Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 355 · 2018

Informatyka i Ekonometria 13

**Jacek Jakieła**

Politechnika Rzeszowska
Wydział Budowy Maszyn i Lotnictwa
jjakiela@prz.edu.pl

**Joanna Wójcik**

Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie
Wydział Informatyki Stosowanej
jwojcik@wsiz.rzeszow.pl

# PRZEGLĄD PROBLEMÓW BEZPIECZEŃSTWA INFORMACJI ORAZ PRYWATNOŚCI W AKADEMICKIM NAUCZANIU NA ODLEGŁOŚĆ

**Streszczenie:** Platformy nauczania na odległość stały się istotnym elementem propozycji wartości współczesnych uczelni wyższych. Dzięki wykorzystaniu platform zdalnego nauczania można znacząco uatrakcyjnić materiały dydaktyczne, dostosować tempo przyswajania wiedzy do indywidualnych możliwości studentów oraz ciągle udoskonalać proces kształcenia. Do tej pory rozwój tego typu przedsięwzięć skupiał się przede wszystkim na opracowywaniu atrakcyjnych treści, zgodnych z wypracowanymi przez branżę standardami. Często zaniedbywano aspekty bezpieczeństwa informacji i prywatności użytkowników. Wpływa to negatywnie na wykorzystanie przez użytkowników pełnych możliwości platformy i znacznie ogranicza liczbę reakcji sprzężenia zwrotnego. To z kolei stanowi barierę dla prowadzenia szeroko zakrojonych analiz, dzięki którym można podnosić jakość kształcenia. Artykuł prezentuje analizę i krytykę piśmiennictwa dotyczącego tworzenia polityki bezpieczeństwa informacji i prywatności dla rozwiązań nauczania na odległość oraz wskazuje możliwe kierunki działań w tym zakresie.

**Słowa kluczowe:** bezpieczeństwo informacji, prywatność, nauczanie na odległość, polityka bezpieczeństwa.

**JEL Classification:** I210, M15.

## Wprowadzenie

Nauczanie na odległość stało się w polskich uczelniach wyższych powszechną praktyką. W zasadzie każda z polskich uczelni prowadzi obecnie nauczanie w modelu hybrydowym (*blended-learning*), w pełni udostępniając online treści wybranych przedmiotów lub traktując e-learning jako uzupełnienie oferty tradycyjnej. W większości przypadków nauczyciele akademiccy i studenci ko-

rzystają z nauczania na odległość dobrowolnie. Niestety wysokie koszty tworzenia atrakcyjnych, interaktywnych treści oraz zarządzania procesem nauczania na odległość powodują, że kwestie bezpieczeństwa informacji oraz prywatności, które wymagają kolejnych inwestycji, schodzą na dalszy plan. Celem niniejszego artykułu jest krytyczna analiza piśmiennictwa dotyczącego bezpieczeństwa systemów e-learningowych (a nie ogólnie systemów informacyjnych zarządzania) oraz sformułowanie docelowego wzorca zachowania szkół wyższych w zakresie bezpieczeństwa i prywatności użytkowników tychże systemów.

Edgar Weippl, autor jedynej jak do tej pory monografii dedykowanej bezpieczeństwu systemów e-learningowym, podkreśla trzy podstawowe cechy nauczania na odległość, z którymi związane są zagrożenia dla bezpieczeństwa. Są to [Weippl, 2005, s. 9-11]:

1. Zakres (*scope*) – przygotowanie kursów e-learningowych wiąże się z większą czasochłonnością niż uruchomienie zajęć tradycyjnych.
2. Współzależność (*interdependence*) – tworzenie kursów e-learningowych wymaga zaangażowania dużej liczby osób (autorzy merytoryczni, techniczni, metodycy zdalnego nauczania, testerzy) i jest traktowane jako projekt z określonym czasem i budżetem.
3. Globalny zasięg (*global reach*) – kursy są tworzone z zamiarem ich dostarczenia do coraz większej liczby osób, nieraz nawet na rynek międzynarodowy, jak to ma miejsce w przypadku masowych otwartych kursów online (*massive open online courses*), co sprawia, że trudniej jest chronić poufne treści oraz tożsamość użytkowników platformy.

