinformacyjnych to takie przedsięwzięcia, które mają na celu uniemożliwienie niepowołanym osobom dostępu do zasobów informacyjnych, do których można dotrzeć poprzez przechwycenie emisji radiowych, analizę ruchu w sieciach radiowych lub wprowadzanie w błąd tych, którzy taką analizę mogą prowadzić. Natomiast bezpieczeństwo systemów łączności obejmuje systemy transmisji, bezpieczeństwo środków utrudniających oraz środków mających na celu fizyczną ochronę systemów łączności, materiałów i informacji związanych z systemami łączności[27]. Istotne jest ograniczenie możliwości nieuprawnionego dostępu do przechowywanych, przetwarzanych i przesyłanych informacji bez oddziaływania na system oraz ograniczenie możliwości nieuprawnionego oddziaływania na systemy, które może spowodować zmiany funkcjonowania sieci teleinformacyjnej, dostępu do przesyłanych, przetwarzanych i przechowywanych informacji; dezinformację; zniszczenie informacji; sfałszowanie lub nieuprawnioną modyfikację informacji[28].

Niezmiernie ważnym dla organizacji publicznych jest zapewnienie odpowiedniej ochrony takich procesów, jak: gromadzenie, przetwarzanie i udostępnianie danych wyłącznie uprawnionym osobom, co wynika z zajmowanych

[27] M. Herman, *Potęga wywiadu*, Bellona, Warszawa 2002, s. 170.

[28] A. Barczyk, T. Sydoruk, *Bezpieczeństwo systemów informacyjnych zarządzania*, Bellona, Warszawa 2003, s. 70.

stanowisk pracy i przypisanych im zadań. Często natomiast można zauważyć naklejone na monitory kartki z hasłami dostępu, bałagan na biurku, pozostawianie bez nadzoru dokumentów, wyrzucanie do kosza korespondencji z istotnymi dla organizacji informacjami, gubienie nośników informacji, które to zachowania wynikają z braku wiedzy i nieświadomości użytkowników[29]. Kolejną sytuacją powodującą zagrożenie bezpieczeństwa informacyjnego jest przesyłanie poufnych informacji pocztą elektroniczną w sposób niechroniony, nawet wtedy, gdy pracownik posiada dostęp do chronionego systemu poczty[30].

Systemy teleinformatyczne, stanowiąc obecnie najważniejszy element w zakresie przechowywania, przesyłania i przetwarzania informacji, są narażone na liczne zagrożenia. Wśród nich można wyróżnić dwie główne grupy:

- zagrożenia dla informacji przechowywanych w systemach teleinformatycznych;
- zagrożenia dla infrastruktury teleinformatycznej.

Do pierwszej grupy należą m.in.: przechwyt, zniszczenie, modyfikacja i utrudnienie (uniemożliwiające) dostęp do informacji. Działania takie mogą przybierać różne formy, do których zalicza się włamanie do sieci lub jej elektroniczny podsłuch, złamanie zabezpieczeń, bombardowanie serwera danych (jednoczesne i wielokrotne próby połączenia z serwerem danych przez dużą liczbę komputerów użytkowników nieuprawnionych do uzyskania danych, co prowadzi do tego, że legalny uczestnik nie będzie miał możliwości połączenia się z serwerem).

Do drugiej grupy zagrożeń należą fizyczne zniszczenie lub uszkodzenie urządzeń wchodzących w skład systemów teleinformatycznych, obezwładnienie ich obsługi i zabezpieczeń (np. atak terrorystyczny).

Instalowanie nielegalnego oprogramowania, przekraczanie uprawnień przez pracowników administracji, popełnianie błędów wskutek niedbalstwa użytkowników, włamanie hackerów czy kradzież kluczy kryptograficznych – to tylko niektóre zagrożenia, na które narażone są systemy teleinformatyczne, a w nich poufne dane, informacje wrażliwe oraz wszelkie informacje ważne zarówno dla pojedynczego użytkownika, jak i instytucji czy to prywatnych, czy państwowych.

[29] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Wyd. AON, Warszawa 2010, s. 6.
[30] R.J. Sutton, *Bezpieczeństwo telekomunikacji*, WKŁ, Warszawa 2004, s. 17.

Dostępność mobilnych urządzeń zewnętrznych w pracy, przetwarzanie w chmurze czy nieświadomość pracowników oraz korzystanie z portali społecznościowych, to niektóre z przyczyn utraty danych przez większość firm.

