„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych” finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Identyfikowanie i szacowanie ryzyk związanych z bezpieczeństwem informatycznym w szkołach wyższych

Dr hab. Małgorzata Ganczar

Konferencja : Wzmacnianie odporności szkół wyższych na cyberataki poprzez podnoszenie kompetencji cyfrowych

Ministerstwo Edukacji i Nauki

UKSW UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

CLTC Centrum Liderów Transformacji Cyfrowej

Bezpieczeństwo

Bezpieczeństwo – stan, w którym dane dobra są zabezpieczone, tzn. nie istnieje obawa ich utraty.

W praktyce stan ten jest niemożliwy do osiągnięcia, ponieważ nigdy nie będziemy mieć stuprocentowej pewności, że zasoby, takie jak wiedza czy informacja, nie są narażone na ataki lub próby przejęcia.

Zapewnienie bezpieczeństwa informacji jest procesem ograniczenia ryzyka lub prawdopodobieństwa wystąpienia szkody.

Zagrożenie zawsze będzie istnieć. Wprowadzając jednak parę „prostych” zasad w podmiocie, możemy zmniejszyć ryzyko ujawnienia/utraty cennych informacji.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Bezpieczeństwo informatyczne

Bezpieczeństwo informatyczne odnosi się do praktyk, procedur, narzędzi i zabezpieczeń mających na celu ochronę systemów informatycznych, danych, sieci komputerowych oraz innych informacji przed nieautoryzowanym dostępem, używaniem, zmianami czy zniszczeniem. Jest to dziedzina, która ma kluczowe znaczenie w świecie cyfrowym, gdzie dane są coraz bardziej wartościowe i narażone na różnego rodzaju zagrożenia.

Bezpieczeństwo informatyczne **jest procesem ciągłym i wymaga stałej uwagi**, ponieważ zagrożenia cyfrowe ewoluują wraz z rozwojem technologii. Firmy oraz instytucje muszą stale aktualizować swoje metody, narzędzia i wiedzę, aby skutecznie chronić swoje zasoby informatyczne.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Bezpieczeństwo informatyczne

Bezpieczeństwo informatyczne obejmuje wiele obszarów, w tym:

Zabezpieczenia sieciowe: Ochrona infrastruktury sieciowej przed atakami z zewnątrz, w tym np.: złośliwym oprogramowaniem, hakerami, atakami DDoS i innymi zagrożeniami.
Ochrona danych: Zabezpieczenie informacji przed nieautoryzowanym dostępem, kradzieżą, utratą lub uszkodzeniem. To może obejmować szyfrowanie danych, zarządzanie dostępem, tworzenie kopii zapasowych i inne strategie zabezpieczające.
Zarządzanie zagrożeniami: Identyfikacja, monitorowanie i reagowanie na potencjalne lub rzeczywiste zagrożenia w czasie rzeczywistym, wykorzystując systemy monitorowania, analizę logów oraz narzędzia do wykrywania i reagowania na incydenty.
Bezpieczeństwo aplikacji: Zapewnienie bezpieczeństwa aplikacji komputerowych poprzez audyty kodu, poprawne zarządzanie uwierzytelnianiem i uprawnieniami oraz eliminowanie podatności na ataki.
Świadomość użytkowników: Edukacja pracowników i użytkowników końcowych w zakresie bezpiecznego korzystania z systemów informatycznych, rozpoznawania zagrożeń, używania silnych haseł i przestrzegania najlepszych praktyk w zakresie bezpieczeństwa.
Zgodność z regulacjami: Zapewnienie, że systemy informatyczne są zgodne z obowiązującymi przepisami, standardami branżowymi i regulacjami dotyczącymi ochrony danych, takimi jak RODO (GDPR), HIPAA czy inne odpowiednie przepisy.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Zarządzanie bezpieczeństwem informacji w polskich aktach prawnych:

❖ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych – rozdział 8 bezpieczeństwo teleinformatyczne, art. 49 ust. 1 „Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo.