Autorskie kursy oraz uczelniane platformy nauczania na odległość powinny być traktowane jako zasób wiedzy uczelni, stanowiący istotny element propozycji wartości w ramach ich oferty dydaktycznej. Współcześni użytkownicy systemów e-learningowych, określani terminami „cyfrowi tubylcy" oraz „cyfrowi emigranci", mają dobrze sprecyzowane oczekiwania wobec środowisk zdalnego nauczania. Oczekiwania te, oprócz użyteczności, dotyczą również takich aspektów, jak bezpieczeństwo i ochrona danych osobowych [Bandara, Ioras, Maher, 2014, s. 728]. Oznacza to, że każda z uczelni powinna w sposób krytyczny przyjrzeć się polityce bezpieczeństwa w zakresie nauczania na odległość, oczywiście o ile taka polityka została utworzona.

Wyniki badań bibliometrycznych przeprowadzonych przez H. Batorowską [2017, s. 9-28], w których analizie poddano 479 rekordów z bazy Katalogu Biblioteki Narodowej oraz 1053 artykuły z lat 2002-2017 z konferencji „Edukacja XXI wieku" organizowanej przez Wyższą Szkołę Bezpieczeństwa z Poznania, pokazują duży wzrost zainteresowania zagadnieniami bezpieczeństwa informa-

cyjnego. Dotyczy to głównie rozwiązań IT, gdzie najczęściej poruszane są tematy systemów teleinformatycznych, infrastruktury teleinformatycznej, jej obsługi i eksploatacji oraz technicznych aspektów bezpieczeństwa danych.

Artykuły poświęcone bezpieczeństwu informacji w zdalnym nauczaniu w zasadzie się nie pojawiają, a nieliczne dotyczą edukacji online, gdzie bezpieczeństwo jest tematem szkolenia. Dostępne w języku polskim opracowania, jak np. [Woźniak-Zapór, 2016, s. 87-97], mają formę studium przypadku i skupiają się na analizie możliwości zabezpieczenia informacji oraz technicznych środkach bezpieczeństwa platform e-learningowych. Brak opracowań w tym zakresie wskazuje na konieczność prowadzenia badań w kierunku bezpieczeństwa informacji i prywatności odbiorców treści dydaktycznych w modelu zdalnego nauczania.

Wydaje się, że niedocenianie problemów bezpieczeństwa i prywatności w nauczaniu na odległość w polskich uczelniach związane jest z charakterem udostępnianych kursów. Często kursy e-learningowe przygotowywane są jedynie do przedmiotów dla studiów I stopnia o charakterze podstawowym, ponieważ może z nich skorzystać duża grupa studentów. Treści kursów i ich forma są elektroniczną kopią materiałów drukowanych, a tym samym problem ochrony tego typu zasobów staje się marginalny. Część uczelni udostępnia również materiały dydaktyczne w postaci Otwartych Zasobów Edukacyjnych, które z założenia powinny być współdzielone bez większych ograniczeń, zgodnie z ideą dzielenia się wiedzą. Regulacje prawne niepozwalające prowadzić studiów i egzaminować studentów w pełnym zakresie online istotnie wpływają na marginalizowanie kwestii bezpieczeństwa. W następnej sekcji artykułu poddano analizie główne role interesariuszy rozwiązań zdalnego nauczania oraz związane z nimi aspekty bezpieczeństwa i prywatności.

## 1. Interesariusze systemów zdalnego nauczania

Utworzenie kursów w modelu zdalnego nauczania i prowadzenie za ich pomocą dydaktyki wymaga zaangażowania wielu osób, które odgrywają w tych procesach dobrze zdefiniowane role. Są to osoby prowadzące nadzór pedagogiczny i wybierające kursy do wykonania, autorzy treści dydaktycznych, nauczyciele akademiccy realizujący szkolenia online, metodycy zdalnego nauczania, recenzenci treści, korektorzy, zespół techniczny – programiści, testerzy, specjaliści UX (*user experience*), oraz studenci. Z każdą z ról związane są istotne aspekty bezpieczeństwa informacji oraz prywatności, które sygnalizowane są przez obawy zgłaszane przez interesariuszy.

## 1.1. Autorzy treści

Główne obawy autorów kursów online związane z bezpieczeństwem to:

