



**Wydział Elektroniki
i Technik Informatycznych**

POLITECHNIKA WARSZAWSKA

**Program studiów
na kierunku
Cyberbezpieczeństwo**

**studia stacjonarne
I stopnia
o profilu ogólnoakademickim**

grudzień 2018 r.

Zadanie 14 - *Nowoczesne kształcenie w zakresie bezpieczeństwa teleinformatycznego na nowym kierunku Cyberbezpieczeństwo na studiach I stopnia*, realizowane w ramach projektu „NERW PW. Nauka – Edukacja – Rozwój – Współpraca”, współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego



**Fundusze
Europejskie**
Wiedza Edukacja Rozwój

**Politechnika
Warszawska**

Unia Europejska
Europejski Fundusz Społeczny



I. WPROWADZENIE

Zapewnienie bezpieczeństwa teleinformatycznego – bezpieczeństwa działania systemów komputerowych i sieci teleinformatycznych w warunkach różnego typu zagrożeń, których skala rośnie wraz z upowszechnieniem urządzeń mobilnych, ma obecnie krytyczne znaczenie dla funkcjonowania różnych gałęzi gospodarki i administracji państwa, a także dla zapewnienia bezpieczeństwa użytkowników sieci publicznych.

Znajduje to odzwierciedlenie w ofercie szkół wyższych w różnych krajach. W raporcie „2014 Best Schools for Cybersecurity”, opublikowanym przez Ponemon Institute¹, można znaleźć ranking najlepszych programów studiów w zakresie „cybersecurity”, prowadzonych w uczelniach amerykańskich. Bardziej interesująca niż sam ranking jest jednak informacja, że wyboru dokonano spośród 183 takich programów.

Choć na rodzimym rynku pracy odczuwany jest wyraźny brak specjalistów w zakresie cyberbezpieczeństwa (bezpieczeństwa teleinformatycznego), artykułowany przez przedstawicieli różnych instytucji publicznych i podmiotów gospodarczych, możliwości zdobycia wiedzy i umiejętności w tym zakresie, oferowane przez polskie uczelnie, a w szczególności przez Politechnikę Warszawską, są dość skromne.

W roku akademickim 2017/2018 na Wydziale Elektroniki i Technik Informacyjnych PW uruchomiono w ramach studiów II stopnia na kierunku *Telekomunikacja* specjalność *Teleinformatyka i Cyberbezpieczeństwo*. W ofercie Wydziału znajdują się też cieszące się dużym zainteresowaniem studia podyplomowe *Ochrona informacji w sieciach i systemach teleinformatycznych: projektowanie i audyt zabezpieczeń* oraz *Bezpieczeństwo Systemów Informacyjnych wraz z Technikami Biometrycznymi*. Prowadzone są liczne projekty badawcze w tym zakresie, w szczególności w utworzonym w 2015 r. w Instytucie Telekomunikacji PW Zakładzie Cyberbezpieczeństwa.

Brak w ofercie Politechniki Warszawskiej programu studiów I stopnia, który zarówno w swej nazwie, jak i zawartości merytorycznej odnosiłby się do problematyki cyberbezpieczeństwa, przy potencjale umożliwiającym stworzenie i realizację takiego programu, wydaje się być oznaką nie dość szybkiego reagowania na zmiany w otoczeniu społeczno-gospodarczym (w rozumieniu globalnym, ale także lokalnym). Inicjatywa uruchomienia studiów na kierunku *Cyberbezpieczeństwo* zmierza do uzupełnienia tego deficytu i wypełnienia przez Uczelnię luki w podaży pożądaných usług edukacyjnych.

Program studiów I stopnia na kierunku *Cyberbezpieczeństwo* opracowano w ramach realizacji projektu Nauka – Edukacja – Rozwój – Współpraca (NERW PW), finansowanego z Programu Operacyjnego Wiedza Edukacja Rozwój.

Przedłożona dokumentacja tych studiów została sporządzona z uwzględnieniem:

- przepisów ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce i związanych z nią rozporządzeń,
- wymagań określonych w uchwałach Senatu PW: 366/XLVII/2011, 210/XLVIII/2014, 334/XLVIII/2015, 49/XLIXI/2017 oraz 83/XLIXI/2017, z modyfikacjami wynikającymi z przepisów ww. ustawy i związanych z nią rozporządzeń.

¹ 2014 Best Schools for Cybersecurity, Ponemon Institute Research Report, Ponemon Institute LLC, February 2014.

II. OGÓLNA CHARAKTERYSTYKA STUDIÓW

1. NAZWA KIERUNKU STUDIÓW

Cyberbezpieczeństwo
w języku angielskim: **Cybersecurity**

2. POZIOM STUDIÓW/KSZTAŁCENIA

studia I stopnia

3. PROFIL STUDIÓW/KSZTAŁCENIA

ogólnoakademicki

4. FORMA STUDIÓW

studia stacjonarne

5. TYTUŁ ZAWODOWY UZYSKIWANY PRZEZ ABSOLWENTA

inżynier
w języku angielskim: **Bachelor of Science**

6. PRZYPORZĄDKOWANIE DO OBSZARU/OBSZARÓW KSZTAŁCENIA

nie dotyczy (zgodnie z przepisami ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce)

7. WSKAZANIE DZIEDZIN NAUKI I DYSCYPLIN NAUKOWYCH, DO KTÓRYCH ODNOSZĄ SIĘ EFEKTY UCZENIA SIĘ/EFEKTY KSZTAŁCENIA

dziedzina: **dziedzina nauk inżynieryjno-technicznych**
dyscyplina: **informatyka techniczna i telekomunikacja**

8. ZWIĄZEK Z MISJĄ UCZELNI I STRATEGIĄ JEJ ROZWOJU

Przedstawiona propozycja programowa jest zgodna z misją i wizją rozwoju Politechniki Warszawskiej, zawartą w jej strategii rozwoju². Elementem tej wizji jest bowiem dążenie do tego, aby Politechnika Warszawska była uczelnią, która jest krajowym liderem wprowadzania innowacji programowych i metodycznych w procesie kształcenia.

Propozycja ta wpisuje się też w realizację nadrzędnego celu rozwoju PW, zdefiniowanego w *Strategii* jako „kształcenie służące przygotowaniu wysoko wykwalifikowanej kadry o kompetencjach/umiejętnościach odpowiadających aktualnym i przewidywanym w przyszłości potrzebom społecznym i gospodarczym”, m.in. przez:

- poprawę stopnia dopasowania kompetencji absolwentów do potrzeb gospodarczych i społecznych oraz kształtowanie tych potrzeb (CO K1.2),
- dostosowanie wymagań programowych do standardów międzynarodowych (CO K2.2),
- stworzenie studentom możliwie najlepszych warunków do studiowania, w wyniku m.in. zwiększenia wkładu studentów w kształtowanie programu i procesu dydaktycznego oraz stosowania nowoczesnych, efektywnych metod, technik i narzędzi kształcenia, a w szczególności zastępowania tradycyjnych form nauczania,

² *Strategia Rozwoju Politechniki Warszawskiej do roku 2020*, Warszawa 2011

opartych na przekazywaniu wiedzy (wykłady), bardziej efektywnymi metodami, kładącymi nacisk na aktywność studenta, takimi jak nauczanie zorientowane na rozwiązywanie problemów i realizację projektów (CO K2.4).