❖Pojęcia:

ryzyko - kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

szacowanie ryzyka - całościowy proces analizy i oceny ryzyka;

zarządzanie ryzykiem - skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Zarządzanie bezpieczeństwem informacji w polskich aktach prawnych:

❖Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych, dalej rozporządzenie 2016/679)

❖wprowadza skuteczne procedury i mechanizmy koncentrujące się na tych operacjach przetwarzania, które mogą powodować ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie
wystąpienia i wadze.

❖Należy podkreślić, że analizy ryzyka dokonujemy z perspektywy osoby, której dane dotyczą, a nie administratora.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Zarządzanie bezpieczeństwem informacji w polskich aktach prawnych:

❖Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

❖ §20 rozporządzenia KRI zobowiązuje podmiot realizujący zadania publiczne do opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji, który zapewnia poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

❖W § 20 ust. 2 wskazano warunki jakie powinno zapewnić kierownictwo podmiotu publicznego w zakresie realizacji systemu zarządzania bezpieczeństwem informacji.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Zarządzanie bezpieczeństwem informacji w polskich aktach prawnych:

Za spełnienie wymagań rozporządzenia KRI uznaje się opracowanie systemu zarządzania bezpieczeństwem informacji na podstawie Polskiej Normy PN-ISO/IEC 27001, przy jednoczesnym ustanawianiu zabezpieczeń, zarządzaniu ryzykiem oraz audytowaniu systemu na podstawie:

- ❖ PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń,
- ❖ PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem,
- ❖ PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

❖SZBI opiera się na zabezpieczeniach proceduralno-prawnych, fizycznych i informatycznych, świadomości pracowników oraz posiadanych aktywach: informacje, sprzęt, zasoby ludzkie, infrastruktura, itd.

❖Norma PN-ISO/IEC 27001 określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji z uwzględnieniem uwarunkowań, w których działa Podmiot. Wymagania mają charakter ogólny i są przeznaczone do stosowania w podmiocie każdego rodzaju, wielkości czy charakteru.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Zarządzanie bezpieczeństwem informacji w polskich aktach prawnych:

Norma PN-ISO 31000. Zarządzanie ryzykiem. Zasady i wytyczne. Wprowadzona w 2009 r. norma ISO 31000 jest przede wszystkim zbiorem ram, procesów i zasad, których należy przestrzegać przy wdrażaniu procesu oceny ryzyka w każdej organizacji. Norma ta wskazuje, że każda ocena ryzyka, nieważne, czy dotycząca bezpieczeństwa informacji, ryzyka finansowego czy innego obszaru, powinna kierować się zaleceniami nowej normy – przy założeniu, że głównym celem ISO 31000 nie jest zamiana wymagań innych standardów, lecz ujednolicenie w nich procesów zarządzania ryzykiem.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Zarządzanie bezpieczeństwem informacji na przykładzie HIPAA:

HIPAA (Health Insurance Portability and Accountability Act) to amerykańskie prawo regulujące ochronę danych osobowych pacjentów oraz normy dotyczące bezpieczeństwa informacji w sektorze opieki zdrowotnej. HIPAA nakłada na organizacje medyczne i wszystkie podmioty przetwarzające dane zdrowotne szereg wymogów dotyczących bezpieczeństwa, prywatności i standaryzacji przepływu informacji medycznych. Jednym z kluczowych aspektów HIPAA jest konieczność szacowania ryzyka związanego z bezpieczeństwem informacji w sektorze opieki zdrowotnej. W kontekście HIPAA szacowanie ryzyka jest procesem, który ma na celu identyfikację, ocenę i zarządzanie potencjalnymi zagrożeniami dla bezpieczeństwa danych zdrowotnych pacjentów.

