ZESZYTY NAUKOWE WSOWL

Nr 4 (162) 2011 ISSN 1731-8157

Ireneusz J. JÓŹWIAK[*]
Artur SZLESZYŃSKI[**]

ROLA ORAZ BEZPIECZEŃSTWO INFORMACJI W UCZELNI PUBLICZNEJ I NIEPUBLICZNEJ

W artykule przedstawiono rolę informacji w działalności uczelni publicznej i niepublicznej. Podano kryterium sprawnego funkcjonowania systemu informacyjnego wewnątrz uczelni. Zaprezentowano definicje inherentnej i pragmatycznej jakości informacji. Następnie przedstawiono kryteria wartościujące informację w procesie podejmowania decyzji. Określono rodzaje zagrożeń dla bezpieczeństwa informacji, przypisując je do źródeł zewnętrznych i wewnętrznych. Opisano organizację systemu zarządzania bezpieczeństwem informacji w uczelni, którego ważnym elementem jest forum bezpieczeństwa. Uzasadniono konieczność tworzenia systemu zarządzania bezpieczeństwem informacji w uczelni publicznej lub niepublicznej.

Słowa kluczowe: *bezpieczeństwo informacji, system zarządzania bezpieczeństwem informacji, wartość informacji, szkolnictwo wyższe*

WSTĘP

System informacyjny jest elementem składowym (podsystemem) systemu, jakim jest organizacja. System informacyjny każdej organizacji odpowiedzialny jest za utrzymanie jej w homeostazie. Sprawne działanie systemu informacyjnego umożliwia osiąganie celów biznesowych, stawianych przed organizacją. W przypadku szkoły wyższej celami tymi będą: prowadzenie badań naukowych podnoszących poziom wiedzy w danej dziedzinie naukowej oraz transfer wiedzy wykonywany w trakcie procesu dydaktycznego. Dodatkowo w przypadku uczelni niepublicznych, będą to również cele biznesowe, polegające na uzyskaniu założonego wyniku finansowego, który umożliwi działanie organizacji. Zatem informacja w systemie informacyjnym ma na celu zapewnienie możliwości kierowania uczelnią, polegającą na uzyskaniu pożądanych zachowań u odbiorców wiadomości.

[*] dr hab. inż. Ireneusz J. JÓŹWIAK – Wydział Informatyki i Zarządzania Politechniki Wrocławskiej

[**] mjr mgr inż. Artur SZLESZYŃSKI – Wydział Zarządzania Wyższej Szkoły Oficerskiej Wojsk Lądowych

W komórkach organizacyjnych uczelni przetwarzane są dane dotyczące: pracowników, studentów, prowadzonych kursów, wyników badań itp. Obecnie przetwarzanie wymienionych rodzajów informacji odbywa się przy wykorzystaniu narzędzi informatycznych. Narzędzia te przyspieszają procesy selekcji, agregacji oraz wyszukiwania danych potrzebnych do sprawnego funkcjonowania uczelni. Działania te wynikają z potrzeb szkoły wyższej oraz jej współpracy z otoczeniem zewnętrznym. Zbiory danych gromadzonych przez komórki organizacyjne uczelni, udostępniane są podmiotom zewnętrznym[1], co jest rezultatem wypełnienia zapisów prawa powszechnego, np. prawa podatkowego. Zadaniem uczelni jest ochrona posiadanych zasobów informacyjnych.

Informacja, która jest obiektem niematerialnym i stanowi zasób posiadający wartość materialną lub niematerialną. Materialna wartość informacji związana jest ze spodziewaną korzyścią mającą swój ekwiwalent w kwotach pieniężnych[2]. Przykładem wartości materialnej mogą być przychody z patentów czy wzorów użytkowych. Niematerialna wartość informacji związana jest z wiedzą zdobytą przez uczelnię lub jej renomą. Próba określenia wartości niematerialnej dla wiedzy lub renomy jest trudna i opiera się na szacunkach, a nie wyliczeniach.

Informacja, jako zasób o szczególnym znaczeniu dla organizacji[3], powinna być właściwie chroniona. Norma PN ISO/IEC-17799 stwierdza, że informacja dla organizacji jest tak samo ważna jak zasoby finansowe czy nieruchomości[4]. Kwestie związane z ochroną zasobów informacyjnych regulują zapisy prawa powszechnego[5] oraz normy krajowe i zagraniczne[6]. Za niewłaściwą ochronę zasobów informacyjnych akty prawne przewidują kary pieniężne do kary pozbawienia wolności[7] włącznie. Konkludując, ochrona informacji nie jest tylko „dobrą wolą" władz organizacji. Wymóg skutecznej ochrony informacji wynika z przepisów prawa szczegółowego. Ignorowanie nakazów prawnych przez podmiot gromadzący i przetwarzający dane może skutkować konsekwencjami karnymi oraz utratą zaufania u osób lub instytucji współpracujących z uczelnią. Potencjalne straty, będące wynikiem zaniedbań w obszarze ochrony informacji, będą miały wymiar materialny i niematerialny.