- rozpowszechnianie materiałów bez wiedzy ich autorów, co nie jest jedynie nieuzasadnionym podejrzeniem (wiele wartościowych blogów zostało zamkniętych z powodu bezprawnego powielania ich treści bez podania autora); analiza serwisów współdzielenia plików (*peer-to-peer*) pokazuje również dużą zawartość materiałów dydaktycznych, które są udostępniane bezprawnie, ponieważ prawa autorskie należą do uczelni,
- nieuprawnione modyfikacje treści i ich dalsze rozpowszechnianie jako materiałów oryginalnych,
- brak znajomości przepisów prawa autorskiego dzieł wytworzonych w trakcie związania umową o pracę (art. 12 Prawa autorskiego stanowi, że „pracodawca, którego pracownik stworzył utwór w wyniku wykonywania obowiązków ze stosunków pracy, nabywa z chwilą przyjęcia utworu autorskie prawa majątkowe w granicach wynikających z celu umowy o pracę i zgodnego zamiaru stron" [za: Prauzner, 2013, s. 41]) oraz zdarzające się po stronie autorów naruszenia tych przepisów, np. kopiowanie obrazów bezpośrednio z wyników wyszukiwarki Google,
- pominięcie danych twórcy na liście autorów materiałów, w przypadku opracowywania treści w zespole,
- niski poziom zaufania do technologii IT związanych ze zdalnym nauczaniem.

Jak wiadomo, w przypadku kursów online, które są produktami cyfrowymi, istnieje możliwość łatwego ich powielania. Wprawdzie nie ma możliwości pełnego zabezpieczenia kursu przez tego typu praktykami, ale należy podkreślić, że w przypadku bardziej interaktywnych kursów, z wieloma powiązaniami w zakresie treści, animacji czy modułów weryfikujących wiedzę (quizy, testy etc.), jest to mocno utrudnione – po skopiowaniu kurs nie działa w pełnym zakresie, a treści są wybrakowane. Najłatwiej jest powielać materiały w postaci prezentacji (np. Ms-PowerPoint), plików w formacie PDF czy obrazów, choć istnieją metody zabezpieczenia tych plików przed otwarciem, wydrukiem czy nieuprawnioną modyfikacją. Gdy nakład pracy związany z kopiowaniem treści jest zbyt duży, wówczas do powielania zazwyczaj nie dochodzi. Obawy autorów związane z nieuprawnionym kopiowaniem przygotowanych przez nich treści często manifestują się poprzez dodatkowe zabezpieczanie materiałów hasłami na poziomie plików i udostępnianie haseł studentom podczas zajęć. Jest to powszechna praktyka stosowana pomimo tego, że w większości przypadków kursy na platformie udostępniane są jedynie grupom, które i tak mają określony przedmiot związany z kursem przypisany w planach studiów.

## 1.2. Nauczyciele akademiccy

Główne obawy nauczycieli akademickich związane z bezpieczeństwem informacji i prywatnością dotyczą:

- rzeczywistej tożsamości studentów biorących udział w procesie weryfikacji wiedzy,
- samodzielności studentów przy opracowywaniu materiałów zaliczeniowych,
- bezpieczeństwa wystawianych na platformie ocen,
- możliwości podmiany wysłanych przez studentów prac,
- możliwości śledzenia i długookresowego przechowywania treści dyskusji, w przypadku kursów dotyczących umiejętności „miękkich", w których najistotniejsza jest interakcja student–nauczyciel, student–zespół,
- standaryzacji, która zmniejsza elastyczność nauczania, negatywnie wpływa na kreatywność i dynamiczne dostosowywanie treści dydaktycznych do możliwości studentów i grupy,
- nieuprawnionego dostępu do wrażliwych danych użytkowników platformy,
- kradzieży własności intelektualnej w przypadku wykorzystania platformy w charakterze repozytorium gromadzącego oryginalne wyniki pracy,
- kontroli i możliwej ingerencji przełożonych w proces dydaktyczny.

Część obaw związana jest ściśle z aspektami technicznymi, jednak wiele z nich wymaga podjęcia działań systemowych, opracowania i wdrożenia w skali całej uczelni odpowiedniej strategii nauczania na odległość oraz wprowadzenia i egzekwowania przestrzegania dobrze zdefiniowanej polityki bezpieczeństwa.

## 1.3. Studenci

Studenci korzystający z platformy w dużej mierze wykonują jedynie konieczne do zaliczenia danego przedmiotu czynności z obawy przed:

- skopiowaniem swoich prac przez innych studentów,
- redukcją asymetrii informacji dotyczących ilości poświęcanego na naukę czasu, który może być monitorowany z wykorzystaniem statystyk gromadzonych na platformie (w przypadku tradycyjnych zajęć nie ma możliwości weryfikacji aktywności studenta poza salą wykładową),
- problemami technicznymi skutkującymi niemożnością przesłania pracy zaliczeniowej lub weryfikacji zdobytej wiedzy w terminach określonych przez harmonogram sesji egzaminacyjnej; tego typu problemy najczęściej wynikają z braku umiejętności w zakresie korzystania z funkcjonalności platformy nauczania na odległość,

– możliwością wykorzystania wypowiedzi w dyskusji w sposób nieuprawniony zarówno przez innych studentów, jak i nauczyciela,
– problemami z edycją wprowadzonej do systemu wypowiedzi,
– brakiem możliwości anonimowych wypowiedzi,
– długim przechowywaniem na platformie śladów działań lub przeciwnie, zbyt krótkim czasem gromadzenia danych, m.in. w przypadku tworzenia profilu elektronicznego, który zawiera np. portfolio zrealizowanych w trakcie studiów projektów i może być wykorzystany przy poszukiwaniu pracy.