Podmioty objęte przepisami HIPAA, takie jak szpitale, przychodnie, **uczelnie medyczne** czy dostawcy usług medycznych, są zobowiązane do przeprowadzania regularnych audytów bezpieczeństwa, w tym szacowania ryzyka, aby zapewnić zgodność z wymaganiami prawnymi i chronić poufność danych zdrowotnych pacjentów.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Zarządzanie bezpieczeństwem informacji na przykładzie HIPAA:

Proces szacowania ryzyka w kontekście HIPAA obejmuje następujące kroki:
Identyfikacja zagrożeń: Ocena potencjalnych zagrożeń dla danych zdrowotnych, takich jak ataki hakerskie, kradzież danych, błędy ludzkie, awarie systemów itp.
Ocena ryzyka: Określenie prawdopodobieństwa wystąpienia zagrożeń oraz skutków, jakie mogą się pojawić w przypadku naruszenia bezpieczeństwa danych zdrowotnych.
Zarządzanie ryzykiem: Opracowanie strategii i działań mających na celu minimalizację ryzyka, które obejmuje stosowanie odpowiednich zabezpieczeń technicznych, polityk i procedur w celu ochrony danych zdrowotnych.
Monitorowanie i aktualizacja: Proces szacowania ryzyka w ramach HIPAA nie jest statyczny i wymaga regularnego monitorowania, oceny i aktualizacji. To pozwala na dostosowanie zabezpieczeń do zmieniających się zagrożeń i środowiska informatycznego.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Mechanizm szacowania ryzyka:

1) Pierwszym krokiem do wdrożenia systemu zarządzania bezpieczeństwem informacji jest zidentyfikowanie: informacji, zagrożeń występujących w organizacji i aktywów, które są bezpośrednio lub pośrednio związane z obiegiem informacji.
2) Kolejnym etapem szacowania ryzyka jest wartościowanie informacji i przypisanie im właścicieli.
3) Kolejnym etapem jest identyfikacja i analiza zagrożeń.
4) Ostatecznym efektem jest ocena ryzyka, na podstawie której można określić odpowiednie plany zarządzania ryzykiem w celu zminimalizowania istniejącego ryzyka do akceptowalnego poziomu. W ramach analizy ryzyka należy ocenić jakie informacje ma w swoich zasobach podmiot, jakim ryzykiem obarczone jest przetwarzanie informacji w tych zbiorach, by następnie wdrożyć mechanizmy zapobiegające wystąpieniu tych ryzyk.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Identyfikowanie ryzyka:

Identyfikowanie ryzyka to kluczowy krok w zarządzaniu ryzykiem, niezależnie od branży czy dziedziny. Obejmuje ono proces identyfikacji potencjalnych zagrożeń, szans na wystąpienie niepożądanych zdarzeń oraz konsekwencji, jakie mogą wyniknąć z tych zdarzeń. Proces ten może być realizowany na różnych poziomach, w różnych obszarach i dla różnych celów.

Identyfikowanie ryzyka w szkołach wyższych pozwala na zrozumienie potencjalnych zagrożeń, co umożliwia podejmowanie działań zapobiegawczych, minimalizujących ryzyko i zapewniających bezpieczeństwo instytucji oraz jej interesariuszy. To kluczowy element skutecznego zarządzania instytucją edukacyjną.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Identyfikowanie ryzyka:

Rozpoznanie potencjalnych zagrożeń: Zidentyfikowanie i zrozumienie różnych rodzajów zagrożeń, które mogą mieć wpływ na działalność, projekt czy organizację. Zagrożenia mogą być związane z technologią, ludźmi, procesami, środowiskiem czy zewnętrznymi czynnikami.
Analiza przyczyn i skutków: Zrozumienie, jakie czynniki mogą prowadzić do pojawienia się zagrożeń oraz jakie mogą być skutki tych zagrożeń. Warto ocenić, jakie konsekwencje będą mieć dla organizacji czy projektu.
Identyfikacja aktywów: Określenie i zrozumienie wartościowych aktywów, które mogą być zagrożone. Mogą to być dane, zasoby finansowe, technologie, ludzie czy wizerunek np. szkoły wyższej.
Wykorzystanie różnych metod identyfikacji ryzyka: Istnieje wiele metod identyfikacji ryzyka, takich jak analiza SWOT, analiza scenariuszy, techniki braistormingu czy mapowanie ryzyka.
Zbieranie informacji od interesariuszy: Włączenie osób z różnych dziedzin, departamentów czy zewnętrznych ekspertów do identyfikacji ryzyka może dostarczyć szerokiej gamy perspektyw i punktów widzenia.
Tworzenie katalogu ryzyka: Zbieranie identyfikowanych zagrożeń w spójny katalog, który może służyć jako baza do dalszej analizy, oceny i zarządzania ryzykiem.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Identyfikowanie ryzyka w szkołach wyższych (kluczowe obszary):