1. ROLA INFORMACJI W DZIAŁALNOŚCI UCZELNI

Żeby mówić o systemie informacyjnym, należy przedstawić jego strukturę. W strukturze systemu informacyjnego wyróżnia się trzy elementy: źródło informacji, kanał transmisyjny oraz odbiorca[8]. Strukturę systemu informacyjnego uczelni przedstawiono na rysunku 1. W uczelni źródłami informacji będą władze uczelni, nauczyciele akademiccy, pracownicy administracyjni, studenci, organizacje zewnętrzne znajdujące się w otoczeniu uczelni. Grupa odbiorców posiada taki sam skład, jak

---

1 Pod tym pojęciem rozumie się np. systemy informatyczne wykorzystywane przez uczelnię, takie jak system kadrowo – płacowy itp.

2 Zob. A. Aczel, *Statystyka w zarządzaniu* s. 104.

3 Zob. B. Hysa, *Jakość informacji…*s. 77. *Polska Norma PN-ISO/IEC-17799:2007*.

6 Zob. *Polska Norma PN-ISO/IEC-17799:2007*.

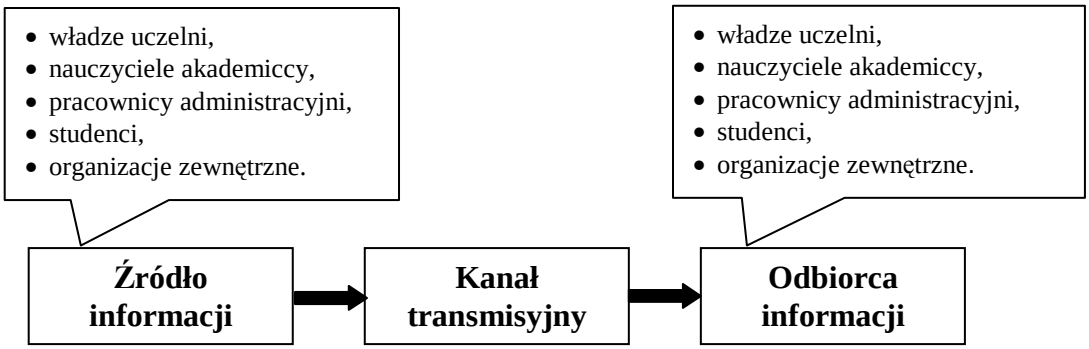
5 Zob. Ustawa o ochronie danych osobowych, Kodeks karny, Ustawa o nieuczciwej konkurencji, itp.

6 Zob. *Polska Norma PN-ISO/IEC 17799:2007 …, International Standard ISO/IEC-15408….*

7 Zob. Ustawa o ochronie danych osobowych, Kodeks karny, Ustawa o nieuczciwej konkurencji, itp.

8 Zob. P. Sienkiewicz, *Inżynieria systemów…*, s. 60.

opisana wcześniej grupa źródeł informacji. Kanałami transmisyjnymi będą druk, obraz oraz media elektroniczne. Taki sam skład źródeł informacji oraz odbiorców informacji oznacza, że system ten działa dwukierunkowo. Źródło informacji po wysłaniu wiadomości do systemu będzie oczekiwało na informację zwrotną, czyli zmieni funkcję na odbiorcę informacji.



Rys. 1. Struktura systemu informacyjnego uczelni

Źródło: Opracowanie własne na podstawie P. Sienkiewicz, Inżynieria systemów wybrane zastosowania wojskowe, Wydawnictwo Ministerstwa Obrony Narodowej, Warszawa 1983

We wstępie stwierdzono, że rolą informacji jest utrzymanie systemu, którym jest uczelnia, w homeostazie. Informacja ma umożliwić stymulowanie podsystemów do działania lub działań zgodnych z wolą władz uczelni. Zwrotnie uzyskuje się informacje diagnostyczne potwierdzające realizację przekazanych działań lub informujące o problemach uniemożliwiających lub opóźniających wykonanie przekazanych zadań.

Jednym z podstawowych zadań uczelni jest realizacja funkcji edukacyjnej, polegająca na kształceniu studentów według przyjętego programu zgodnego z kierunkiem studiów. Do realizacji procesu kształcenia potrzebne są zasoby, do których należą wykładowcy, studenci, sale wykładowe lub laboratoryjne wraz z niezbędnym wyposażeniem. Informacja o posiadanych zasobach, programach studiów, aktualnym stanie wiedzy oraz oczekiwaniach pracodawców zatrudniających absolwentów uczelni (organizacje zewnętrzne), umożliwia podejmowanie decyzji, rezultatem których są modyfikacje oferty edukacyjnej, zgodnie z oczekiwaniami studentów i pracodawców.

W przedstawionym procesie uczestniczą, wymienione w strukturze systemu informacyjnego, grupy osób. Od systemu informacyjnego oczekuje się sprawnego przekazywania informacji w obu kierunkach. Sprawne przekazywanie informacji wewnątrz i na zewnątrz systemu można zdefiniować jako terminowe (informacja od źródła do odbiorcy powinna być dostarczona w najkrótszym czasie) i wierne (treść informacji, w kanale transmisyjnym, powinna zostać niezmieniona) przekazywanie wiadomości.