Badania pokazują [May, George, 2011, s. 6], że w przypadku stosowania na platformie e-learningowej narzędzi do prowadzenia analiz treści dyskusji zarówno studenci, jak i prowadzący nie czują się pewnie i unikają pozostawiania śladów online. Brak mechanizmów związanych z zapewnieniem odpowiednio wysokiego poziomu prywatności użytkowników platformy oraz bezpieczeństwa informacji skutkuje brakiem możliwości wykorzystania statystyk na temat aktywności studentów w procesie ciągłego doskonalenia oferty dydaktycznej uczelni. Jest to poważny problem, ponieważ na jakości kształcenia powinno zależeć obydwu stronom – uczelni, jak również studentom.

### 1.4. Nadzór dydaktyczny

Osoby pełniące rolę nadzoru dydaktycznego to m.in. kierownicy katedr, dziekani i prodziekani oraz pracownicy administracyjni związani z realizacją procesu dydaktycznego. Główne pytania związane z bezpieczeństwem dotyczą następujących kwestii:
– Czy dostęp do kursów e-learningowych mają tylko uprawnieni użytkownicy?
– Czy można ufać tożsamości użytkowników platformy, zwłaszcza w sytuacji, gdy użytkownik pobiera za aktywności online określone świadczenia, np. stypendium naukowe, wynagrodzenie za prowadzenie zajęć online?
– Czy raporty tworzone na podstawie statystyk gromadzonych na platformie dotyczących studentów i nauczycieli akademickich nie zawierają błędów?

## 2. Systemy klasy LMS/LCMS a kwestie bezpieczeństwa oraz prywatności

LMS (*Learning Management System*) i LCMS (*Learning Content Management System*) to platformy, bez których niemożliwe byłoby nauczanie na odległość. Obecnie trudno jest precyzyjnie rozdzielić te kategorie systemów.

Większość stosowanych platform e-learningowych służy do administracji programami szkoleniowymi, zarządzania treściami, jak również może posiadać funkcjonalności związane z prowadzeniem wirtualnej klasy (*virtual classroom system*).

## 2.1. Charakterystyka danych zbieranych przez platformy zdalnego nauczania

Platformy e-learningowe dostarczają dużą liczbę szczegółowych charakterystyk opisujących zarówno wykorzystanie treści dydaktycznych, jak i aktywności użytkowników (tabela 1).

**Tabela 1.** Podstawowe statystyki zapisywane na platformie e-learningowej

| | **Podstawowe statystyki** |
|---|---|
| **Użytkownicy** | – godziny logowania,<br>– adres IP użytkownika,<br>– lokalizacja użytkownika,<br>– aktywność użytkownika w funkcji czasu,<br>– udział w dyskusjach na forum dyskusyjnym,<br>– udział w czacie |
| **Studenci** | – liczba uzyskanych punktów z testów,<br>– czas rozpoczęcia i zakończenia testu,<br>– liczba podejść do testu,<br>– przesłane prace zaliczeniowe,<br>– aktywność w dyskusjach (pomiędzy studentami, pomiędzy studentem a nauczycielem),<br>– status wypełnienia ankiety ewaluacyjnej |
| **Nauczyciele akademiccy** | – ilość zamieszczonych plików,<br>– ilość wystawionych ocen,<br>– liczba założonych wątków i udzielonych odpowiedzi w dyskusjach,<br>– czas reakcji na pytania skierowane przez studenta do prowadzącego |
| **Treści szkoleniowe** | – czas spędzony na przeglądaniu danego elementu kursu,<br>– pobrane pliki,<br>– ilość kliknięć w obszarze danego elementu kursu,<br>– procent realizacji efektu kształcenia związany z danych modułem kursu |

Źródło: Opracowanie własne.

