WPROWADZENIE

Współcześnie informacja stała się nadrzędnym celem pozyskiwania wszelkich danych przez osoby stosujące nielegalne praktyki dla intratnych zysków, sposobów przejęcia władzy czy też osłabienia bezpieczeństwa narodowego. Niezależnie od tego, jaką formę przybiera informacja lub za pomocą jakich środków jest udostępniana lub przechowywana, zaleca się, aby zawsze była w odpowiedni sposób chroniona. Bezpieczeństwo systemu informacyjnego jest ważne zarówno dla sektora publicznego, jak i prywatnego, służąc ochronie infrastruktury krytycznej. W obu sektorach bezpieczeństwo systemu informacyjnego może funkcjonować jako dźwignia biznesu, np. umożliwiając wprowadzenie e-rządu lub e-gospodarki oraz unikanie lub redukowanie odpowiednich ryzyk. Wzajemne przenikanie się sieci publicznych i prywatnych oraz współużytkowanie zasobów informacyjnych utrudnia utrzymanie kontroli dostępu. Tendencja wprowadzania rozproszonego przetwarzania także osłabia skuteczność centralnych, specjalizowanych mechanizmów zarządzania[1].

Bezpieczeństwo systemu informacyjnego w erze globalizmu informacji jest nieustannym obiektem cyberataków, stąd wymaga nie tylko odpowiedniego systemu zabezpieczeń poprzez system teleinformatyczny, ale również ochrony prawnej. Uregulowania prawne w połączeniu z właściwym systemem informacyjnym są w stanie ograniczyć zagrożenia w strefie informacji do akceptowalnych. Skuteczna ochrona systemu informacyjnego wymaga permanentnego monitoringu otoczenia wewnętrznego i zewnętrznego w każdej organizacji. Galopująca skala przestępstw w obszarze informacji i trudności w identyfikacji cyberprzestępców stanowią o istności podejmowanej problematyki, zwłaszcza że brakuje specjalistów ochrony systemów informacyjnych przed hakerami. Podmioty gospodarcze pozostają same z powyższym problemem, który zakłóca ich prawidłowy rozwój i umniejsza ochronę aktywów. Kolejnym istotnym aspektem bezpieczeństwa systemu informacyjnego jest obszerna skala zagrożeń oraz rażące w skutkach próby osłabienia, zniszczenia, a nawet przejęcia jednostek organizacyjnych przez środowisko cyberprzestępców, konkurencji, obcych państw itp.

Bezpieczeństwo informacyjne niejednokrotnie uznawane jest jako element systemu informatycznego, jako synonim bezpieczeństwa komputerowego, telekomunikacyjnego[2], czy bezpieczeństwa sieciowego[3]. S. Kowalkowski, bezpieczeństwem informacyjnym określa zakres bezpieczeństwa przyjmujący wzrost

[1] PN-ISO/IEC 17799:2007, s. 9.

[2] Zob. R. J. Sutton, *Bezpieczeństwo telekomunikacji*, przeł. G. Stawikowski, Wydawnictwo Komunikacji i Łączności, Warszawa 2004, s. 17.

[3] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa 2010, s. 22.

znaczenia informacji w zachowaniu stabilności współczesnych międzynarodowych systemów ekonomicznych oraz uwzględniający zabezpieczenie przed atakami sieciowymi, a także skutkami ataków fizycznych i plasuje obok bezpieczeństwa politycznego, militarnego, ekonomicznego, społecznego, kulturowego, ekologicznego i ideologicznego[4].

System bezpieczeństwa informacyjnego powinien składać się z trzech ściśle powiązanych ze sobą i wchodzących w różne korelacje podsystemów:

- ***systemu bezpieczeństwa fizycznego***, w ramach którego zasoby informacyjne są fizycznie oddzielone od otoczenia, stosowane są systemy kontroli dostępu, itp. np. fizyczne zabezpieczenia pomieszczeń, w których znajdują się serwery. Dotyczy to także danych jawnych (niechronionych na podstawie regulacji ustawowych), bowiem w takim przypadku ochrona fizyczna koncentruje się m.in. na niedopuszczaniu do zniszczenia fizycznego nośników informacji tak, aby zapobiec jej utraceniu;
- ***system bezpieczeństwa personalnego***, a zatem określenia kręgu podmiotów, które posiadają różny stopień uprawnień dostępu. Możemy zatem wyróżnić osoby, które mają fizycznie dostęp do nośników informacji (np. technicy), mają dostęp do zasobów informacyjnych (w całości lub w części) czy mają uprawnienia do wprowadzania zmian w systemie (np. dodawania nowych rekordów, usuwania rekordów czy ich edytowania w formie zmiany treści);
- ***systemu bezpieczeństwa informacyjnego*** (w przypadku – co w obecnych czasach jest standardem – elektronicznego przetwarzania informacji), a zatem narzędzi pozwalających na zachowanie kontroli dostępu, dystrybucji uprawnień, zapobieganie nieuprawnionemu dostępowi, zapobieganie nieuprawnionej instalacji złośliwego oprogramowania itp.)[5].

O problemie utrzymania bezpieczeństwa systemu informacyjnego Winn Schwartau pisał w swej książęce opisującej walkę informacyjną, którą zdefiniował, jako:

> działania ukierunkowane na ochronę, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacyjnych albo też zaprzeczenie informacjom po to, aby osiągnąć korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem[6].

[4] S. Kowalkowski (red.) Niemilitarne zagrożenia bezpieczeństwa publicznego, AON, Warszawa 2011, s. 13-15.

[5] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka zarządzanie bezpieczeństwem*, Difin, Warszawa 2012, s. 29-30.

[6] W. Schwartau, *Information Warfare*, New York 1994. Por.: P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005, s. 132.

Podobnego zdania jest L. Ciborowski, który uważa, że:

> wszelkie działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego działania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron jest walką informacyjną, która lokuje się w grupie walk niezbrojnych pomijających fizyczne niszczenie i zagrożenie życia[7].

Systemy informacyjne bez wystarczającej kontroli bezpieczeństwa mogą okazać się piętą Achillesową tak, jak „w trakcie kampanii wyborczej w 2016 r. Rosjanie hakowali systemy wyborcze we wszystkich 50 stanach USA – podała w raporcie Komisja do spraw Wywiadu Senatu Stanów Zjednoczonych. Wcześniejsze ustalenia w tej sprawie nie wskazywały na tak szeroką operację Kremla. Komisja Senatu USA opisała „bezprecedensowy poziom aktywności przeciwko państwowej infrastrukturze wyborczej". Miała ona na celu poszukiwanie słabych stron w zabezpieczaniu wyborczego systemu informatycznego. Raport stwierdza, że nie ma dowodów, że bezpośrednio wpłynięto na rozkład głosów. Przyznaje jednocześnie, że Rosjanie mieli możliwości, by „wykasować lub zmienić wyborcze dane" w Illinois. „Rosyjskie zamiary dotyczące amerykańskiej infrastruktury wyborczej pozostają niejasne". Ustalenia Komisji nie podejmują bezpośredniej krytyki amerykańskich agencji wywiadowczych czy poszczególnych stanów. Wykazują jednak, że rosyjskie działania były w 2016 r. niedoceniane, a ostrzeżenia przed nimi „zbyt ciche"[8].

Ujęte w monografii artykuły mają wymiar teoretyczny, jak i praktyczny; wiele z nich ma charakter interdyscyplinarny. Dążeniem autorów niniejszej publikacji jest zaprezentowanie wyników badań naukowych, podzielenie się doświadczeniami wywodzącymi się z praktyki oraz doświadczeniami naukowo-badawczymi, podjęcie dyskusji i wymiany myśli oraz wskazanie nowych obszarów badań w zakresie etyki w zarządzaniu. Wnioski zawarte w prezentowanych artykułach stanowią przyczynek do dalszych pogłębionych badań oraz dociekań naukowych i praktycznych.

Autorzy wyrażają nadzieję, iż treści zawarte w niniejszej monografii przyczynią się do rozwoju wiedzy o bezpieczeństwie systemów informacyjnych w organizacji.

prof. dr hab. inż. Jarosław Wołejszo
dr hab. Krzysztof Rejman
dr Małgorzata Wilczyńska

[7] L. Ciborowski, *Walka informacyjna*, Wydawnictwo Adam Marszałek, Toruń 2001, s. 68.
[8] https://www.tvn24.pl/wiadomosci-ze-swiata,2/senat-usa-rosjanie-hakowali-systemy-wyborcze-we-wszystkich-stanach,956132.html [dostęp: 17.05.2021].