Zagrożenia cyberprzestrzeni

Kolejną sferą działalności ludzkiej, wciąż zyskującą na znaczeniu i wymagającą ochrony i obrony, jest cyberprzestrzeń. „Oprócz pozytywnych aspektów wykorzystywania cyberprzestrzeni istnieją także negatywne formy ludzkiej działalności, a mianowicie, podobnie jak w normalnej przestrzeni, tak i tu dochodzi do popełniania przestępstw czy też aktów cyberterroryzmu, a nawet wykorzystywania tej przestrzeni przez różne państwa do nielegalnej działalności lub agresji przeciwko innym podmiotom[31].

Cyberprzestrzeń można określić jako pewnego rodzaju przestrzeń komunikacyjną, która jest tworzona dzięki systemowi powiązań internetowych. Zauważyć należy, że cyberprzestrzeń stanowi obszar kooperacji o charakterze pozytywnym, co doprowadzić może do rozwijania się sfery edukacyjnej, komunikowania się społecznego, gospodarki narodowej, jak również innych sfer. Jest ona również obszarem kooperacji o charakterze negatywnym. Taki rodzaj aktywności może przejawiać się pod czterema postaciami, a mianowicie[32]:

- cyberinwigilacji polegającej na zaostrzonej kontroli społeczeństwa przy wykorzystaniu narzędzi teleinformatycznych w krajach o ustroju autorytarnym i totalitarnym;
- cyberprzestępczości, która przejawiać się może w wykorzystaniu cyberprzestrzeni do celów kryminalnych, szczególnie w odniesieniu do przestępczości zorganizowanej i mającej charakter ekonomiczny;
- cyberterroryzmu, który polega na wykorzystywaniu cyberprzestrzeni do prowadzenia działań terrorystycznych;
- cyberwojny polegającej na wykorzystaniu cyberprzestrzeni jako czwartego (poza ziemią, morzem i powietrzem) wymiaru do prowadzenia działań o charakterze wojennym.

[31] S. Bąbas, P. Kowalski, *Bezpieczeństwo w warunkach zmian społecznych, cywilizacyjnych i kulturowych*, Wyższa Szkoła Handlowa im. Króla Stefana Batorego, Piotrków Trybunalski 2014, s. 436.
[32] P. Sienkiewicz, *Terroryzm w cyberprzestrzeni*, Warszawa 2009, s. 71.

Z cyberprzestrzenią związana jest cyberprzestępczość, którą nazywa się także przestępczością internetową. Pod tym pojęciem kryją się zabronione prawnie działania, które dokonywane są przy pomocy komputerów w sieci internetowej albo przy pomocy technologii informatycznych. Termin ten został unormowany zarówno w naukach prawnych, jak i w dziedzinie zajmującej się bezpieczeństwem teleinformatycznym. Można przyjąć, że cyberprzestępczość odnosi się do trzech kategorii przestępstw, a mianowicie[33]:

- przestępstw o charakterze tradycyjnym, które popełniane są z wykorzystaniem sieci oraz systemów informatycznych;
- publikowania nielegalnych treści;
- pozostałych przestępstw typowych dla sieci elektronicznej.

Zgodnie z D.E. Denning „cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanym w nich, by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien on skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczające szkody, by stwarzać strach”[34].

Istnieje możliwość wyróżnienia obszarów w szczególności narażonych na ataki cyberterrorystyczne. Wskazać należy na[35]:

- systemy wojskowe – przechowujące informacje na temat położenia satelitów, rozlokowania wojsk i sprzętu, dane dotyczące prowadzonych badań nad nowymi typami broni czy też nowoczesnymi systemami wykorzystywanymi do łączności i komunikacji; liczba ataków na tego rodzaju systemy zauważalna była zwłaszcza podczas trwania zimnej wojny, a ich sprawcami byli agenci innych wywiadów;
- systemy przedsiębiorstw – magazynujące dane ważne z punktu widzenia prowadzenia działalności przez daną firmę; zaliczyć do nich należy np. informacje na temat rezerwacji, klientów, technologii, z których przedsiębiorstwo korzysta; atakami na tego rodzaju infrastrukturę mogą

[33] W. Filipowski, *Internet – przestępcza gałąź gospodarki*, „Prokuratura” 2007, nr 1, s. 79.
[34] J. Kisielnicki, *MIS. Systemy informatyczne zarządzania*, Placet, Warszawa 2008, s. 121.
[35] M. Jędrzejewski, *Analiza systemowa zjawiska infoterroryzmu*, Wyd. AON, Warszawa 2002, s. 32.

zajmować się pracownicy albo byli pracownicy współpracujący z konkurencją lub też chcący dokonać zemsty na byłym pracodawcy;

- systemy tworzące infrastrukturę krytyczną państwa – do infrastruktury krytycznej państwa zalicza się te systemy, które odnoszą się do funkcjonowania całego państwa, np. systemy bankowo-finansowe, energetyczne, telekomunikacyjne, dostarczania wody, transportu, system służb podejmujących działania w sytuacjach wyjątkowych; w tego rodzaju systemach gromadzone są dane, które są istotne z punktu widzenia bezpieczeństwa całego kraju; ataki na systemy infrastruktury krytycznej państwa są najczęściej dokonywane przez pracowników takich systemów, ale również przez terrorystów.