Są to podstawowe statystyki zbierane przez większość platform nauczania na odległość. W przypadku niektórych uczelni stosowane są jeszcze bardziej zaawansowane rozwiązania, pozwalające na prowadzenie szeroko zakrojonej analityki. Dla przykładu, platforma Blackboard stosowana w Wyższej Szkole Informatyki i Zarządzania w Rzeszowie zawiera cztery moduły:

1. Moduł zarządzania kursami (*Course Delivery*) – oprócz standardowych zadań pozwala na projektowanie ścieżek nauczania, czyli dostarczanie różnych treści dla studentów, w zależności od ich wiedzy początkowej oraz poczynionych postępów. Pozwala również na tworzenie grup, z których każda może

dysponować swoją przestrzenią roboczą. Możliwa jest integracja platformy z narzędziami Web 2.0.

2. Moduł zarządzania treścią (*Content Management*) – umożliwia przechowywanie oraz wyszukiwanie dokumentów i plików opatrzonych metadanymi, tworzenie obiektów nauczania (*learning objects*) oraz definiowanie obiegu dokumentów (*workflow*).
3. Moduł oceny wyników (*Outcomes Assessment*) – umożliwia zbieranie danych i monitorowanie wyników studentów, grup roboczych, poziomu zaangażowania prowadzących zajęcia oraz automatyczną ocenę wyników kształcenia i wysyłanie ostrzeżeń w przypadku rezultatów, które znajdują się poniżej zdefiniowanego progu akceptacji.
4. Zarządzanie społecznością i poziomem zaangażowania członków społeczności (*Community Engagement*) – umożliwia tworzenie społeczności, kół zainteresowań oraz stron jednostek organizacyjnych uczelni. Pozwala na dostarczanie spersonalizowanych informacji i usług użytkownikom systemu w zależności od ich roli w systemie. Moduł zapewnia wirtualną przestrzeń dla pracowników i grup projektowych, gdzie użytkownicy mogą współdzielić zasoby, współpracować i wchodzić w interakcję. Pozwala również na tworzenie portfolio z prezentacją dokonań danej osoby lub jednostki organizacyjnej.

Przedstawione funkcjonalności, w połączeniu z danymi gromadzonymi na platformie oraz w systemach uczelni (przy założeniu pełnej integracji rozwiązań informatycznych wspierających zdalne nauczanie i działalność operacyjną uczelni, jak np. system dziekanatowy), pozwalają na tworzenie wyrafinowanych i szczegółowych raportów umożliwiających wgląd w procesy związane z dydaktyką, jej efektywnością i jakością całego procesu kształcenia.

Część administratorów uczelnianych platform e-learningowych dodatkowo posługuje się narzędziem Google Analytics, aby jeszcze dokładniej monitorować zachowania użytkowników (w szczególności w przypadku ogólnie dostępnych platform z otwartymi zasobami edukacyjnymi). Informacje, które można uzyskać, to: urządzenia, za pomocą których użytkownicy korzystają z platformy, ich zainteresowania, sposób dotarcia na stronę itp. Tworzone są również autorskie narzędzia wspierające pracę nauczycieli i pozwalające na bardziej zaawansowaną analitykę procesu nauczania. Coraz większym zainteresowaniem cieszą się narzędzia do analizy dyskusji oraz sieci społecznościowych, których opis można znaleźć w [Lockyer, Heathcote, Dawson, 2013, s. 1445].

Od początku nowego wieku dobrze widoczny jest trend dotyczący wzrostu ilości i intensywności badań w obszarach analityki akademickiej oraz analityki procesu nauczania [Van Barneveld, Arnold, Campbell, 2012, s. 1-11]. W związ-

ku z tym jest prawdopodobne, że w najbliższej przyszłości analizowane będą duże ilości danych pochodzących z różnych źródeł, dotyczących kandydatów na studia, studentów, pracowników uczelni oraz absolwentów. Z jednej strony pozwoli to na przygotowywanie lepiej dopasowanej do potrzeb odbiorców wysokiej jakości oferty dydaktycznej i usprawni procesy zarządzania uczelnią. Z drugiej strony tego typu działania staną się źródłem dużych wyzwań dla bezpieczeństwa informacji i prywatności użytkowników platform nauczania na odległość.