Informacja pełni funkcje stymulujące dla jej odbiorców (określa czego oczekuje decydent) i funkcje informacyjne dla decydenta (diagnozuje aktualny stan realizacji przekazanych zadań). Przez decydenta należy rozumieć nie tylko władze uczelni, ale również pracowników administracyjnych, nauczycieli akademickich, studentów oraz otoczenie zewnętrzne (np. pracodawców, ministerstwo itp.). Wykonawcami będą te

same grupy osób, jednak każda grupa będzie wykonywać zadania adekwatnie do ich miejsca w hierarchii szkoły wyższej oraz posiadanych kompetencji.

Funkcja edukacyjna nie jest jedyną wykonywaną przez szkołę wyższą. Kolejną funkcją zewnętrzną realizowaną przez uczelnię jest prowadzenie badań naukowych lub działalności innowacyjno – wdrożeniowej. Działalność ta umożliwia uczelni pozyskiwanie środków oraz zdobywanie doświadczeń przenoszonych do procesu kształcenia. Jej wyniki mają wpływ na modyfikację planów działania szkoły wyższej, tak by możliwie najlepiej dostosować ofertę edukacyjną do potrzeb rynku oraz oczekiwań studentów.

Wymienione procesy korzystają z informacji do podejmowania decyzji o działaniach uczelni. Podejmowanie decyzji jest zaś wyborem pewnego sposobu działania[9], co wiąże się konsekwencjami w wymiarze finansowym. Od jakości przekazywanych informacji oraz czasu ich transmisji w systemie informacyjnym zależy skuteczność procesu decyzyjnego. Pojęcie jakości informacji można zdefiniować w dwóch obszarach – jako jakość inherentną lub jakość pragmatyczną[10]. Inherentna jakość informacji oznacza zdolność przekazu do dokładnego opisu obiektu będącego podmiotem wiadomości. Pragmatyczna jakość informacji oznacza jej użyteczność w procesie podejmowania decyzji, co oznacza, że treść wiadomości może zostać wykorzystana, przez jej odbiorcę do realizacji zamierzonych celów.

Do dalszych rozważań przyjęta zostanie definicja pragmatycznej jakości informacji. Wybór pragmatycznej jakości informacji wynika z faktu, iż możliwe jest określenie korzyści, jakie związane są z wykorzystaniem informacji. Na podstawie rozważań dotyczących roli informacji w funkcjach edukacyjnej i badawczej, można przyjąć, że informacja posiada wartość. Ocena wartości informacji przez decydenta, zostanie przeprowadzona przy pomocy dwóch kryteriów oceny. Pierwszym jest zmniejszenie stopnia niepewności u decydenta, skutkujące podjęciem właściwej (czasami optymalnej) decyzji. Drugim kryterium oceny będzie spodziewana korzyść wynikająca z decyzji podjętej na podstawie informacji.

W przypadku pierwszego kryterium optymalności decyzji będzie minimalna wartość funkcji niepewności. Sytuacja decyzyjna opisana jest wzorem (1)

$$N(i) \rightarrow min \tag{1}$$

gdzie:

$N(i)$ – wartość funkcji niepewności

i – informacja przekazana decydentowi

Wzór (1) przedstawia inne ujęcie entropii informacyjnej określającej stan niewiedzy, która występuje w teorii informacji. Pominięcie ilościowej miary rozmiaru wiadomości stosowanej powszechnie w telekomunikacji ma na celu przedstawienie wpływu informacji na decyzję podejmowaną przez decydenta. Informacje docierające do decydenta tworzą obszar decyzyjny. Obszar ten definiowany jest stanem wiedzy decydenta, o problemie decyzyjnym przed otrzymaniem danej wiadomości oraz po jej otrzymaniu[11]. Sytuację tę można przedstawić przy pomocy równania (2)[12].

[9] Zob. B. Hysa, *Jakość…*, op. cit., s. 77.

[10] Ibidem, s. 79.

[11] Zob. P. Sienkiewicz, *Inżynieria…*, op. cit., s. 64.

$$I(X,Y) = H(X) - H(X/Y) \quad (2)$$

gdzie:

I(X,Y) – ilość informacji, jaką niesie sygnał Y,

H(X) – entropia informacyjna sygnału X (stopień niepewności przed odebraniem sygnału Y)

H(X/Y) – entropia informacyjna po odebraniu sygnału Y

Informacja jest użyteczna dla decydenta wtedy, gdy zmniejsza jego niepewność, czyli tym więcej danych dostarczane jest osobie podejmującej decyzję. Zatem entropia informacji (*H(X)*) wpływa na stan wiedzy o problemie decyzyjnym, a przez to pozwala wybrać najlepszy wariant decyzyjny.