Cyberkonflikty to konflikty cybernetyczne, działania prowadzone w sieciach komputerowych. Ich celem jest uszkodzenie fizycznych elementów infrastruktury państwa (szczególnie narażona jest tutaj infrastruktura krytyczna). Cyberprzestępczość jest zjawiskiem zagrażającym dobru chronionemu prawem, które może okazać się groźne zarówno dla osób fizycznych, jak i dla całej infrastruktury publicznej, charakteryzując się efektywnością i szerokim spektrum działań cyberprzestępców[36].

Jednakże najgroźniejszym zjawiskiem w cyberprzestrzeni jest aktualnie cyberterroryzm, czyli działania: mające na celu próbę ataku lub atak na sieci, systemy informacyjne; powodujące zniszczenie infrastruktury państwa bądź też próby zastraszenia poszczególnych rządów i społeczeństw; wykorzystujące zdobycze technologii informacyjnej wyrządzającej szkody. Najczęściej atakowane są rządowe strony internetowe, infrastruktura bankowa oraz infrastruktura krytyczna.

Można wyróżnić dwa rodzaje ataków cyberterrorystycznych, przy czym jest możliwość ich wzajemnego uzupełniania się, jak również mogą one stanowić samodzielną akcję albo część większej kampanii, a są to[37]: atak, który ma miejsce w cyberprzestrzeni, atak fizyczny na systemy informacyjne.

[36] M. Wódka, *Wyzwania dla bezpieczeństwa informacyjnego w Polsce i Unii Europejskiej*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Pracownia Wydawnicza WH UPH, Siedlce-Warszawa 2016, s. 168.
[37] Tamże, s. 11.

Bez względu na rodzaj cyberataki mogą powodować zachwianie stabilności gospodarki kraju, a nawet całego świata. W odniesieniu do ataku fizycznego – terroryści w obrębie cyberprzestrzeni przeprowadzają działania, które ułatwiają lub pozorują uderzenie w rzeczywistym świecie. W takim przypadku nie jest konieczne posiadanie wiedzy informatycznej, ponieważ możliwe jest użycie tradycyjnych środków, do których zalicza się materiały wybuchowe. Ważne jest posiadanie wiedzy na temat tego, w które miejsce może być skierowane uderzenie.

Działania cyberprzestępcze mogą wywierać istotny wpływ na bezpieczeństwo państwa, jego struktur oraz społeczeństwa. Do takich zagrożeń w tym obszarze możemy zaliczyć m.in.: hacking komputerowy, podsłuch, sabotaż, szpiegostwo przemysłowe i polityczne, bezprawne niszczenie informacji, fałszerstwo, oszustwo, kradzież danych, blokowanie dostępu do usług. Cyberprzestępstwa przynoszą grupom przestępczym ogromne zyski zmniejszające dochody przedsiębiorstw, które w nieodpowiedni sposób chronią swoje dane (np. ze względów oszczędnościowych).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej stanowi, że jednym z priorytetów jest „zapewnienie bezpieczeństwa funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni. „Szczególnie ważna jest: współpraca i koordynacja działań ochronnych z przedmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej – prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni; wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie; rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców; prowadzenie walki informacyjnej w cyberprzestrzeni; współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych”[38].

[38] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 24-35.

Infrastruktura krytyczna

Z punktu widzenia cyberterroryzmu najskuteczniejsze są ataki przeprowadzane na systemy należące do infrastruktury krytycznej państwa. Wynika to z faktu, że tego rodzaju ataki powodują najdotkliwsze skutki, co z kolei jest celem działania terrorystów. Dążą oni do osiągnięcia jak najszerszych negatywnych skutków, które dotkną możliwie jak największą liczbę ludności cywilnej. Badacze tematu twierdzą, że już pojawienie się symptomów wystąpienia ataku cyberterrorystycznego powoduje uruchomienie procedur, jakie są niezbędne do zapobieżenia takiemu atakowi. W związku z tym należy zdefiniować potencjalne cele, które są narażone na ataki w pierwszej kolejności[39].