W *Strategii* wskazano, że działania prowadzące do osiągnięcia celu CO K1.2 powinny obejmować m.in.

- współdziałanie Uczelni przy podejmowaniu kluczowych decyzji dotyczących funkcjonowania i rozwoju systemu kształcenia na Uczelni, jak również w ramach bieżącej działalności związanej z tworzeniem oferty dydaktycznej oraz projektowaniem i realizacją procesu kształcenia,
- kształtowanie potrzeb społecznych w wyniku wprowadzania programów studiów i innych form kształcenia dotyczących tematyki, która w przyszłości powinna być istotna dla rozwoju społeczeństwa i gospodarki opartej na wiedzy, co właśnie ma miejsce w przypadku inicjatywy związanej z uruchomieniem studiów na kierunku *Cyberbezpieczeństwo*.

Inicjatywa uruchomienia studiów na kierunku *Cyberbezpieczeństwo* może być również traktowane jako forma realizacji postanowień zawartych w podpisanych na poziomie Uczelni porozumieniach z NCK (Narodowe Centrum Kryptologii) i ABW (Agencja Bezpieczeństwa Wewnętrznego).

Uruchomienie kształcenia na kierunku *Cyberbezpieczeństwo* jest także zgodne ze strategią rozwoju Wydziału³, w której zapisano podobne jak w przypadku Uczelni cele, a mianowicie:

- CS K1. Dostosowanie oferty edukacyjnej wydziału do potrzeb gospodarczych i społecznych,
- CO K1.1. Unowocześnienie i zracjonalizowanie oferty studiów,
- CO K1.2. Poprawa stopnia dopasowania kompetencji absolwentów do potrzeb gospodarczych i społecznych oraz kształtowanie tych potrzeb.

Podsumowując, inicjatywa uruchomienia studiów I stopnia na kierunku *Cyberbezpieczeństwo* stanowi istotny – m.in. z punktu widzenia wizerunkowego – krok w kierunku unowocześnienia i uatrakcyjnienia oferty kształcenia na Politechnice Warszawskiej, a zwłaszcza poprawy stopnia jej dopasowania do potrzeb nowoczesnego społeczeństwa, którego funkcjonowanie jest w sposób krytyczny uzależnione od sprawności infrastruktury teleinformatycznej.

9. OGÓLNE CELE KSZTAŁCENIA ORAZ MOŻLIWOŚCI ZATRUDNIENIA (TYPOWE MIEJSCA PRACY) I KONTYNUACJI KSZTAŁCENIA PRZEZ ABSOLWENTÓW

Absolwent ma ogólną wiedzę i umiejętności, m.in. z zakresu matematyki, informatyki technicznej i telekomunikacji, niezbędne do kształtowania specjalistycznych kompetencji w zakresie cyberbezpieczeństwa oraz umożliwiające pogłębianie i uzupełnianie tych kompetencji wraz z rozwojem technologii i innymi zmianami zachodzącymi w sferze gospodarczo-społecznej.

Potrafi wykorzystać nabyte kompetencje do formułowania i rozwiązywania złożonych i nietypowych problemów z zakresu cyberbezpieczeństwa, a w szczególności zadań dotyczących:

- wykorzystywania informacji pochodzących z różnych źródeł do identyfikowania i analizowania podatności i zagrożeń dla bezpieczeństwa danych, systemów informacyjnych i sieci teleinformatycznych,

³ *Strategia rozwoju WEiTI do roku 2020*, Warszawa 2012.

- projektowania, realizowania, testowania i utrzymania infrastruktury (sprzętu i oprogramowania) służącej zapewnieniu bezpieczeństwa systemów i sieci teleinformatycznych,
- reagowania na sytuacje wymagające interwencji w celu przeciwdziałania zaistniałym lub spodziewanym atakom, stwarzającym zagrożenie dla bezpieczeństwa systemów i sieci teleinformatycznych, w sposób minimalizujący skutki tych ataków.

Posiadając także wiedzę z zakresu zagadnień ogólnospołecznych (m.in. prawa, zarządzania, socjologii, etyki) oraz umiejętności interpersonalne, potrafi współpracować z osobami odpowiedzialnymi za bezpieczeństwo funkcjonowania dużych instytucji i organizacji oraz infrastruktury krytycznej państwa.

Zestaw kompetencji absolwenta (efektów uczenia się) oraz program studiów prowadzący do uzyskania tych kompetencji określono m.in. na podstawie raportu *National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework*, NIST (USA), 2017, z uwzględnieniem uwag przekazanych przez przedstawicieli kilkunastu instytucji zainteresowanych zatrudnieniem osób posiadających tę kwalifikację, reprezentujących instytucje administracji centralnej, instytucje finansowe, firmy informatyczne i operatorów sieci telekomunikacyjnych.

Absolwent jest przygotowany do pracy w firmach tworzących rozwiązania informatyczne (sprzęt i oprogramowanie) o odpowiednim poziomie bezpieczeństwa oraz specjalistyczne rozwiązania służące zapewnieniu bezpieczeństwa systemów i sieci teleinformatycznych. Może też pracować w firmach/instytucjach o różnym profilu działalności, wykorzystujących nowoczesne rozwiązania informatyczne, w szczególności – w instytucjach sektora finansowego, administracji publicznej, a także w instytucjach zajmujących się różnymi aspektami bezpieczeństwa państwa.

Planowane jest stworzenie absolwentom możliwości kontynuacji kształcenia na studiach II stopnia i zdobycia tytułu zawodowego mgr inż. Dotyczy to osób, które uzyskają tytuł zawodowy inżyniera w roku 2022 lub później.

w języku angielskim:

The graduate has basic knowledge and skills in mathematics, computer engineering and telecommunications, necessary to develop specialised competencies in cybersecurity and to upgrade these competencies as technology progresses and socioeconomic changes take place.

He/she is able to use these competencies to identify and solve a spectrum of complex and non-trivial cybersecurity related problems, in particular:

- to use information collected from a variety of sources to identify and analyze vulnerabilities and threats for security of data, information systems, and computer networks,
- to design, implement, test and maintain the infrastructure (hardware and software) required to effectively provide information systems and computer networks with a required level of security,
- to react to urgent situations in order to mitigate immediate and potential threats/attacks on the security of information systems and computer networks so that to minimise the consequences of these attacks.

Having also non-technical knowledge (law, management, sociology, ethics) and interpersonal competences, he/she is able to cooperate with people responsible for security of large institutions/organisations and critical infrastructure of the country.

The intended competencies (learning outcomes) of the graduate and the curriculum intended to achieve these competencies have been developed based, inter alia, on report

National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework, NIST (USA), 2017, and comments submitted by representatives of ca. 15 institutions interested in hiring the graduates (institutions of central administration, financial institutions, ICT companies, and telecom operators).

The diploma holder can work for companies that develop and implement reliable hardware and software solutions or specialised solutions that provide information systems and computer networks with a required level of security.