Drugie kryterium odnoszone jest do wartości oczekiwanej korzyści powstałej w wyniku podjęcia decyzji na podstawie odebranej informacji. Określenie wartości informacji szacowane będzie na podstawie funkcji zysku wyrażonej przy pomocy wzoru (3)

$$Z(i) = P(i) - K(i) \quad (3)$$

gdzie:

Z(i) – spodziewany zysk będący skutkiem podjęcia decyzji na podstawie informacji *i*

i – informacja

P(i) – oczekiwany przychód powstały w wyniku wykorzystania informacji *i*

K(i) – przewidywany koszt realizacji przedsięwzięcia na podstawie informacji *i*

Analizując wzory (1) i (3), można stwierdzić, że wartość informacji dla decydenta rośnie wraz ze zmniejszeniem niepewności (wiedza decydenta o problemie decyzyjnym jest większa), a funkcja przewidywanego zysku zmierza do wartości maksymalnej.

2. BEZPIECZEŃSTWO INFORMACJI

Bezpieczeństwo informacyjne jest jednym z istotnych składników bezpieczeństwa funkcjonowania szkoły wyższej. Uczelnia jako organizacja działa w określonym otoczeniu prawnym. Do prawidłowego funkcjonowania szkoły konieczne jest bezpieczeństwo otoczenia, informacyjne oraz teleinformatyczne. Relacje pomiędzy wymienionymi rodzajami bezpieczeństwa pokazano na rysunku 2.

Pomimo iż informacja posiada wartość, jej ochrona bywa często lekceważona. Świadczą o tym wyniki badań przeprowadzonych przez firmę IDG, dotyczące ochrony informacji w jednostkach administracji publicznej. Do próby badawczej wytypowano urzędy administracji szczebla centralnego (ministerstwa, urzędy wojewódzkie, urzędy miast w dużych miejscowościach) oraz urzędy administracji samorządowej (urzędy gmin, urzędy powiatowe)[13].

---

[12] Ibidem, s. 64.

[13] *Bezpieczeństwo informacji w administracji publicznej w Polsce*, s. 3.

Rys. 2. Relacja pomiędzy bezpieczeństwem otoczenia szkoły wyższej a bezpieczeństwem informacyjnym i teleinformatycznym

Źródło: Opracowanie własne na podstawie A. Białas, Bezpieczeństwo informacji i usług we współczesnej instytucji i firmie, WNT, Warszawa 2006

Analiza zebranych danych pozwala stwierdzić, że bezpieczeństwo informacyjne oraz bezpieczeństwo teleinformatyczne organów administracji jest różne. Wysokie jest w przypadku urzędów administracji centralnej (ministerstwa, urzędy wojewódzkie, urzędy miejskie itp.), a niskie w urzędach administracji lokalnej (urzędy powiatowe, urzędy gminne). Rozbieżności te są wynikiem świadomości (kierownictwa i pracowników) dotyczącej zagrożeń dla bezpieczeństwa informacji[14]. Badania pokazały, że jednostki administracji centralnej kwestie bezpieczeństwa informacji traktowały kompleksowo. Oznaczało to rozwój organizacyjnego i technicznego aspektu bezpieczeństwa informacji. Jednostki samorządu lokalnego, nie dysponując takimi zasobami, jak jednostki administracji centralnej, nie były w stanie kompleksowo poradzić sobie z ochroną zasobów informacyjnych. Jednostki administracji centralnej współpracują z podmiotami zewnętrznymi, którymi są jednostki organizacyjne, np. Unii Europejskiej lub Sojuszu NATO. Możliwość współpracy informacyjnej (uzyskanie prawa do wymiany informacji) z jednym z wymienionych podmiotów wymaga poddania się, przez jednostkę administracyjną, procedurze sprawdzającej. Po uzyskaniu pozytywnego wyniku procedury sprawdzającej, jednostka administracji otrzymuje certyfikat. Dokument ten potwierdza przestrzeganie ustalonych przez prawo zasad bezpiecznej wymiany i przechowywania informacji. Procedura weryfikacyjna odbywa się w trakcie zewnętrznego audytu bezpieczeństwa informacji. Audyt ten wykonywany jest przez służby ochrony państwa[15] lub firmy posiadające akredytację agencji ochrony informacji z NATO i (lub) Unii Europejskiej.

W pracy systemów teleinformatycznych występują incydenty związane z naruszeniami bezpieczeństwa informacji znajdujących się wewnątrz elementów systemu. Ankieterzy zapytali respondentów, czy wykryte incydenty są zgłaszane organom

[14] Ibidem, s. 15.

[15] Ustawa o ochronie informacji niejawnych, art. 60 pp. 2, s. 30.

ścigania (policja lub prokuratura). Większość respondentów stwierdziła, iż tego typu incydenty nie są zgłaszane organom ścigania. Uzasadnieniem udzielonej odpowiedzi jest fakt niskiej skuteczności[16] organów ścigania w identyfikacji i zatrzymaniu sprawców.