## 2.2. Bezpieczeństwo i prywatność w branżowych standardach e-learningowych

Organizacje zajmujące się standaryzacją zdalnego nauczania główny nacisk kładą na przygotowywanie specyfikacji protokołów komunikacji pomiędzy kursami e-learningowymi a platformą e-learningową oraz standardów tworzenia rozproszonych repozytoriów obiektów nauczania. Nie oznacza to, że kwestie prywatności i bezpieczeństwa informacji są całkowicie zaniedbywane, ale zapisy są formułowane ogólnikowo. Najbardziej rozbudowanym jest standard IEEE P1484, zawierający specyfikację prywatnych i publicznych informacji istotnych z punktu widzenia różnych interesariuszy systemu, w standardzie IMS LIP znajdują się ogólne informacje o prywatności, natomiast standardy AICC, ARIADNE, ADL-SCORM są przede wszystkim zorientowane na metadane [El-Khatib i in., 2003, s. 5-6]. W żadnym ze standardów nie wskazano na konkretne modele bezpieczeństwa oraz technologie.

Jedną z nielicznych prac dotyczących bezpieczeństwa informacji w platformach nauczania na odległość jest praca doktorska C.J. Eibla [2010, s. 78-82]. Opracowanie to zawiera wyniki analizy zagrożeń w zakresie bezpieczeństwa informacji i prywatności, która została przeprowadzona dla dwóch szeroko wykorzystywanych platform open-source: Moodle oraz Illias. Wyciągnięte w ramach analizy wnioski nie są zbyt optymistyczne. Co prawda na obu platformach zaimplementowane są mechanizmy zarządzania bezpieczeństwem oraz prywatnością, ale znaleziono wiele luk i słabych punktów ww. rozwiązań. W przypadku komercyjnych platform e-learningowych trudno jest określić ich poziom bezpieczeństwa, gdyż kod nie jest ogólnie dostępny. W związku z tym badania prowadzone w tym obszarze koncentrują się przede wszystkim na platformach otwartych.

## 3. Główne filary bezpieczeństwa systemów e-learningowych

Cztery podstawowe wymagania dotyczące bezpieczeństwa informacji i prywatności, w odniesieniu do platformy e-learningowej, to [Weippl, 2005, s. 6-7; Vasilescu, Tatar, Codreanu, 2011, s. 73]:

1. **Poufność** (*secrecy*) – użytkownicy mają dostęp jedyne do materiałów, do których zostaną im przydzielone prawa. Ponieważ większość platform e-learningowych na uczelni jest zintegrowanych z systemem dziekanatowym, studenci otrzymują dostęp do realizowanych w danym semestrze kursów, jak również do funkcjonalności ogólnie dostępnych (otwarte kursy, sekcja pomocy technicznej).
2. **Integralność** (*integrity*) – oznacza, że tylko uprawnieni użytkownicy i programy mogą dokonywać modyfikacji danych umieszczonych na platformie e-learningowej, a także konfiguracji platformy. Nieuprawnione modyfikacje materiałów dydaktycznych mogą skutkować przekazaniem do nauki niewłaściwych treści. Naruszenie integralności danych może nie być działaniem celowym i może wystąpić przez przypadek (np. modyfikacje i kopiowanie kursów bez konsultacji przez jedną z osób zarządzających treściami). Nie zmienia to jednak faktu, że system powinien być przed tym odpowiednio zabezpieczony.
3. **Dostępność** (*availabity*) – oznacza z jednej strony, że platforma e-learningowa powinna być dostępna dla wszystkich zainteresowanych, w zakresie praw, które posiadają, za pomocą posiadanego sprzętu elektronicznego, w tym urządzeń mobilnych, ale jednocześnie nie może być podatna na ataki hackerskie. Z drugiej strony, powinna być również odpowiednio zabezpieczona przed utratą danych oraz awariami sprzętu.
4. **Niezaprzeczalność** (*non-repudiation*) – oznacza brak możliwości usunięcia śladów działań podejmowanych na platformie e-learningowej, np. usunięcia pracy projektowej czy też egzaminu studenta przez nauczyciela lub podmiany oceny. W każdej z tych sytuacji powinna istnieć możliwość śledzenia logów platformy i określenia osoby, która wykonała daną czynność na platformie.

W odniesieniu do obecnej ustawy o ochronie danych osobowych każdy użytkownik platformy powinien mieć prawo dostępu do swoich danych oraz możliwość ich modyfikacji. Nie stoi to w sprzeczności z integralnością danych. W sytuacji, gdy użytkownik nie jest uprawniony do samodzielnej edycji, czynność tę może wykonywać administrator platformy [Lichy, Lipiński, 2014, s. 38].