He/she can also work for various companies/institutions which rely on modern information and computer systems, in particular in financial service sector, public administration and institutions dealing with various aspects of national security.

From 2022, the BS programme graduates will be given an opportunity to continue studying towards a qualification at EQF level 7 (Master of Science in Cybersecurity).

10. WYMAGANIA WSTĘPNE

Nie ma wymagań formalnych, od kandydatów na studia oczekuje się jednak kompetencji analitycznych oraz gotowości do systematycznej pracy i samodzielnego zdobywania wiedzy i umiejętności.

11. ZASADY REKRUTACJI

Zasady ogólnie obowiązujące w PW – rekrutacja oparta na wynikach egzaminu maturalnego.

12. RÓŻNICE W STOSUNKU DO INNYCH PROGRAMÓW O PODOBNE ZDEFINIOWANYCH CELACH I EFEKTACH PROWADZONYCH W UCZELNI

W Politechnice Warszawskiej nie jest prowadzony program studiów I stopnia o podobnie zdefiniowanych celach i efektach. Wyróżniającą cechą opracowanego programu jest znaczny zasób wiedzy i umiejętności z zakresu cyberbezpieczeństwa, osiągniany przez studenta (absolwenta). Zasób ten kształtują:

- specjalistyczne przedmioty z zakresu cyberbezpieczeństwa, prowadzone w wymiarze 40 punktów ECTS,
- inne przedmioty, w których zagadnienia cyberbezpieczeństwa służą jako przykłady zastosowania metod o charakterze bardziej uniwersalnym,
- proces dyplomowania – prace dyplomowe dotyczące zagadnień z zakresu cyberbezpieczeństwa.

Wybrane zagadnienia z zakresu cyberbezpieczeństwa stanowią elementy innych programów studiów I stopnia prowadzonych lub planowanych na PW (studia na innych kierunkach na Wydziale Elektroniki i Technik Informacyjnych, studia na kierunku „Inżynieria bezpieczeństwa infrastruktury krytycznej” na Wydziale Zarządzania), jednakże żaden z tych programów nie traktuje zagadnień cyberbezpieczeństwa w stopniu porównywalnym – co do zakresu i głębokości – z proponowanym nowym programem.

Większy komponent zajęć z zakresu cyberbezpieczeństwa występuje w programie studiów II stopnia na kierunku „Telekomunikacja”, prowadzonym na Wydziale Elektroniki i Technik Informacyjnych, w ramach którego to kierunku oferowana jest specjalność „Teleinformatyka i cyberbezpieczeństwo”. Jednakże – ze względu na poziom (studia II stopnia), jak i ograniczony zakres oferty zajęć (specjalność, a nie kierunek) – zakres zdobywanych przez studenta kompetencji związanych z cyberbezpieczeństwem jest w tym przypadku wyraźnie inny niż w proponowanym programie.

Liczne zajęcia z zakresu cyberbezpieczeństwa występują w programie studiów podyplomowych „Ochrona informacji w sieciach i systemach teleinformatycznych: projektowanie i audyt zabezpieczeń”, a także w programie studiów podyplomowych *Bezpieczeństwo Systemów Informacyjnych wraz z Technikami Biometrycznymi*, prowadzonych na Wydziale Elektroniki i Technik Informacyjnych.

III. EFEKTY UCZENIA SIĘ

Efekty uczenia się zestawiono w tabeli w załączniku 1.

W tabeli – zgodnie z wymaganiami określonymi w art. 67 ust. 1 pkt 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce – znajdują się także odniesienia do:

- uniwersalnych charakterystyk pierwszego stopnia efektów uczenia się dla kwalifikacji na poziomie 6 Polskiej Ramy Kwalifikacji, określonych w załączniku do ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz.U. 2016 poz. 64),
- charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomie 6 Polskiej Ramy Kwalifikacji, typowych dla kwalifikacji uzyskiwanych w ramach systemu szkolnictwa wyższego i nauki, określonych w Rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6–8 Polskiej Ramy Kwalifikacji (Dz.U. 2018, poz. 2218), z uwzględnieniem rozszerzenia kodu składnika dokonany w sposób analogiczny do przyjętego w uchwale nr 83/XLIX/2017 Senatu PW z dnia 19 kwietnia 2017 r. w sprawie przyjęcia przez Politechnikę Warszawską kodu składnika charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego.

Należy zwrócić uwagę, że w ww. rozporządzeniu (co wynika z przepisów ustawy) nie są określone efekty dla obszaru studiów technicznych, tak jak to było we wcześniej obowiązującym rozporządzeniu. Odniesienia dotyczą jedynie:

- charakterystyk ogólnych odnoszących się do wszystkich programów studiów (część I rozporządzenia),
- charakterystyk odnoszących się do programów studiów umożliwiających uzyskanie kompetencji inżynierskich (część III rozporządzenia),

przy czym charakterystyki te różnicują niektóre z wymienionych w nich efektów w zależności od profilu studiów (sformułowania dla studiów o profilu ogólnoakademickim różnią się od sformułowań dla studiów o profilu praktycznym).

Z tabeli wynika, że efekty uczenia się zdefiniowane dla programu studiów I stopnia na kierunku Cyberbezpieczeństwo – profil ogólnoakademicki pokrywają wszystkie efekty uczenia się wymienione w ww. aktach prawnych, odnoszące się do tego programu.

W tabeli zamieszczonej w załączniku 1 przedstawiono ponadto odniesienia do efektów uczenia się (student outcomes), określonych w kryteriach akredytacji przyjętych przez Accreditation Board for Engineering and Technology – ABET (USA, zasięg globalny). Zestawienie tych efektów znajduje się w załączniku 2. Obejmuje ono efekty wymienione w następujących dokumentach:

1. Criteria for Accrediting Engineering Programs Effective for Reviews During the 2018-2019 Accreditation Cycle, ABET 2017;
<http://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2018-2019>;
2. Criteria for Accrediting Computing Programs Effective for Reviews During the 2018-2019 Accreditation Cycle, ABET 2017;
<http://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2018-2019>.

W dokumencie [1] znajdują się efekty uczenia się dla programów w zakresie „engineering” dla akredytacji programów rozpoczynających się

- w roku akademickim 2018/19,
- w roku akademickim 2019/20 (zgodnie z od dawna diskutowana zmianą).

W dokumencie [2] znajdują się efekty uczenia się dla programów w zakresie „computing” dla akredytacji programów rozpoczynających się w roku akademickim 2018/19, gdzie sformułowano także dodatkowe kryteria odnoszące się do programów w zakresie „cybersecurity”.

IV. PROGRAM STUDIÓW

1. LICZBA PUNKTÓW ECTS KONIECZNA DLA UZYSKANIA KWALIFIKACJI (TYTUŁU ZAWODOWEGO)

210 punktów ECTS + 4 punkty ECTS (praktyka)

2. NOMINALNA LICZBA SEMESTRÓW

7 semestrów

3. ŁĄCZNA LICZBA GODZIN ZAJĘĆ (wymaganie określenia tej liczby wynika z przepisów rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów)

Łączny wymiar zajęć objętych planem studiów wynosi 2580 godz.