Powinno pojawić się pytanie – co łączy raport dotyczący bezpieczeństwa informacji w jednostkach administracji publicznej z bezpieczeństwem informacji wykorzystywanej w funkcjonowaniu uczelni publicznej i niepublicznej? Oba podmioty, uczelnie i urzędy, działają w tym samym systemie prawnym, który definiuje ich zachowania w obszarze bezpieczeństwa informacji. Można przyjąć, że w obu przypadkach poziom ochrony informacji zależny jest od stopnia świadomości władz uczelni oraz pracowników odpowiedzialnych za ochronę i użytkowanie zasobów informacyjnych. Poziom ochrony zależy od środków przeznaczonych na ochronę informacji w każdej postaci[17]. Tym, co odróżnia uczelnię od urzędu, jest występowanie dodatkowego zagrożenia związanego z wykrywaniem podatności w systemie bezpieczeństwa informacji przez studentów. Celem działania studentów penetrujących system zabezpieczeń jest chęć wykazania się wysokimi umiejętnościami w dziedzinie bezpieczeństwa teleinformatycznego. Innym motywem działania atakującego może być chęć zmiany niekorzystnej oceny lub próba uzyskania stypendium itp. Jest to możliwe, gdyż dane te przechowywane są w systemach podłączonych do systemów ogólnodostępnych[18].

Oceniając system informacyjny uczelni, można wyodrębnić dwie grupy zagrożeń dla bezpieczeństwa informacji. Pierwszą z nich stanowią elementy otoczenia systemu informacyjnego uczelni, nazywane źródłami zewnętrznymi zagrożeń. Do tej grupy należą następujące podmioty:

- firmy i instytucje współpracujące z uczelnią (urzędy, banki, przedsiębiorstwa itp.);
- sieć telekomunikacyjna;
- hakerzy.

Drugą grupę źródeł zagrożeń dla bezpieczeństwa informacji stanowią elementy systemu informacyjnego uczelni, nazywane wewnętrznymi źródłami zagrożeń, do których należą:

- oprogramowanie (aplikacje, aplikacje webowe itp.);
- sprzęt informatyczny (komputery, drukarki, terminale, urządzenia sieciowe itp.);
- pracownicy uczelni;
- studenci.

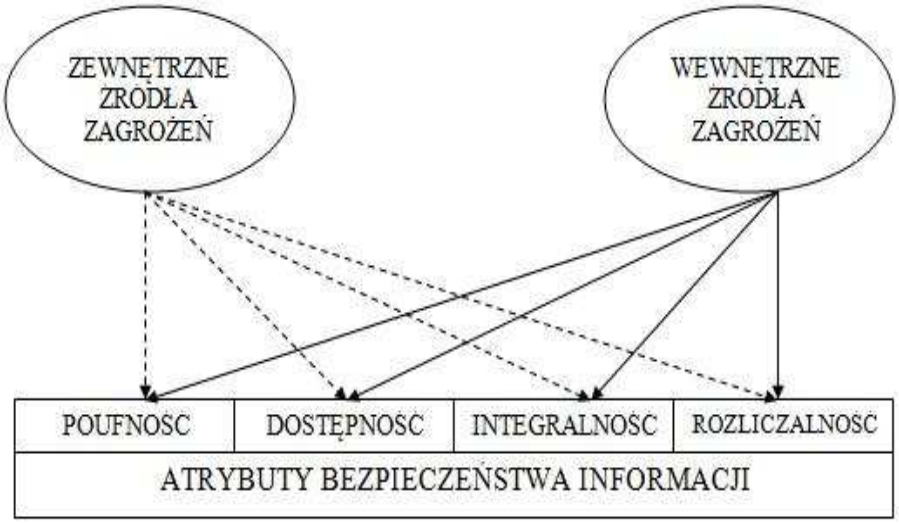
---

[16] *Bezpieczeństwo informacji* …, op. cit., s. 11.

[17] A. Białas, *Bezpieczeństwo informacji* …, s. 27.

[18] Pod pojęciem systemu ogólnodostępnego rozumie się system informacyjny pozwalający studentom i pracownikom uczelni na dostęp do informacji dotyczących programu kształcenia, uzyskanych wyników, stypendiów, pomocy materialnej itp. Dostęp do informacji może odbywać się na terenie uczelni poprzez terminale, ale powszechnie stosowany jest dostęp za pomocą przeglądarek internetowych lub technologii WAP dostępnej w telefonach komórkowych. System taki posiada ustalone zasady dostępu do określonego typu informacji nazywane również zasadami bezpieczeństwa. Przy określaniu uprawnień w dostępie do informacji wykorzystywana jest zasada wiedzy koniecznej.

Każda z wymienionych grup może celowo lub przypadkowo wpływać na bezpieczeństwo informacji gromadzonej, przetwarzanej i przesyłanej w systemie informacyjnym uczelni. Wynikiem takiego oddziaływania będzie zmiana wartości atrybutów bezpieczeństwa informacji[19], takich jak: poufność, dostępność, integralność i rozliczalność. Oddziaływania pomiędzy źródłami zagrożeń a atrybutami bezpieczeństwa informacji przedstawiono na rysunku 3.