## 4. Wymagania dotyczące polityki bezpieczeństwa

Biorąc pod uwagę przedstawione obawy poszczególnych interesariuszy systemów zdalnego nauczania, każda z uczelni powinna mieć opracowaną i wdrożoną politykę bezpieczeństwa, ciągle monitorowaną i udoskonalaną. Polityka bezpieczeństwa systemów e-learningowych powinna zawierać informacje o [Ferencz, Goldsmith, 1998, s. 7]:

- typach przechowywanych danych, celu ich przechowywania oraz danych osób mających do nich dostęp,
- miarach stosowanych do zagwarantowania poufności i integralności danych,
- minimalnej ilości zbieranych danych oraz czasie ich przechowywania,
- gwarancji użycia danych tylko w celach, w których były zbierane (dodatkowe użycie jedynie w niebudzących wątpliwości sytuacjach),
- zakazie rozpowszechniania danych poza uniwersytetem (w przypadku ujawniania danych partnerom outsourcingowym uzyskanie od nich zgody na stosowanie uczelnianej polityki bezpieczeństwa),
- sposobie dostępu do własnych danych oraz możliwości ich modyfikacji,
- sposobie audytu bezpieczeństwa systemu e-learningowego oraz
- działaniach edukacyjnych z zakresu bezpieczeństwa, prawie prywatności oraz określenie zachowania organizacji w sytuacji zagrożenia.

Ze względu na specyfikę systemów e-learningowych polityka bezpieczeństwa powinna zostać utworzona w odniesieniu do konkretnej, funkcjonującej na uczelni platformy e-learningowej. Powinna być również spójna z polityką bezpieczeństwa innych systemów informatycznych funkcjonujących w ramach uczelni, z którymi platforma współpracuje. Mając na uwadze wdrażaną w Polsce dyrektywę RODO, można stwierdzić, że każda uczelnia odpowiada za udowodnienie poszanowania zasad bezpieczeństwa i prywatności. Polityka bezpieczeństwa powinna być zaakceptowana przez kadrę zarządzającą uczelnią (retor, kanclerz, dziekani) oraz wszystkich pracowników, zarówno dydaktycznych, jak i administracyjnych. Ze względu na korzyści wynikające z analiz prowadzonych na podstawie danych pozyskanych z platformy oraz obawy ze strony studentów i pracowników uczelni należy (oprócz udostępnienia polityki bezpieczeństwa) poinformować każdorazowo studentów i nauczycieli akademickich przed przystąpieniem do wybranego kursu o:

- zależnościach pomiędzy częścią tradycyjną i zdalną, warunkach zaliczenia, sposobach konsultacji,
- zbieranych danych w tracie korzystania z kursu i ich wpływie na ocenę końcową,

– czasie przechowywania zarchiwizowanego kursu (np. w odniesieniu do możliwej kontroli Państwowej Komisji Akredytacyjnej kursy powinny być przechowywane 6 semestrów),
– możliwym wykorzystaniu danych do badań naukowych (o ile takie są planowane) [Wallace, 2007, s. 94].

Ważny jest również dobór rejestrowanych na platformie parametrów. Zamiast włączać śledzenie wszystkich możliwych charakterystyk w każdym z prowadzonych kursów, należy wybrać te, które są najważniejsze z punktu widzenia monitorowania oraz ulepszania procesu dydaktycznego.

## Podsumowanie

Dominujący obecnie trend uczenia się przez całe życie oraz zmiany w prawodawstwie (RODO) wymuszają wypracowanie odpowiedniego podejścia do kwestii bezpieczeństwa informacji i prywatności. W korporacjach, które mocno inwestują w kapitał ludzki, poprzez ciągły rozwój i szkolenia pracowników, kwestie bezpieczeństwa i prywatności brane są pod uwagę w szerszym zakresie [El-Khatib i in., 2003, s. 1-19]. Uczelnie wyższe również będą musiały zmierzyć się z tym problemem. Do tej pory większość działań dotyczyła głównie tworzenia innowacyjnych treści dydaktycznych, platform lub aplikacji wspierających nauczanie. W kolejnej fazie rozwoju, gdzie istotne stało się dostarczanie spersonalizowanych treści, tworzenie zaawansowanych, specjalistycznych kursów, traktowanie platformy e-learningowej jako systemu zarządzania wiedzą, przejście w stronę otwartych standardów czy też mobilność nauczania, rozwój rozwiązań stosowanych w ramach polityki bezpieczeństwa nabiera większego znaczenia [Zuev, 2012, s. 25; El-Khatib i in., 2003, s. 2].