Biorąc pod uwagę inne formy zajęć wymagających bezpośredniego udziału studenta i nauczycieli akademickich lub innych osób prowadzących zajęcia (egzaminy, konsultacje), łączny wymiar zajęć wymagających bezpośredniego udziału nauczycieli akademickich wynosi 2709 godz., co odpowiada 108 punktom ECTS (patrz załącznik 5).

4. OPIS POSZCZEGÓLNYCH PRZEDMIOTÓW/MODUŁÓW ZAJĘĆ

Opis przedmiotów w formacie przyjętym przez Wydziałową Komisję Akredytacji Przedmiotów (WKAP), działającą w ramach Wewnętrznego Systemu Zapewniania Jakości Kształcenia (patrz punkt VI), znajduje się w załączniku 3.

5. WYMIAR, ZASADY I FORMA ODBYWANIA PRAKTYK ZAWODOWYCH ORAZ LICZBA PUNKTÓW ECTS, JAKĄ STUDENT MUSI UZYSKAĆ W RAMACH TYCH PRAKTYK

Taka nazwa podpunktu (inna niż w uchwale Senatu PW) wynika z przepisów Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (§ 3 ust. 1 pkt 8)

a) wymiar

Minimalny wymiar czasowy praktyk obowiązkowych wynosi 160 godzin, co odpowiada czterem tygodniom pracy, po 8 godzin dziennie.

b) zasady

- Praktyki studenckie są niezbędnym uzupełnieniem procesu kształcenia. Cele praktyk studenckich są następujące:
 - zastosowanie w praktyce wiedzy i umiejętności zdobytych w trakcie studiów,
 - zdobycie nowej wiedzy i umiejętności praktycznych,
 - rozpoznanie potrzeb i wymagań pracodawców dotyczących nowych pracowników,
 - poznanie systemu organizacji przedsiębiorstwa oraz uwarunkowań i reguł obowiązujących w środowisku pracy,
 - kształtowanie właściwego stosunku do pracy: dbanie o jakość pracy, terminowość wykonywania zadań, prawidłowa współpraca z innymi osobami i komórkami w przedsiębiorstwie, rozwój własnej inicjatywy w środowisku pracy, nabycie umiejętności pracy w zespole.

- Studenci studiów pierwszego stopnia odbywają praktyki po ukończeniu piątego semestru. Praktyki obowiązkowe powinny być zrealizowane przez studenta przed złożeniem pracy dyplomowej.
- Praktyka studencka może się odbyć przed ukończeniem przez studenta piątego semestru, decyzję w tej sprawie podejmuje Pełnomocnik Dziekana ds. Praktyk.
- Minimalny wymiar czasowy praktyk studenckich wynosi 160 godzin.
- Praktyki studenckie powinny odbywać się w przedsiębiorstwach, instytucjach lub placówkach naukowo-badawczych na stanowiskach pracy o profilu zgodnym z kierunkiem studiów, lub w ramach prac naukowo-badawczych i projektów technicznych prowadzonych na Wydziale i Uczelni.
- Miejsce odbywania praktyki student powinien znaleźć samodzielnie.
- W razie trudności w samodzielnym znalezieniu miejsca odbywania praktyki, student może korzystać z pomocy Opiekuna Praktyk lub Pełnomocnika Dziekana ds. Praktyk.
- Miejsce odbywania praktyki oraz jej program powinny być zaakceptowane przez Opiekuna Praktyk.
- Dowolna praktyka, w tym praktyka zagraniczna, może również zostać zaliczona jako praktyka studencka, jeśli spełniła wymagania stawiane praktykom studenckim.
- Praca zawodowa studenta, w tym praca za granicą, może zostać zaliczona jako praktyka studencka, jeśli spełniła wymagania stawiane praktykom studenckim.
- Zaliczenie praktyki odbywa się na podstawie zaświadczenia z podmiotu zewnętrznego o odbyciu praktyki i sporządzonego przez studenta raportu z praktyki, zawierającego opinię przedstawiciela podmiotu zewnętrznego.

c) formy

- Praktyka obowiązkowa – podstawowa forma praktyki. Student samodzielnie znajduje miejsce odbywania praktyki. Program praktyki jest akceptowany, ze strony Uczelni, przez Instytutowego Opiekuna Praktyk. Praktyka jest zaliczana przez Instytutowego Opiekuna Praktyk na podstawie zaświadczenia z przedsiębiorstwa o odbyciu praktyki i sporządzonego przez studenta raportu zawierającego opinię przygotowaną przez przedstawiciela przedsiębiorstwa.
- Staż długoterminowy – staże długoterminowe są realizowane w ramach Programu Rozwojowego Politechniki Warszawskiej. Staże trwają od 3 do 6 miesięcy po minimum 20 godzin tygodniowo. Zasady organizacji i zaliczania są takie same jak dla praktyk obowiązkowych.
- Praktyka dobrowolna – praktyki dobrowolne są organizowane przez studentów samodzielnie na warunkach indywidualnie ustalanych przez studenta z przedsiębiorstwem. Jeżeli przedsiębiorstwo lub student oczekują uczestnictwa Uczelni w porozumieniu o praktyce, to wymagamy od studenta ubezpieczenia się od nieszczęśliwych wypadków i ograniczenia czasu praktyki do maksimum sześciu miesięcy. Praktyka dobrowolna jest zaliczana przez Instytutowego Opiekuna Praktyk jako praktyka obowiązkowa na podstawie zaświadczenia z przedsiębiorstwa o odbyciu praktyki i sporządzonego przez studenta raportu zawierającego opinię przygotowaną przez przedstawiciela przedsiębiorstwa, jeśli prace wykonywane przez studenta odpowiadają wymiarem czasowym i poziomem wymaganiom stawianym praktyce obowiązkowej.
- Praca – praktyka może zostać zaliczona na podstawie wykonywania przez studenta pracy zarobkowej na dowolnych warunkach (etat, umowa zlecenie, umowa o dzieło). Praca studenta jest zaliczana przez Instytutowego Opiekuna Praktyk jako praktyka obowiązkowa na podstawie zaświadczenia o pracy z przedsiębiorstwa i sporządzonego przez studenta raportu zawierającego opinię przygotowaną przez przedstawiciela przedsiębiorstwa, jeśli prace wykonywane przez studenta odpowiadają wymiarem czasowym i poziomem wymaganiom stawianym praktyce obowiązkowej.

6. MATRYCA EFEKTÓW UCZENIA SIĘ (EFEKTY UCZENIA SIĘ – PRZEDMIOTY/MODUŁY ZAJĘĆ)

Matryca efektów uczenia się znajduje się w załączniku 4.