Ustawa o zarządzaniu kryzysowym[40] stanowi, że należy przez to rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa;
- łączności;
- sieci teleinformatycznych;
- finansowe;
- zaopatrzenia w żywność;
- zaopatrzenia w wodę;
- ochrony zdrowia;
- transportowe;
- ratownicze;
- zapewniające ciągłość działania administracji publicznej;
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

[39] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa we współczesnym świecie*, Aspra, Warszawa 2003, s. 79.
[40] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. Nr 89, poz. 590 ze zm.).

Ze statystyk na temat ochrony infrastruktury krytycznej Stanów Zjednoczonych wynika, że podmioty działające w sieci zlokalizowanej na terenie Arabii Saudyjskiej, Indonezji i Pakistanu podejmowały wielokrotne próby sprawdzania systemów amerykańskich zabezpieczeń sieci komunikacyjnych i systemów alarmowych, jak również sieci energetycznych, wodociągów i elektrowni atomowych. Pokazuje to, że ochrona infrastruktury krytycznej każdego państwa powinna być priorytetem działań związanych z bezpieczeństwem całego państwa. W czasach cyfryzacji bezpieczeństwo cybernetyczne stanowi ważny aspekt funkcjonowania każdego kraju.

Zwykle mówi się o atakach na węzły telekomunikacyjne, teleinformatyczne oraz informacyjne – zaburzenie ich funkcjonowania ma na celu wywołanie w społeczeństwie rozruchów, paniki, strachu, lęku, dezintegracji, poczucia niepewności i zagrożenia.

Do krytycznej infrastruktury telekomunikacyjnej zakwalifikowano w szczególności:

- systemy i sieci telekomunikacyjne obsługujące określony region (państwo, mniejsze jednostki terytorialne);
- sieci teleinformatyczne, telekomunikacyjne, które są niezbędne do prawidłowego, statutowego wykonywania zadań przez organy administracji publicznej (rządowej i samorządowej);
- sieci teleinformatyczne, telekomunikacyjne służące wymianie danych w siłach zbrojnych;
- rejestry państwowe w warstwie aplikacyjnej[41].

Natomiast w kwestii infrastruktury teleinformatycznej na działanie ataków cyberterrorystycznych są szczególnie narażone:

- stacje bazowe i satelitarne;
- miejsca przebiegu telekomunikacyjnych linii międzycentralowych oraz elementarnych linii komunikacyjnych;
- różne obiekty telekomunikacyjne, np. stacje czołowe, węzły dostępowe, wyniesione koncentratory itp.;
- centrale telekomunikacyjne obsługujące instytucje państwowe, urzędy oraz organizacje, których zadaniem jest likwidacja wszelakich zagrożeń;

[41] Tamże, s. 28.

- miejsca posiadające serwery zarządzające danymi, systemami i kluczowymi bazami wykorzystywanymi przez administrację publiczną (PESEL, Regon, CEPIK, Kataster, rejestry sądowe, rejestry państwowe i in.);
- centra zarządzania i utrzymania infrastruktury telekomunikacyjnej[42].

Jak wynika z powyższego zestawienia, na ataki cyberterrorystyczne są najczęściej narażone systemy komputerowe wykorzystywane przez instytucje państwowe, których sprawne funkcjonowanie ma ogromne znaczenie dla porządku publicznego oraz codziennego życia obywateli. Obszary zainteresowania cyberprzestępców nie są wybierane przypadkowo, gdyż – uderzając w infrastrukturę państwową – wyrządzają szkodę wszystkim członkom społeczeństw, którzy z owej infrastruktury korzystają. Z tego powodu tak istotna jest ochrona owej infrastruktury przed destrukcyjnym wpływem cyberterrorystów.

Ochrona infrastruktury krytycznej to zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtwarzania infrastruktury krytycznej na wypadek zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Prawną podstawę tych działań stanowi ustawa o zarządzaniu kryzysowym, która wraz z rozporządzeniami wykonawczymi Rady Ministrów określającymi: sposób realizacji obowiązków i współpracy w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK)[43], strukturę, sposób tworzenia oraz aktualizowania planów ochrony infrastruktury krytycznej[44], dostarcza formalnych narzędzi do identyfikacji infrastruktury krytycznej i stworzenia warunków do poprawy jej bezpieczeństwa. Wymienione przepisy prawa zdefiniowały podstawowe obowiązki podmiotów zaangażowanych w ochronę infrastruktury krytycznej oraz relacje pomiędzy nimi w ramach współpracy w realizacji NPOIK i przygotowania planów ochrony infrastruktury krytycznej.

[42] Tamże.

[43] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. Nr 83, poz. 541).

[44] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. Nr 83, poz. 542).