Szkoły wyższe mogą być narażone na różnorodne ryzyka, w tym związane z bezpieczeństwem informatycznym, zarządzaniem danymi, aspektami finansowymi, zarządzaniem kadrami, reputacją instytucji czy też zagrożeniami zewnętrznymi.

- **Analiza zagrożeń związanych z bezpieczeństwem informatycznym:** Uczelnie gromadzą dane osobowe, dane badawcze i inne dane nieosobowe.
- **Ocena ryzyka związanego z zarządzaniem danymi:** Przechowywanie i zarządzanie danymi studentów, pracowników i innych interesariuszy wymaga uwzględnienia ryzyka związanego z prywatnością, zgodnością z przepisami dotyczącymi ochrony danych osobowych oraz możliwością utraty lub kradzieży danych.
- **Ocena ryzyka reputacji:** Zachowanie dobrej reputacji szkoły wyższej jest kluczowe. W związku z tym, identyfikowanie ryzyka związanego z incydentami, które mogą wpłynąć na wizerunek szkoły, jest istotne (informacje o wyciekach danych, informacje o kradzieży laptopa z danymi osobowymi).
- **Analiza zagrożeń związanych z bezpieczeństwem fizycznym:** Zapewnienie bezpieczeństwa na terenie kampusu, zarządzanie zagrożeniami związanymi z wypadkami, incydentami bezpieczeństwa publicznego czy też incydentami medycznymi.
- **Konsultacje z zespołem zarządzającym ryzykiem:** Utworzenie zespołu lub komitetu ds. zarządzania ryzykiem, który będzie odpowiedzialny za identyfikowanie, analizę i monitorowanie ryzyka.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Wnioski:

❖Proces identyfikowania ryzyka i jego oszacowanie jest **składową procesu podejmowania decyzji, ułatwiającą** kierującym podejmowanie świadomych i właściwych wyborów, ustalenia priorytetów działań oraz rozpoznawania alternatywnych kierunków działań w przypadku zaistniałych zagrożeń, zdarzeń i sytuacji kryzysowych

❖ Szacowanie **ryzyka to proces dlatego powinien być dynamiczny, powtarzalny oraz zdolny reagować na zmiany, ponieważ wewnętrzne i zewnętrzne ryzyka zmieniają się, pojawiają** się nowe ryzyka, a niektóre zanikają.

❖Idea podejścia opartego na ryzyku polega na tym, że **ryzykiem najlepiej zarządza ten kto je zna**. Ważne aby skład zespołu ds. szacowania ryzyka bezpieczeństwa informacji obejmował przedstawicieli wszystkich obszarów podmiotu (m.in. pełnomocnik ds. systemu zarządzani jakością, dyrektorzy, kierownicy działów, pracownik kadr, kierownik biura zarządu, administrator sieci, itp.). Praca w tak zbudowanym zespole umożliwiła objęcie wszystkich procesów realizowanych w organizacji związanych z tematem bezpieczeństwa informacji.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Wykorzystane źródła:

D. Wróblewski (red.), Zarządzanie ryzykiem – przegląd wybranych metodyk, Józefów 2015;
M. Ganczar, Zarządzanie bezpieczeństwem informacji a cyberbezpieczeństwo w podmiotach publicznych, [w:] G. Szpor, A. Gryszczyńska (red.), Cyberpandemia, Warszawa 2020;
William N. LaForge, Campus Governance in U.S. Universities and Colleges, Review of European and Comparative Law, VOLUME XLII
YEAR 2020, ISSUE 3, pp. 113-140.

„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625