7. OPIS SPOSOBU SPRAWDZANIA WYBRANYCH EFEKTÓW UCZENIA SIĘ (DLA PROGRAMU) Z ODNIESIENIEM DO KONKRETNÝCH PRZEDMIOTÓW, FORM ZAJĘĆ I SPRAWDZIANÓW REALIZOWANYCH W RAMACH KAŻDEJ Z TYCH FORM

Wybrano następujące efekty uczenia się z zakresu wiedzy, umiejętności i kompetencji społecznych, zdefiniowane dla programu studiów (załącznik 1):

W04

ma wiedzę w zakresie techniki cyfrowej i sprzętowych komponentów systemów komputerowych i sieci teleinformatycznych, obejmującą m.in.:

- *podstawy techniki cyfrowej,*
 - *metody projektowania układów i systemów cyfrowych z wykorzystaniem różnych typów komponentów,*
 - *architekturę i organizację systemów komputerowych,*
- tworząc podstawy do projektowania warstwy sprzętowej systemów teleinformatycznych, w szczególności rozwiązań związanych z zapewnieniem cyberbezpieczeństwa tych systemów*

Wiedzę w tym zakresie student uzyskuje przede wszystkim w ramach przedmiotów obowiązkowych:

- *Podstawy techniki cyfrowej,*
- *Systemy cyfrowe,*
- *Systemy komputerowe: architektura i programowanie,*

odpowiadających zakresom wiedzy wymienionym w opisie tego efektu.

Wiedza uzyskiwana przez studenta jest sprawdzana bezpośrednio na sprawdzianach realizowanych w warunkach audytoryjnych (kolokwiach oraz – w przypadku przedmiotu *Podstawy techniki cyfrowej* – także na egzaminie), obejmujących głównie rozwiązywanie zadań. Przede wszystkim jest jednak sprawdzana w sposób pośredni, a zarazem najważniejszy z punktu widzenia wykształcenia inżyniera – przez weryfikację umiejętności jej wykorzystania. W ramach ww. przedmiotów następuje to na zajęciach praktycznych (z każdym z tych przedmiotów są związane zajęcia laboratoryjne i projekt), podczas których studenci, wykorzystując wiedzę wyniesioną z wykładów i samodzielnych studiów, projektują, realizują i testują komponenty sprzętowe stanowiące rozwiązania prostych zadań inżynierskich.

Umiejętnością wykorzystania zdobytej na ww. przedmiotach wiedzy student musi się także wykazać na bardziej zaawansowanych przedmiotach, w szczególności przedmiotach:

- *Komputerowe i sieciowe systemy operacyjne,*
- *Komutacja i routing w Internecie,*
- *Sieci bezprzewodowe komórkowe, lokalne i sensorowe,*
- *Sieci lokalne i sieci centrów,*
- *Bezpieczeństwo systemów i oprogramowania,*
- *Kryminalistyka cyfrowa,*

w ramach których – na zajęciach praktycznych – projektuje i analizuje w laboratoriach rozwiązania używane w warstwie sprzętowej systemów teleinformatycznych, w szczególności rozwiązania związane z zapewnieniem cyberbezpieczeństwa tych systemów. Jakość tych rozwiązań, wynikająca z posiadanej przez studenta wiedzy i umiejętności jej wykorzystania, jest weryfikowana metodami przyjętymi w tych przedmiotach (patrz załącznik 3)

W przypadku studentów realizujących w ramach procesu dyplomowania projekt zawierający komponent sprzętowy, odpowiednio pogłębiona – na przedmiotach obowiązkowych i obieralnych oraz w ramach samodzielnych studiów – wiedza z zakresu techniki cyfrowej stanowi podstawę do realizacji projektu dyplomowego i jest weryfikowana w procesie recenzowania pracy dyplomowej i podczas jej obrony.

U05

potrafi – przy identyfikowaniu problemów i formułowaniu specyfikacji zadań inżynierskich oraz problemów badawczych związanych z zapewnieniem cyberbezpieczeństwa oraz rozwiązywaniu tych zadań – dostrzec i uwzględnić ich aspekty systemowe i pozatechniczne (ekonomiczne, społeczne, etyczne, czynnik ludzki i inne) oraz dokonać wstępnej oceny ekonomicznej proponowanych rozwiązań.

Formułowanie i rozwiązywanie zadań inżynierskich z zakresu cyberbezpieczeństwa to podstawowe umiejętności zdobywane w ramach przedmiotów z klasy CYBERBEZPIECZEŃSTWO. Obejmuje to także aspekty systemowe i pozatechniczne. Reprezentatywnymi przykładami przedmiotów dających studentom umiejętności w tym zakresie są:

- *Bezpieczeństwo komunikacji,*
- *Bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbezpieczeństwem.*

Pierwszy z przedmiotów, *Bezpieczeństwo komunikacji*, w ramach ćwiczeń laboratoryjnych, uświadamia studentom zagrożenia wynikające ze złośliwych działań użytkowników sieci i prezentuje możliwe opcje stosowania zabezpieczeń, wybierane z uwzględnieniem aspektów ekonomicznych (koszt pozyskania, nakład pracy przy wdrożeniu, itp.). Stopień opanowania tych umiejętności jest sprawdzany w czasie prezentacji raportów z ćwiczeń laboratoryjnych i sprawozdania z projektu.

Przedmiot *Bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbezpieczeństwem* jest w całości poświęcony systemowym i pozatechnicznym aspektom cyberbezpieczeństwa związanym ze stosowaniem technologii ochrony informacji i zasobów sieciowych. Zajęcia praktyczne w formie *case study* są w tym przypadku idealną metodą zdobywania i weryfikowania, także w czasie dyskusji i wzajemnej oceny w ramach grupy studenckiej, umiejętności dotyczących zarządzania bezpieczeństwem, ekonomii bezpieczeństwa i aspektów socjotechnicznych cyberbezpieczeństwa. Raport z projektu i egzamin są podsumowującym elementem sprawdzenia zdobytych umiejętności.

Znaczne pogłębienie umiejętności określonych przez U05 następuje w ramach realizacji przez każdego studenta co najmniej 3 przedmiotów z klasy CYBERBEZPIECZEŃSTWO – PRZEDMIOTY OBIERALNE.

Efekt U05 jest uzyskiwany także, choć może w mniejszym stopniu, na przedmiotach z innych klas, zwłaszcza z klasy TELEINFORMATYKA.

W przypadku wielu studentów, rozwiązujących w ramach procesu dyplomowania zadania inżynierskie oraz problemy badawcze związane z zapewnieniem cyberbezpieczeństwa, analiza aspektów systemowych i pozatechnicznych, w tym ekonomicznych, proponowanych rozwiązań stanowi integralną część pracy, a umiejętność przeprowadzenia takiej analizy jest weryfikowana w procesie recenzowania pracy dyplomowej i podczas jej obrony.

U07

potrafi ocenić możliwości funkcjonowania systemu lub sieci w warunkach wystąpienia zagrożeń; potrafi przewidzieć skutki (techniczne, ekonomiczne, społeczne i inne)

ataków stwarzających zagrożenie dla bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych oraz zaproponować działania minimalizujące te skutki.

Klasa CYBERBEZPIECZEŃSTWO dotyczy w całości zagrożeń bezpieczeństwa rozumianych wieloaspektowo, od ich identyfikacji, poprzez ocenę skutków technicznych, ekonomicznych i społecznych, do propozycji przeciwdziałań i próby ich realizacji. Umiejętności z tym związane, z naciskiem na aspekt techniczny, student uzyskuje głównie w ramach przedmiotów:

- *Wprowadzenie do cyberbezpieczeństwa,*
- *Bezpieczeństwo danych,*
- *Bezpieczeństwo systemów i oprogramowania,*
- *Bezpieczeństwo komunikacji,*
- *Kryminalistyka cyfrowa.*

Weryfikacja zdobytych umiejętności następuje podczas rozwiązywania zadań o charakterze praktycznym na egzaminach (przedmioty: *Bezpieczeństwo danych, Bezpieczeństwo systemów i oprogramowania, Bezpieczeństwo komunikacji*) oraz, w znacznie większym stopniu, w trakcie realizacji zadań projektowych i realizacji ćwiczeń laboratoryjnych.