Zagrożenia ze strony obcych służb specjalnych

Bezpieczeństwo informacji zależy przede wszystkim od jakości ich ochrony. Jednakże należy mieć świadomość, że zapewnienie nawet najwyższego poziomu bezpieczeństwa nie zlikwiduje zagrożeń, jakie stwarzają obce służby specjalne i organizacje terrorystyczne. Dlatego też jednym z kluczowych zadań ustawowych, jakie należy uwzględnić w systemie ochrony informacji niejawnych, jest rozpoznawanie zagrożeń wywiadowczych i terrorystycznych.

Szczególnym zagrożeniem informacyjnym dotyczącym bezpieczeństwa państwa jest szpiegostwo. Zasługuje ono na wyjątkowe potraktowanie chociażby z dwóch względów, tj. trudności w jego wykrywaniu oraz szkód, jakie mogą powstać w zakresie bezpieczeństwa państwa.

Szpiegostwo, w ujęciu leksykalnym, oznacza działanie przestępcze dokonywane na szkodę określonego państwa, polegające na podjęciu pracy na rzecz obcego wywiadu, a zwłaszcza na zbieraniu i przekazywaniu informacji obcemu wywiadowi lub na ich gromadzeniu i przechowywaniu w celu przekazania obcemu wywiadowi. Natomiast szpiegiem jest osoba zdobywająca i przekazująca obcemu państwu informacje stanowiące tajemnicę państwową lub wojskową[45].

Służby wywiadowcze każdego państwa najczęściej swoją uwagę koncentrują na siłach zbrojnych innego państwa. Ma to swoje uzasadnienie, gdyż na ogół to wojsko jako pierwsze wykorzystuje wszelkiego rodzaju innowacje i zdobycze naukowo-techniczne. No i oczywiście stanowi najistotniejszy element systemu obrony i bezpieczeństwa państwa. Z tego też względu właśnie w wojsku przetwarza się najwięcej informacji niejawnych, tych najistotniejszych z punktu widzenia obronności państwa.

Ze względu na obszary zainteresowań możemy mówić o wywiadzie wojskowym, ekonomicznym, politycznym (tu mieści się terroryzm), naukowym, komputerowym (elektronicznym).

- Szpiegostwo wchodzi w skład działań wywiadowczych, którymi zajmują się służby informacyjne, a do ich zadań należy:
  - rozpoznawanie potencjałów gospodarczych i obronnych oraz administracji i szczebli decyzyjnych innych państw;

[45] P. Thiem, *Ochrona informacji niejawnych. Materiały do szkolenia pracowników*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2003, s. 10.

- zbieranie danych o istotnych osobach i instytucjach;
- organizowanie aktów dywersji, werbowanie agentów, manipulowanie informacyjne i wprowadzenie potencjalnego obiektu działań w błąd;
- ochrona własnego państwa i jego podmiotów przed oddziaływaniem informacyjnym przeciwnika.

Kolejnym wyzwaniem, z którym muszą się zmierzyć poszczególne państwa, jest wykorzystywanie Internetu do celów wywiadowczych, a zwłaszcza szpiegostwa gospodarczego. Stosowanie różnego rodzaju urządzeń podsłuchowych oraz rejestratorów obrazu przez niepowołane do tego osoby stało się zjawiskiem zagrażającym zarówno firmom prywatnym, jak i instytucjom państwowym. Szczególną aktywność w tym zakresie przejawia tzw. szpiegostwo korporacyjne.

Wywiad jest instytucją, wychodzącą z działaniami na zewnątrz, której celem jest uzyskiwanie informacji dla kierowniczych organów państwa, danej struktury, która nim kieruje.

- Swoje cele wywiad realizuje poprzez:
  - tzw. „biały wywiad" – informacje zdobywane przez analizę oficjalnych dokumentów (prasy, radia, telewizji, wydawnictw książkowych, Internetu, biuletynów wewnętrznych, jawnych dokumentów, zwłaszcza rządowych, sądowych
    i innych rejestrów urzędowych, dokumentacji technicznej, patentowej, wyników badań opinii społecznej itd.) są zasadniczym źródłem pozyskiwania wiedzy, wynika z tego szczególna ranga właściwej ochrony informacji, zwłaszcza wrażliwych;
  - agenturę – sieć osób tajnie współpracujących ze służbą wywiadu, których celem jest zdobywanie, potwierdzanie i pogłębianie informacji;
  - środki techniczne – podsłuch telefoniczny, zewnętrzny podsłuch obiektu, podgląd (filmowanie i fotografowanie), kontrola korespondencji, tajna rewizja, włamania do sieci komputerowej itp.