Rys. 3. Oddziaływanie zewnętrznych i wewnętrznych źródeł zagrożeń na atrybuty bezpieczeństwa informacji gromadzonej, przetwarzanej i dystrybuowanej w systemie informacyjnym uczelni

Źródło: Opracowanie własne

Zmiana wartości atrybutów bezpieczeństwa informacji związana jest z różnymi konsekwencjami dla funkcjonowania szkoły. Od krótkotrwałego braku dostępu do zasobu informacyjnego do zatrzymania działania wydziału uczelni. Ocenę częstości występowania zagrożeń oraz ich konsekwencje realizuje się w trakcie analizy ryzyka. Jej wyniki są wytycznymi do zarządzania ryzykiem wewnątrz uczelni. Analiza określa wrażliwość zasobu informacyjnego oraz związane z nim częstość występowania zagrożeń i ich konsekwencje.

Chcąc zarządzać ryzykiem dla bezpieczeństwa informacji w uczelni, należy utworzyć forum bezpieczeństwa informacji uczelni. Forum bezpieczeństwa jest elementem systemu zarządzania bezpieczeństwem informacji w szkole wyższej. Utworzenia takiej struktury zaleca norma PN ISO/IEC-17799. Celem działania forum wewnątrz organizacji jest:

- identyfikacja zagrożeń dla bezpieczeństwa informacji;
- utworzenie dokumentacji systemu bezpieczeństwa informacji;
- zapewnienie środków niezbędnych do redukcji zagrożeń,
- monitorowanie zagrożeń i incydentów w bezpieczeństwie informacji.

Tworząc system zarządzania bezpieczeństwem informacji, należy określić, jakie grupy informacji są najważniejsze dla funkcjonowania szkoły wyższej. Identyfikacji

[19] *PN ISO/IEC-17799:2007*, op. cit.

zasobów, które powinny podlegać ochronie można dokonać na podstawie kryterium kosztu będącego konsekwencją niewdrożenia procedur chroniących dany zasób informacyjny. Jeżeli szacowana wartość konsekwencji jest wysoka, oznacza to, że analizowany zasób powinien podlegać szczególnej ochronie, gdyż ma on duży wpływ na zapewnienie ciągłości działania uczelni.

Władze uczelni, tworząc forum bezpieczeństwa informacji wewnątrz uczelni, powinny w jego składzie umieścić przedstawicieli:

- rektora, senatu i kanclerza;
- wydziałów, katedr, instytutów i zakładów;
- komórek wspierających działalność uczelni (kwestury, kadr, dział IT, radcy prawnego itp.);
- firm i organizacji współpracujących z uczelnią;
- konsultantów zewnętrznych wspomagających pracę zespołu (tylko, gdy zachodzi taka potrzeba).

Zadaniem przedstawicieli jednostek organizacyjnych szkoły wyższej jest wskazanie tych zasobów informacyjnych, które posiadają kluczowe znaczenie dla bieżącego funkcjonowania oraz planowej strategii rozwoju uczelni. Do wymienionej grupy można zaliczyć informacje dotyczące:

- działalności patentowej i wynalazczej;
- wyników prowadzonych prac naukowo – badawczych, prac zleconych, itp.;
- ochrony własności intelektualnej uczelni;
- danych osobowych studentów i pracowników szkoły wyższej;
- wyników procesu kształcenia (efektywność, problemy w realizacji zajęć, itp.);
- wyników analiz mających wpływ na planowanie strategii rozwoju uczelni;
- planowej współpracy z otoczeniem biznesowym, jednostkami administracji rządowej i samorządowej itp.;
- oczekiwań otoczenia biznesowego w stosunku do absolwentów uczelni (studiów pierwszego i drugiego stopnia, studiów podyplomowych, kursów specjalistycznych itp.);
- oczekiwań studentów związanych z realizowanym programem studiów;
- współpracy naukowo – badawczej z uczelniami i jednostkami naukowo – badawczymi w kraju i zagranicą;
- danych finansowych uczelni.

Znając obiekty informacyjne podlegające ochronie, można określić potencjalne zagrożenia oraz przewidywane konsekwencje ich wystąpienia. Wiedza ta posłuży do opracowania strategii zarządzania ryzykiem. Celem działań związanych z zarządzaniem ryzkiem jest ciągłe i skuteczne chronienie posiadanych zasobów. W literaturze przedmiotu

przedstawiane są trzy strategie zarządzania ryzykiem: redukcja, transferowanie i ignorowanie[20].

Strategia redukcji będzie dążyła do eliminacji zagrożenia lub minimalizacji negatywnych konsekwencji jego wystąpienia. Działaniami podejmowanymi w tej strategii są np.: nadawanie uprawnień w dostępie do zasobów przechowywanych w komputerowych systemach informacyjnych, monitorowanie działania elementów systemu, stosowanie oprogramowania antywirusowego czy stałe wykonywanie kopii bezpieczeństwa danych.

Strategia transferowania polega na ubezpieczeniu się od konsekwencji wystąpienia zagrożenia. Stosowana jest wtedy, gdy nie można wyeliminować zagrożenia lub gdy koszt budowania systemu ochrony jest ekonomicznie nieuzasadniony. Przykładem zagrożeń, których nie można wyeliminować są: klęski żywiołowe, pożary itp.