Zajęcia praktyczne związane z przedmiotem *Wprowadzenie do cyberbezpieczeństwa* dają studentowi szerokie (na podstawowym poziomie) umiejętności postępowania z zagrożeniami, weryfikowane przez realizację i raportowanie wyników ćwiczeń laboratoryjnych, obejmujących zadania związane z monitorowaniem sieci i systemów, modelowaniem, symulowaniem i wykrywaniem zagrożeń oraz testów penetracyjnych systemów. Zadanie projektowe weryfikuje umiejętności dotyczące postępowania z incydentami bezpieczeństwa w podstawowym zakresie. Ta umiejętność zostaje później, w ramach przedmiotu *Kryminalistyka cyfrowa*, znacznie rozwinięta i powtórnie zweryfikowana na zaawansowanym poziomie w ramach zajęć laboratoryjnych, podczas których realizowane są zadania śledcze z wykorzystaniem specjalistycznych technik i oprogramowania.

Trzy pozostałe ww. przedmioty z klasy CYBERBEZPIECZEŃSTWO: *Bezpieczeństwo danych, Bezpieczeństwo komunikacji i Bezpieczeństwo systemów i oprogramowania* rozwijają umiejętności związane z bezpieczeństwem zasobów informacyjnych, sieci teleinformatycznych i serwerów/węzłów sieci. Projekt związany z przedmiotem *Bezpieczeństwo danych*, uzupełniony o dwa ćwiczenia laboratoryjne, umożliwi weryfikację umiejętności studentów w zakresie doboru rozwiązań bezpieczeństwa, ich implementacji i oceny jakości dla systemów przechowujących i przetwarzanych dane. Laboratoria i projekt związane z przedmiotem *Bezpieczeństwo komunikacji* umożliwią weryfikację tych umiejętności dla systemów transmisyjnych, a projekt związany z przedmiotem *Bezpieczeństwo systemów i oprogramowania* zweryfikuje stopień opanowania przez studentów umiejętności ochrony urządzeń stosowanych w sieciach teleinformatycznych wraz z ich oprogramowaniem.

Wymienione wyżej metody weryfikacji umiejętności uwzględniają nie tylko techniczny aspekt cyberbezpieczeństwa. Każda implementacja, przeprowadzone badanie laboratoryjne lub analiza bezpieczeństwa wiąże się z koniecznością wyboru konkretnego rozwiązania, a ten wybór dokonywany jest na podstawie szerszej analizy uwzględniającej aspekt ekonomiczny. Ponadto, w ramach przedmiotu *Kryminalistyka cyfrowa* dużo uwagi poświęca się aspektom społecznym (odpowiedzialność dostawcy/użytkownika usługi, konsekwencje działań, itp.), a przyjęte sposoby weryfikacji zdobytych przez studenta na zajęciach praktycznych umiejętności obejmują także sprawdzenie kompetencji w tym zakresie.

Podsumowując, przyjęte w przedmiotach obowiązkowych z klasy CYBERBEZPIECZEŃSTWO sposoby weryfikacji umiejętności studenta zapewniają osiągnięcie w pełni efektu U07. W praktyce, znaczne pogłębienie umiejętności określonych przez U07 następuje w ramach realizacji przez każdego studenta co najmniej 3 przedmiotów z klasy CYBERBEZPIECZEŃSTWO – PRZEDMIOTY OBIERALNE.

Efekt U07 jest uzyskiwany także, choć może w mniejszym stopniu, na przedmiotach z innych klas, zwłaszcza z klasy TELEINFORMATYKA.

W przypadku wielu studentów, rozwiązujących w ramach procesu dyplomowania zadania inżynierskie oraz problemy badawcze związane z oceną skutków ataków stwarzających zagrożenie dla bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych oraz opracowaniem rozwiązań minimalizujących te skutki, umiejętność przeprowadzenia takiej oceny i zaproponowania mechanizmów przeciwdziałania jest weryfikowana w procesie recenzowania pracy dyplomowej i podczas jej obrony.

U13

ma umiejętność samokształcenia się, m.in. w celu podnoszenia kompetencji zawodowych

oraz KS01

rozumie potrzebę stałego aktualizowania i wzbogacania posiadanej wiedzy – podnoszenia kompetencji zawodowych, osobistych i społecznych

Te dwa efekty omawiane są łącznie ze względu na bliską relację metod weryfikacji. Weryfikacja KS01, jak każdego z innego efektu z grupy kompetencji społecznych, opisujących postawy (a nie umiejętności), nastręcza trudności. Toteż przyjmuje się, że uzyskanie przez studenta tego typu trudno weryfikowalnych efektów następuje w wyniku stosowania odpowiednich metod kształcenia stymulujących kreowanie pożądanych postaw.

W przypadku „rozumienia potrzeby stałego aktualizowania i wzbogacania posiadanej wiedzy – podnoszenia kompetencji zawodowych, osobistych i społecznych” polega to m.in. na takiej koncepcji prowadzenia przedmiotów, która czyni samodzielne poszukiwanie i analizowanie przez studenta materiałów źródłowych warunkiem wykonania zadań przewidzianych w programie przedmiotu.

W opracowanym programie studiów występuje wiele przedmiotów, w których opisie w sposób jawny uwidoczniono umiejętność samokształcenia – samodzielnego zdobywania przez studenta wiedzy – jako warunku realizacji zadań, zwykle zadań o charakterze projektowym. Przykładami takich przedmiotów, prowadzonych na początkowych semestrach, kiedy zdobycie umiejętności samokształcenia i zrozumienie potrzeby stałego wzbogacania posiadanej wiedzy ma szczególnie istotne znaczenie, są (patrz załącznik 3 oraz załącznik 4):

- *Pozatechniczne aspekty pracy inżyniera,*
- *Szybkie prototypowanie inżynierskie,*
- przedmioty z klasy MATEMATYKA,
- *Wprowadzenie do cyberbezpieczeństwa.*

Efekty U03 oraz KS01 są oczywiście uzyskiwane także na bardziej zaawansowanych przedmiotach, a zwłaszcza w procesie dyplomowania.

8. PLAN STUDIÓW

Wzorcowy plan studiów zamieszczono w załączniku 6. Każdy student – w ramach indywidualizacji toku studiów – może realizować ten plan w wybrany przez siebie sposób, zapewniający spełnienie wymagań programowych i rejestracyjnych, m.in. przez wybór przedmiotów obieralnych oraz regulowanie tempa studiowania (liczby i zestawu przedmiotów realizowanych na poszczególnych semestrach).