- Zainteresowania wywiadu koncentrują się głównie na:
  - ośrodkach decyzyjnych (poprzez pozyskiwanie informacji i plasowanie tzw. agentury wpływu);
  - węzłach informacyjnych (poprzez przejęcie informacji i możliwość jej deformacji);

- ośrodkach (organach) opiniotwórczych, obiektach militarnych, strategicznych i wrażliwych dla danego systemu;
- obiektach i służbach specjalnych;
- siłach zbrojnych.

- Wywiad w szczególny sposób interesuje się osobami, instytucjami, obiektami, które:
  - posiadają dostęp do ważnych informacji (np. planów mobilizacyjnych, operacyjnych, programów naukowo-badawczych, strategicznych przedsięwzięć gospodarczych) lub ze względu na możliwości (np. przebieg kariery zawodowej, posiadane wpływy, rangę polityczną itp.), że w przyszłości mogą być wpływowe ze względu na pełnienie służby czy pracy w ważnych instytucjach;
  - ze względu na możliwości mogą oddziaływać na kreowanie sprzyjających sytuacji;
  - mogą być wykorzystane w procesie tworzenia bazy do działania;
  - mogą być wykorzystane do konkretnych – ważnych przedsięwzięć wywiadowczych;
  - obiekty, na które ukierunkowane jest działanie wywiadowcze – zgodne z celem działania[46].

- Zagrożenia wywiadowcze, terrorystyczne oraz ze strony przestępczości zorganizowanej (metody działania) to:
  - wykorzystywanie najsłabszych elementów w systemie ochrony (państwa, jednostki organizacyjnej, instytucji, obiektu);
  - maskowanie działalności – praca z pozycji innego państwa, organizacji międzynarodowych, ukrywanie celu działania;
  - wykorzystywanie różnic ideologicznych, religijnych, społecznych – głównie dysproporcji w stopie życia ludności (materialne dobra).

W celu zabezpieczenia się przed szpiegostwem w strukturach państwowych tworzone są służby specjalne (tzw. kontrwywiad) zajmujące się rozpoznawaniem obcych wywiadów, ochroną własnych tajemnic państwowych,

[46] B. Jakubus, M. Ryszkowski, dz. cyt., s. 11-17.

zwalczaniem dywersji, sabotażu i innych zagrożeń związanych z działalnością zagranicznych służb.

Trudno precyzyjnie wskazać, które elementy systemu politycznego i obszary działalności społecznej są w kręgu zainteresowania służb specjalnych. Natomiast można to uczynić w stosunku do metod oraz sposobów ich prowadzenia, gdyż są one podobne do wykorzystywanych przez inne służby wywiadowcze na świecie.

Zasoby te składają się z następujących elementów:

- „akredytowany personel dyplomatyczny w Polsce, w tym rezydenci wywiadu funkcjonujący w ambasadach;
- pracownicy służb specjalnych wykonujący zadania wywiadowcze pod przykryciem różnych podmiotów gospodarczych, stowarzyszeń i fundacji;
- przypuszcza się, że dogodnym miejscem prowadzenia tej działalności są regiony graniczące z Rzeczpospolitą, a szczególnie Obwód Kaliningradzki.

Prowadzenie tego typu działań pokazuje m.in. fakt wydalenia w 2000 r. dziewięciu dyplomatów rosyjskich za prowadzenie działań niezgodnych ze statutem dyplomaty (szpiegostwo)”[47].

Przeciwdziałanie zagrożeniom

Bezpieczeństwo informacji jest to dziedzina, której znaczenie w ostatnim czasie gwałtownie rośnie. Jest to jednocześnie dziedzina tak stara, jak sam człowiek, który od zarania swojego istnienia był skazany na zdobywanie informacji (np. na temat tego, gdzie znajdują się zasoby pożywienia i wody), jej ocenę (np. czy członek plemienia, który podał taką informację, jest wiarygodny i czy ta informacja może być przydatna) oraz jej ochronę (np. przez tworzenie kręgów „wtajemniczonych” wojowników, szamanów, jej utrwalanie, najpierw w przekazach ustnych, a potem pisemnych). Zatem informacja i działania mające na celu jej wykorzystanie i ochronę towarzyszyły człowiekowi od zawsze, ale w ostatnich latach wraz z szybszym rozwojem techniki i związanymi z tym zmianami cywilizacyjnymi, nabrały szczególnego znaczenia.

[47] M. Minkina, M. Niedbała, *Zagrożenia wywiadowcze dla Rzeczypospolitej Polskiej*, [w:] *Postęp w inżynierii bezpieczeństwa*, red. K.A. Skibniewska, M. Lutostański, Wyd. UWM, Olsztyn 2015, s. 46.