Ostatnia ze strategii polega na ignorowaniu zagrożeń i niepodejmowaniu żadnych działań związanych z ochroną informacji. Podejście to wynika z przekonania decydentów, iż informacje wykorzystywane przez szkołę wyższą, nie będą interesującym obiektem dla działań potencjalnego agresora.

Skład forum powinien zapewniać interdyscyplinarne podejście do problematyki bezpieczeństwa, gdyż dotyczy ona ochrony fizycznej, elektronicznej, itp. W wielu uczelniach przyjmuje się, że bezpieczeństwo informacji jest domeną komórki IT szkoły wyższej. Tezę tę potwierdzają badania firmy IDG, w których 58%[21] respondentów wskazało administratora systemu informatycznego, jako osobę odpowiedzialną za bezpieczeństwo informacji.

Myślenie to jest poprawne tylko w przypadku bezpieczeństwa teleinformatycznego w uczelni. Wynika ono z faktu, iż bezpieczeństwo informacji ograniczone zostaje do grupy urządzeń technicznych wykorzystywanych w gromadzeniu, przetwarzaniu i przesyłaniu danych za pomocą lokalnej i rozległej sieci komputerowej. Przykładem wykazującym błędność takie myślenia jest pytanie – w jaki sposób administrator lokalnej sieci komputerowej ma chronić informacje mające postać dokumentów drukowanych, zdjęć, będące przekazem ustnym itp.? Wymienione źródła informacji wskazują, że bezpieczeństwo informacyjne obejmuje większy zakres niż bezpieczeństwo teleinformatyczne. Relacje pomiędzy bezpieczeństwem otoczenia systemu, bezpieczeństwem informacyjnym a bezpieczeństwem teleinformatycznym pokazano na rysunku 2.

Administrator lokalnej sieci komputerowej nie może być odpowiedzialny za kompleksową ochronę informacji wewnątrz uczelni. Może on odpowiadać za ochronę wskazanych wcześniej zasobów informacyjnych, znajdujących się na nośnikach danych urządzeń pracujących w sieci komputerowej.

W jednostkach administracji publicznej kwestie związane z bezpieczeństwem informacji rozdzielone są jako obowiązki dla kilku osób. Sytuacja ta jest wynikiem wprowadzenia przez jednostki administracji rządowej i samorządowej regulacji prawnych nakazujących utworzenie funkcji pełnomocników ochrony informacji niejawnych[22] lub

[20] A. Białas, *Bezpieczeństwo* …, op. cit., s. 84.

[21] *Bezpieczeństwo informacji w...*, op. cit., s. 7.

[22] Ustawa o ochronie informacji niejawnych…, op. cit., s. 28.

administratorów danych osobowych i administratorów baz informacji[23]. Rozmycie odpowiedzialności może skutkować pojawieniem się sytuacji, w których administrator danych osobowych lub pełnomocnik do spraw ochrony informacji niejawnych będą przekonywać, że obsługa zaistniałego incydentu nie należała do ich obowiązków.

Sytuacji opisanej może zapobiec forum ochrony informacji, gdyż cykliczne spotkania lub spotkania organizowane doraźnie przez przedstawiciela rektora pozwolą na koordynowanie funkcjonowania takiego systemu wewnątrz uczelni. Również forum powinno określić, za jakie zdarzenia będzie odpowiadać pełnomocnik ochrony informacji niejawnych, administrator danych osobowych oraz administrator sieci teleinformatycznej.

Zadaniem forum jest przygotowanie i przeprowadzenie szkoleń dla wszystkich pracowników uczelni, partycypujących w systemie informacyjnym uczelni. Konieczność objęcia szkoleniami wszystkich użytkowników wynika z faktu zapoznania pracowników uczelni z potencjalnymi zagrożeniami oraz konsekwencjami ich wystąpienia. Służy to kształtowaniu świadomości zagrożeń u uczestników systemu informacyjnego. Bardzo często przyjmuje się, pomijając ograniczenie rozważań do systemu teleinformatycznego, że środki techniczne rozwiążą wszystkie problemy związane z bezpieczeństwem. Twierdzenie to jest błędne, ponieważ informacja może mieć różne postacie – nie tylko postać cyfrową, umożliwiającą jej przetwarzanie przez sprzęt komputerowy. Ochronę informacji w postaci innej niż elektroniczna, zapewni świadomy użytkownik, który daje rękojmię zachowania jej bezpieczeństwa.

Poświadczenie bezpieczeństwa osobowego będzie wymagało poddania części pracowników uczelni procedurze sprawdzającej prowadzonej przez służby ochrony państwa[24] lub według standardów wzorowanych na procedurach służb ochrony państwa. Przeprowadzenie wszystkich wymienionych czynności sprawi, że system ochrony informacji w uczelni będzie działał sprawnie, wspomagając działalność bieżącą szkoły wyższej.