9. STRUKTURA STUDIÓW

Studia realizowane są wg jednolitego programu (bez specjalności), ale bogata oferta przedmiotów obieralnych (możliwość korzystania z pełnego zestawu przedmiotów prowadzonych na Wydziale), możliwość korzystania z oferty innych wydziałów i innych uczelni, możliwość wyboru tematyki pracy dyplomowej oraz możliwość wyboru miejsca odbywania praktyki umożliwiają studentom konstruowanie indywidualnych ścieżek kształcenia ukierunkowanych na wybraną grupę zagadnień z zakresu cyberbezpieczeństwa, przykładowo:

- bezpieczeństwo danych,
- bezpieczeństwo sprzętowych komponentów systemów komputerowych i sieci teleinformatycznych,
- bezpieczeństwo oprogramowania,
- bezpieczeństwo komunikacji,
- kryminalistyka cyfrowa,
- zarządzanie cyberbezpieczeństwem.

10. ZASADY PROWADZENIA PROCESU DYPLOMOWANIA

Zasady prowadzenia prac dyplomowych i egzaminów dyplomowych określa Księga Jakości Kształcenia Wydziału Elektroniki i Technik Informatycznych Politechniki Warszawskiej (patrz punkt VI).

11. OPIS WYDZIAŁOWEGO SYSTEMU PUNKTOWEGO

W załączniku 7 przedstawiono wymagania programowe dla programu studiów na kierunku Cyberbezpieczeństwo, wyrażone liczbą punktów ECTS, przypisanych do klas programowych (czyli do grup przedmiotów) w układzie semestralnym. Końcowa liczba punktów ECTS w każdej klasie programowej, a także łączna liczba punktów, stanowi wymaganie niezbędne do zrealizowania programu studiów. Przyrost punktów ECTS, przedstawiony w kolejnych semestrach, odpowiada realizacji programu studiów zgodnie z planem modelowym. Plan modelowy stanowi jedną z możliwych realizacji programu studiów, z zachowaniem nominalnego czasu ich trwania, równomiernych obciążeń semestralnych i zaleceń dotyczących następstwa przedmiotów. Dziekan Wydziału opracowuje i udostępnia wymagania rejestracyjne, zarówno pełne jak też warunkowe, uwzględniając możliwości przedłużenia czasu trwania studiów, wynikające z obowiązujących aktów prawnych, oraz zapewnia wdrożenie tych wymagań w informatycznym systemie obsługi studiów.

12. SUMARYCZNE WSKAŹNIKI CHARAKTERYZUJĄCE PROGRAM STUDIÓW

Wyliczenie podanych niżej wartości wskaźników znajduje się w załączniku 5.

- a) liczba punktów ECTS, którą student musi uzyskać na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów:

106 punktów ECTS,

co stanowi 50.5% łącznej liczby punktów przypisanych programowi studiów;

- b) liczba punktów ECTS, którą student musi uzyskać w ramach zajęć o charakterze praktycznym, w tym zajęć laboratoryjnych i projektowych:

102 punkty ECTS,
co stanowi 48.5% łącznej liczby punktów przypisanych programowi studiów;

- c) łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć z zakresu nauk podstawowych, do których odnoszą się efekty uczenia się:

29 punktów ECTS,
co stanowi 14% łącznej liczby punktów przypisanych programowi studiów;

- d) łączna liczba punktów ECTS przypisanych zajęciom związanym z prowadzoną w Uczelni działalnością naukową w dyscyplinie *Informatyka techniczna i telekomunikacja*, do której przyporządkowany jest kierunek studiów, z uwzględnieniem udziału studentów w zajęciach przygotowujących do prowadzenia działalności naukowej lub udziału w tej działalności:

135 punktów ECTS,
co stanowi 64% łącznej liczby punktów przypisanych programowi studiów;

- e) łączna liczba punktów ECTS, którą student musi uzyskać na zajęciach podlegających wyborowi:

74 punkty ECTS,
co stanowi 35% łącznej liczby punktów przypisanych programowi studiów.

V. WARUNKI REALIZACJI PROGRAMU STUDIÓW

Zawarte w uchwale Senatu wymaganie zamieszczenia wykazu nauczycieli akademickich stanowiących minimum kadrowe dla kierunku i stopnia studiów oraz podania innych danych dotyczących tego minimum – w związku ze zmianami regulacji w tym zakresie (przepisy rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów, wobec braku odpowiedniej delegacji w ustawie, nie formułują żadnych wymagań dotyczących minimum kadrowego) – nie ma zastosowania.

W związku z tym przedstawiono ogólną charakterystykę kadry prowadzącej zajęcia na Wydziale, a w szczególności kadry stanowiącej „trzon” realizatorów zajęć na nowym kierunku.

Wydział Elektroniki i Technik Informacyjnych dysponuje kadrami ok. 250 nauczycieli akademickich, w tym niemal 100 samodzielnych pracowników naukowych, z których część zajmuje się w pracach badawczych i działalności dydaktycznej zagadnieniami związanymi z cyberbezpieczeństwem, prowadząc zajęcia z tego zakresu w ramach innych kierunków studiów, w tym uruchomionej z początkiem roku akademickiego 2017/18 na studiach II stopnia w ramach kierunku „Telekomunikacja” specjalności „Teleinformatyka i cyberbezpieczeństwo”.

Uruchomienie studiów I stopnia na kierunku „Cyberbezpieczeństwo” jest inicjatywą wydziałową, w którą zaangażowani będą pracownicy kilku instytutów. Istotną rolę w tym przedsięwzięciu odgrywa kadra Zakładu Cyberbezpieczeństwa (ZCB) funkcjonującego od 2015 roku w strukturze Instytutu Telekomunikacji. Kierownikiem ZCB, a zarazem kierownikiem projektu jest dr hab. inż. Krzysztof Szczypiorski, prof. PW. W ZCB jest ponadto 5 innych samodzielnych pracowników naukowych oraz 3 pracowników naukowo-badawczych i 3 pracowników dydaktycznych.

W dorobku pracowników ZCB znajdują się m.in.:

1. opracowanie ponad 50 metod ukrywania informacji w sieciach teleinformatycznych;
2. opracowanie algorytmów i metod wykrywania nowych ataków na sieci teleinformatyczne (w tym typu zero-day exploit);
3. opracowanie metod wykrywania nowych ataków na interfejsy biometrii głosowej;
4. udział w grantach i projektach finansowanych m.in. przez MNiSW, NCN, NCBiR, MEN, A-STAR (Singapur), Unię Europejską i NATO, US Army i US Air Force, które dotyczyły m.in.:
 - a) bezpieczeństwa sieci bezprzewodowych, w tym: IEEE 802.11, 802.16 i sieci sensorowych,
 - b) nowych metod steganograficznych,
 - c) nowych metod wykrywania anomalii sieciowych,
 - d) nowoczesnych mechanizmów wspierających sieci pojazdów autonomicznych;
5. 3 wnioski patentowe, jeden patent przyznany,
6. ponad 100 artykułów z listy filadelfijskiej, kilkaset innych artykułów na czołowych konferencjach branżowych.