Każde demokratyczne państwo dbając o własne bezpieczeństwo, a więc i bezpieczeństwo obywateli, chroni swoje tajemnice, szanuje prywatność życia i zapewnia ochronę tajemnic zawodowych oraz handlowych[48]. Demokratyzacja życia społecznego wymusza istnienie określonego zasobu informacji objętego szczególną ochroną i – w konsekwencji – dostępnego wyłącznie ściśle określonemu gronu osób, które zostało upoważnione do ich posiadania. Ochrona takich informacji jest jednym z podstawowych zadań państwa i jego wyspecjalizowanych agend. Funkcjonowanie państwa, a więc i jego życia społecznego, nie jest możliwe bez utrzymania w tajemnicy określonych informacji dotyczących jego strategii działania, obrotu gospodarczego, działalności zawodowej osób oraz ich życia prywatnego.

Znaczenie ochrony informacji znalazło odzwierciedlenie m.in. w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2014 r., w której stwierdzono, że: „bezpieczeństwo informacyjne, w tym ochrona informacji niejawnych, to jeden z najważniejszych obszarów funkcjonowania systemu bezpieczeństwa państwa.

Strategiczne zadania w tym zakresie obejmują: zapewnienie bezpieczeństwa informacyjnego państwa poprzez zapobieganie uzyskaniu nieuprawnionego dostępu do informacji niejawnych i ich ujawnieniu; zapewnienie personalnego, technicznego i fizycznego bezpieczeństwa informacji niejawnych; akredytację systemów teleinformatycznych służących przetwarzaniu tych informacji; zapewnienie realizacji funkcji krajowej władzy bezpieczeństwa w celu umożliwienia międzynarodowej wymiany informacji”[49]. „Ważnym zadaniem jest też ciągłe dostosowywanie rozwiązań prawnych, proceduralnych, fizycznych i technicznych do pojawiających się zagrożeń dla przechowywania, przetwarzania i wymiany informacji niejawnych. W tym kontekście istotne znaczenie dla ochrony systemów teleinformatycznych ma rozwój i implementacja narodowych rozwiązań kryptografii”[50].

Zapewnienie bezpieczeństwa informacji jest procesem złożonym i uzależnionym od szeregu czynników, tj.: od umiejętnego zarządzania bezpieczeństwem poszczególnych rodzajów informacji, poziomu świadomości pracowników

[48] M. Polok, *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, WP LexisNexis, Warszawa 2006, s. 10.
[49] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 35.
[50] Tamże, s. 50.

dopuszczonych do przetwarzania informacji oraz odpowiednio dobranych rozwiązań organizacyjno-technicznych. Należy również mieć świadomość, że bezpieczeństwo jest procesem ciągłym, w związku z tym należy udoskonalać mechanizmy zapewniające skuteczną ochronę bezpieczeństwu informacyjnemu.

Szczególnie w ostatnich latach obserwujemy zagrożenia, które nabierają szczególnego i coraz większego znaczenia i związane są z rozwojem techniki. Można zatem postawić tezę, że w przyszłości zagrożenia informacyjne będą miały zasadnicze znaczenie dla bezpieczeństwa państwa i społeczeństwa. Ranga zagrożeń informacyjnych będzie wzrastała wraz ze wzrostem zastosowań dla technik informatycznych.

Na każdym poziomie zarządzania bezpieczeństwem informacji zasadniczym celem jest niedopuszczenie do ich utraty, ujawnienia czy modyfikacji. Należy mieć również na uwadze, aby przyjęte rozwiązania organizacyjno-prawne nie utrudniały czy wręcz uniemożliwiały przepływu informacji.

Zasadniczym elementem niedopuszczenia do przeistoczenia się zagrożeń w niebezpieczeństwo jest właściwa diagnoza zagrożeń. Niski poziom świadomości tych zagrożeń oraz słabe przygotowanie ochronne i obronne społeczeństwa może wykorzystać potencjalny przeciwnik poprzez nieuprawnione korzystanie z dostępu do informacji. Ponadto ochrona informacji i ochrona przed zagrożeniami, o których wiedza jest niepełna, nie będzie skuteczną.

Zatem informacje podlegające ochronie winny być udostępnione wyłącznie osobie uprawnionej, zgodnie z obowiązującymi przepisami i wymogami w tym zakresie. Muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie. Muszą być odpowiednio chronione, z zastosowaniem środków bezpieczeństwa osobowego, fizycznego i technicznego.

Bibliografia

Adamczyk K., Sawicka-Nagańska D., *Operacje informacyjne, wybór terminów, główne założenia*, „Myśl Wojskowa", nr 6 (641), listopad-grudzień 2005.