PODSUMOWANIE

Ochrona zasobów informacyjnych może kłócić się z ideą uczelni, jako miejsca swobodnej i niczym nieskrępowanej wymiany poglądów oferującego nielimitowany dostęp do informacji. Czynności opisane w artykule dotyczące działań związanych z zastosowaniem zasady wiedzy koniecznej stoją w sprzeczności do zasady swobody dyskusji i wymiany wiedzy, poglądów i doświadczeń. Jednak uczelnia, publiczna i niepubliczna, działają w określonym otoczeniu prawnym, które wymusza określone w przepisach działania.

Produktem uczelni, szczególnie tych specjalizujących się w naukach technicznych, jest wiedza dotycząca procesów technologicznych, patentów oraz rozwiązań wynalazczych i nowatorskich. Zdobycie tego rodzaju wiedzy wymagało od uczelni nakładów finansowych. Zatem wiedza ta jest zasobem posiadającym wartość materialną równą ilości wydatkowanych na jej uzyskanie środków pieniężnych. Kradzież takich wiadomości oznacza straty finansowe dla uczelni. Patenty oraz wdrożenia innowacyjne pozwalają uczelni na pozyskiwanie dodatkowych środków na

[23] Ustawa o ochronie danych osobowych…, op. cit., s. 19.

[24] Ustawa o ochronie informacji niejawnych…, op. cit., s. 28.

jej funkcjonowanie. Im więcej patentów i wdrożeń szkoła posiada, tym większą ma szansę na realizację przedsięwzięć badawczych wspólnie z przemysłem.

Przykładem takiego działania może być Instytut Inżynierii Oprogramowania (Software Engineering Institute) z uniwersytetu Carnegie Mellon realizujący prace badawcze dla Sił Powietrznych Stanów Zjednoczonych. Czy można założyć, iż prawdopodobieństwo bezprawnego publikowania cudzych wyników badań jest zerowe? Czy można przyjąć, iż kradzież rozwiązania, które zamierza się opatentować jest zdarzeniem, które nigdy nie wystąpi?

Reasumując, ochrona informacji jest zagadnieniem ważnym, a jednocześnie przedsięwzięciem czasochłonnym i kosztownym. Koszt przedsięwzięć wynika z faktu, iż angażowane są zasoby osobowe i techniczne. Wynika on też z faktu, że jest niemożliwe uzyskanie się rozwiązania gwarantującego 100% bezpieczeństwo zasobu lub zasobów informacyjnych. Proces zabezpieczeń kończy się w momencie osiągnięcia akceptowalnego poziomu ryzyka dla zasobu lub zasobów informacyjnych.

LITERATURA

1. Aczel A., *Statystyka w zarządzaniu*, PWN, Warszawa 2008.
2. *Bezpieczeństwo informacji w administracji publicznej w Polsce.* Wyniki badań redakcji Computerworld przeprowadzonego w ramach przygotowań do V konferencji „Wolność i bezpieczeństwo" w Wieliczce 2008, [online] [dostęp: 2011]. Dostępny w Internecie: ftp://lead.download.idg.pl/lead/cw/raport_bezp1.pdf.
3. Białas A., *Bezpieczeństwo informacji i usług we współczesnej instytucji i firmie*, WNT, Warszawa 2006.
4. Hysa B., *Jakość informacji a podejmowanie decyzji*, [w:] „Zeszyty Naukowe Politechniki Śląskiej", Organizacja i Zarządzanie, z. 54, s. 77 – 84, Gliwice 2010.
5. *International Standard IEC/ISO 15408-1. Information technology – Security techniques - Evaluation criteria for IT Security – Part 1. Introduction and General model, Second edition*, International Organisation for Standardization ISO/IEC, Switzerland 2005.
6. *Polska Norma PN-ISO/IEC 17799:2007. Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*, Polski Komitet Normalizacyjny, Warszawa 2007.
7. Sienkiewicz P., *Inżynieria systemów wybrane zastosowania wojskowe*, Wydawnictwo Ministerstwa Obrony Narodowej, Warszawa 1983.
8. Ustawa o ochronie danych osobowych, Dz. U. nr 133 poz. 883 z dn. 29 sierpnia 1997 z póź. zmianami.
9. Ustawa o ochronie informacji niejawnych, Dz.U.1999 nr 11 poz. 95 nr z dn. 22 stycznia 1999 r. z póź. zmianami.

Ireneusz J. JÓŹWIAK, Artur SZLESZYŃSKI

ROLE AND SECURITY OF INFORMATION IN PUBLIC AND PRIVATE HIGHER EDUCATION SCHOOLS

Summary

The paper presents the role of information in the activity of public or private higher education schools. The paper defines two evaluation criteria for information value. The first of them is uncertainty, which is called information entropy. Then the influence of information entropy on the decision-making process is shown. The types of threats to information security are defined. The other criterion enables the evaluation of the value of message. This is strictly a statistical function of the expected benefits which can occur when a message will be used in the decision-making process. The paper presents a classification of the sources of threats which are divided into two groups: internal or external. The article explains a necessity to establish an information security system in an educational organisation such as a college or a university. Its important part is a security forum, which gathers personnel from each department of a college or a university. The security forum specifies risks for the university information assets which will next be protected by safeguards.

Key words: *information security, information security management system, value of information, higher education*