Poziom zaufania do platformy e-learningowej jest istotny z perspektywy pełnego wykorzystania potencjału zdalnego nauczania [Kritzinger, Von Solms, 2006, s. 323]. Każda z uczelni oferujących zdalne nauczanie powinna przygotować, wdrożyć i ciągle ulepszać politykę bezpieczeństwa. Dzięki temu użytkownicy będą chętniej korzystali z tej formy kształcenia i dostarczali sprzężenie zwrotne, które jest niezbędne dla ciągłego podnoszenia jakości prowadzonej dydaktyki.

## Literatura

Bandara I., Ioras F., Maher I.K. (2014), *Cyber Security Concerns in E-learning Education* [w:] Proceedings of ICERI2014 Conference, Sewilla, 17-19.11.2014.

Barneveld Van A., Arnold K.E., Campbell J.P. (2012), *Analytics in Higher Education: Establishing a Common Language*, "EDUCAUSE Learning Initiative", No. 1(1), s. 1-11.

Batorowska H. (2017), *Bezpieczeństwo informacyjne w dyskursie naukowym – kierunki badań* [w:] H. Batorowska (red.), *Bezpieczeństwo informacyjne w dyskursie naukowym*, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Kraków, s. 9-28.

Eibl C.J. (2010), *Discussion of Information Security in E-learning*, praca doktorska, http://dokumentix.ub.uni-siegen.de/opus/volltexte/2010/444/pdf/eibl.pdf (dostęp: 23.12.2017).

El-Khatib K., Korba L., Xu Y., Yee G. (2003), *Privacy and Security in E-learning*, "International Journal of Distance Education Technologies (IJDET)", Vol. 1(4), s. 1-19.

Ferencz S.K., Goldsmith C.W. (1998), *Privacy Issues in a Virtual Learning Environment*, "Cause/Effect", Vol. 21(1), s. 5-11.

Kritzinger E., Solms Von S.H. (2006), *E-learning: Incorporating Information Security Governance*, "Issues in Informing Science & Information Technology", Vol. 3, s. 319.

Lichy K., Lipiński P. (2014), *E-Learning a ustawa o ochronie danych osobowych*, „Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej", Vol. 37, s. 37-40.

Lockyer L., Heathcote E., Dawson S. (2013), *Informing Pedagogical Action: Aligning Learning Analytics with Learning Design*, "American Behavioral Scientist", Vol. 57(10), s. 1439-1459.

May M., George S. (2011), *Privacy Concerns in E-learning: Is Using Tracking System a Threat?* "International Journal of Information and Education Technology", Vol. 1(1), s. 1-8.

Prauzner T. (2013), *Tworzenie treści dydaktycznych w kształceniu e-learningowym w aspekcie prawnym*, "EduAkcja. Magazyn Edukacji Elektronicznej", nr 2(6), s. 38-43.

Vasilescu C., Tatar L., Codreanu A. (2011), *Integrating Information Security in an E-learning Environment*, "eLearning & Software for Education", Vol. 2, s. 70-75.

Wallace L. (2007), *Online Teaching and University Policy: Investigating the Disconnect*, "International Journal of E-Learning & Distance Education", Vol. 22(1), s. 87-100.

Weippl E.R. (2005), *Security in E-Learning*, Vol. 16, Advances in Information Security, Springer Science & Business Media, Berlin.

Woźniak-Zapór M. (2016), *Zarządzanie bezpieczeństwem informacji – metody przeciwdziałania zagrożeniom bezpieczeństwa informacji na platformie e-learningowej*, „Bezpieczeństwo. Teoria i Praktyka", nr 4(XXV), s. 87-98.

Zuev V.I. (2012), *E-learning Security Models*, "Management Information Systems", Vol. 7(2), s. 024-028.

## A REVIEW OF INFORMATION SECURITY AND PRIVACY ISSUES IN ACADEMIC DISTANCE LEARNING ENVIRONMENT

**Summary:** The contemporary universities use distance learning platforms as an integral ingredient of their value proposition. These solutions can make educational stuff significantly more attractive, adjust the pace of learning and the content to individual students needs and capabilities and enable to constantly improve the university educational processes. So far, the development process of distance learning systems has been focused on improvement of electronic educational materials that comply with distance learning domain standards. Unfortunately to often the issues of information security and users privacy have been neglected. It negatively affects the full usage of platform functionalities by users and constrains the amount of feedback collected by universities. This impact creates the barriers for analytics that can be the driver for improving the quality of education processes. The paper presents the aspects important from the perspective of information security and privacy policy development for distance learning platforms and points to possible courses of action in this area.

**Keywords:** information security, privacy, distance learning, security policy.