Bania K., *Analiza zagrożeń telekomunikacyjnych sektora publicznego,* [w:] *Bezpieczeństwo w telekomunikacji i teleinformatyce*, red. J. Strzelczyk, BBN, Warszawa 2007.

Barczyk A., Sydoruk T., *Bezpieczeństwo systemów informacyjnych zarządzania*, Bellona, Warszawa 2003.

Bąbas S., Kowalski P., *Bezpieczeństwo w warunkach zmian społecznych, cywilizacyjnych i kulturowych*, Wyższa Szkoła Handlowa im. Króla Stefana Batorego, Piotrków Trybunalski 2014.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego,* Wyd. A. Marszałek, Toruń 2006.

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa we współczesnym świecie*, Aspra, Warszawa 2003.

Filipowski W., *Internet – przestępcza gałąź gospodarki*, „Prokuratura" 2007, nr 1.

Herman M., *Potęga wywiadu*, Bellona, Warszawa 2002.

Hildreth S.A., *Cyberwarfare. CRS Report for Congress*, Washington 2001.

Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Wyd. AON, Warszawa 2013.

Jakubus B., Ryszkowski M., *Ochrona informacji niejawnych*, Wyd. Projekt, Warszawa 2001.

Jędrzejewski M., *Analiza systemowa zjawiska infoterroryzmu*, Wyd. AON, Warszawa 2002.

Kaufmann F.X., *Koncepcja socjologii religii*, ZW Nomos, Kraków 2006.

Kisielnicki J., *MIS. Systemy informatyczne zarządzania*, Placet, Warszawa 2008

Korycki S., *System bezpieczeństwa Polski*, Wyd. AON, Warszawa 1994.

Koziej S., *Teoria sztuki wojennej*, Bellona, Warszawa 2011.

Leksykon wiedzy wojskowej, red. Marian Laprus, Wyd. MON, Warszawa 1979.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wyd. A. Marszałek, Toruń 2008.

Liedel K., *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej*, [w:] *Bezpieczeństwo XXI wieku. Asymetryczny świat*, red. K. Liedel, P. Piasecki, T.R. Aleksandrowicz, Difin, Warszawa 2011.

Liderman K., *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012.

Minkina M., Niedbała M., *Zagrożenia wywiadowcze dla Rzeczypospolitej Polskiej*, [w:] *Postęp w inżynierii bezpieczeństwa*, red. K.A. Skibniewska, M. Lutostański, Wyd. UWM, Olsztyn 2015.

Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, Wyd. AON, Warszawa 2010.

Pańkowska M., *Zarządzanie zasobami informatycznymi*, Difin, Warszawa 2001.

Polok M., *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, WP LexisNexis, Warszawa 2006.

Potejko P., *Bezpieczeństwo informacyjne,* [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Aspra, Warszawa 2000.

Sienkiewicz P., *Bezpieczeństwo informacji – wspólne dobro dla racji stanu, bezpieczeństwa i obronności kraju, firm i obywateli*, [w:] *Ochrona informacji niejawnych i biznesowych*, Materiały IV Kongresu, Katowice 2008.

Sienkiewicz P., *Terroryzm w cyberprzestrzeni*, Warszawa 2009.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Sutton R.J., *Bezpieczeństwo telekomunikacji*, WKŁ, Warszawa 2004.

Thiem P., *Ochrona informacji niejawnych. Materiały do szkolenia pracowników*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2003.

Wróblewski R., *Wybrane problemy diagnozy bezpieczeństwa narodowego*, „Zeszyty Naukowe AON" 1991, nr 3/4.

Zięba R., *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych,* [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. B. Bobrow, E. Halizak, R. Zięba, Scholar, Warszawa 1997.

Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Abrys, Kraków 2000.

Information security threats

Summary: Since the dawn of time, information has been an important element in ensuring security and development for both individuals and the state. Recently, its role and importance has been growing rapidly. It takes the form of not only data, but also knowledge and skills. Nowadays, the vast majority of countries with entities of social life and organizations depend on access to information that determines their development and position on the market. Additionally, the vast majority of citizens owns, disposes and processes messages, information, materials (documents), which, for various reasons, should not be generally available. This applies to information resulting from the nature of work as well as the broadly understood private sphere (correspondence, banks, offices, schools, universities, health care facilities, etc.). Due to its role and importance, it is exposed to many different threats. Therefore, the most important task and responsibility of the government and its specialized services in this field is to protect this information. It can be ensured by a properly organized and efficiently functioning system, which will guarantee restrictions on the access of persons, especially to sensitive information, on its proper processing, as well as the use of appropriate and sufficient physical and ICT security measures.
Keywords: *information, threats, prevention, security*