W okresie od czerwca 2017 r. w Zakładzie Cyberbezpieczeństwa realizowane były następujące projekty badawcze z obszaru teleinformatyki i cyberbezpieczeństwa (lista obejmuje projekty w toku, projekty zakończone w tym okresie oraz projekty przyznane, których realizacja rozpocznie się w najbliższym czasie):

1. projekty Horyzont 2020
 - a) Internet Przyszłości w oparciu o sieci radiowe oraz komunikacje światła widzialnego; kierownik w PW: dr hab. Wojciech Mazurczyk;
 - b) Secure Intelligent Methods for Advanced Recognition of malware and stegomalware; kierownik w PW: dr hab. Artur Janicki;

2. Inne projekty międzynarodowe
 - a) Strategic Partnership in Information Security – ParIS (project Erasmus+); kierownik w PW: prof. dr hab. Zbigniew Kotulski;
 - b) Detection and countermeasures against information hiding-based malware – DeColMa (project finansowany przez Federalne Ministerstwo Edukacji i Nauki w Niemczech); kierownik w PW: dr hab. Artur Janicki;
 - c) Energy Efficient and Secure Smart Environment - E2S2E (projekt finansowany przez Federalne Ministerstwo Edukacji i Nauki w Niemczech); kierownik w PW: dr hab. Wojciech Mazurczyk
 - d) SATellite Network of EXperts IV (projekt finansowany przez European Space Agency - partnerstwo stowarzyszone w sieci doskonałości); kierownik w PW: prof. dr hab. Zbigniew Kotulski;
3. Projekty NCBiR
 - a) Platforma detekcji anomalii sieciowych - PDAS (projekt realizowany w ramach programu „CyberSecIdent „Cyberbezpieczeństwo i e-Tożsamość”); kierownik w PW: dr hab. K. Szczypiorski;
 - b) Zaawansowane laboratorium kryminalistyki śledczej (projekt realizowany w ramach programu „CyberSecIdent „Cyberbezpieczeństwo i e-Tożsamość”); kierownik w PW: dr hab. K. Szczypiorski;
 - c) System zabezpieczenia sieci informatycznej oparty na technologii SDN/NFV/MTD oraz sztucznej inteligencji (projekt realizowany w ramach programu „CyberSecIdent „Cyberbezpieczeństwo i e-Tożsamość”); kierownik w PW: dr hab. M. Rawski;
 - d) Innowacyjny komponent sprzętowo-programowy, wykorzystujący specjalizowany układ scalony oraz oprogramowanie, realizujący różne funkcje kryptograficzne, ze szczególnym uwzględnieniem zastosowań w systemach identyfikacji elektronicznej z wysokim poziomem pewności (projekt realizowany w ramach programu „CyberSecIdent „Cyberbezpieczeństwo i e-Tożsamość”); kierownik w PW: dr hab. M. Rawski;
4. Projekt MNiSW

An Efficient Software Defined Network (SDN) - based Framework for Big Data Processing in Cloud Data Center (Polsko-indyjski projekt naukowo-badawczy); kierownik w PW: dr hab. K. Szczypiorski;
5. Grant dziekański

Opracowanie koncepcji "kodu DNA" złośliwego oprogramowania - badania pilotażowe
kierownik w PW: mgr inż. Katarzyna Kamińska;
6. Prace umowne krajowe
 - a) Network Slicing – parametry i właściwości izolacji; kierownik w PW: prof. dr hab. Zbigniew Kotulski;
 - b) Network Slicing – feasibility study of framework for isolated slicing; kierownik w PW: prof. dr hab. Zbigniew Kotulski;
 - c) Network Slicing Isolation - walidacja i ocena proponowanego modelu graficznego do obliczania izolacji; kierownik w PW: prof. dr hab. Zbigniew Kotulski;
 - d) Zagadnienia bezpieczeństwa związane z technologią MEC (Multi Access Edge Computing) - przegląd stanu wiedzy; kierownik w PW: prof. dr hab. Zbigniew Kotulski

Wyrazem uznania dla osiągnięć Zakładu Cyberbezpieczeństwa i znaczenia tych osiągnięć dla społeczeństwa było wręczenie kierownikowi ZCB – prof. K. Szczypiorskiemu, na gali z okazji 25-lecia NASK, która miała miejsce 13 grudnia 2018 r. w Centrum Nauki Kopernik, indywidualnej nagrody im. prof. Tomasza Hofmoka za wkład w rozwój społeczeństwa informacyjnego w dziedzinie cyberbezpieczeństwo.

W przygotowaniu i realizacji nowego programu studiów istotną rolę odgrywają i odgrywać będą pozostali pracownicy Instytutu Telekomunikacji (IT). W IT od kilku lat następuje ewolucja profilu działalności naukowej i dydaktycznej, której przejawem są m.in.:

- dokonane w roku 2015 zmiany w strukturze organizacyjnej Instytutu, w tym utworzenie – oprócz Zakładu Cyberbezpieczeństwa – Zakładu Sieci i Usług Teleinformatycznych, oraz

Zespołu Architektur i Zastosowań Internetu (zachował swą dotychczasową nazwę Zakład Systemów Telekomunikacyjnych),

- znaczny przyrost liczby samodzielnych pracowników naukowych (w okresie ostatnich 3 lat stopień doktora hab. uzyskało 6 pracowników IT, w wyraźnej większości prowadzących badania w zakresie teleinformatyki i cyberbezpieczeństwa,
- coraz większa liczba prac dyplomowych dotyczących zagadnień związanych z teleinformatyką i cyberbezpieczeństwem,
- działalność studenckiego Koła Naukowego Bezpieczeństwa Informacyjnego.

Zespoły prowadzące badania i działalność dydaktyczną w zakresie różnych aspektów cyberbezpieczeństwa znajdują się także w strukturze innych instytutów funkcjonujących w strukturze Wydziału: Instytutu Automatyki i Informatyki Stosowanej, Instytutu Informatyki oraz Instytutu Systemów Elektronicznych.

VI. WEWNĘTRZNY SYSTEM ZAPEWNIENIA JAKOŚCI KSZTAŁCENIA

Wewnętrzny system zapewnienia jakości kształcenia na Wydziale Elektroniki i Technik Informacyjnych PW jest opisany w dokumencie „Księga Jakości Kształcenia Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej”, zatwierdzonym uchwałą Rady Wydziału z dnia 24 marca 2015 r., dostępnym na stronie <http://www.elka.pw.edu.pl/Wydzial/O-WEiTI/Strategia-Wydzialu/Ksiega-Jakosci-Ksztalcenia-Wydzialu-Elektroniki-i-Technik-Informacyjnych-Politechniki-Warszawskiej>.

VII. INNE INFORMACJE

1. SPOSÓB WYKORZYSTANIA WZORCÓW MIĘDZYNARODOWYCH

Zestaw kompetencji absolwenta (efektów uczenia się) oraz zestaw zasadniczych treści zawartych w programie studiów prowadzącym do uzyskania tych kompetencji opracowano korzystając m.in. z następujących materiałów wyznaczających światowe standardy w tym zakresie:

- raportu *National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework*, opracowanego przez National Institute of Standards and Technology, August 2017;
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf;
raport ten zawiera szczegółową charakterystykę pełnego spektrum zróżnicowanych profili/ról zawodowych i związanych z nimi kompetencji (wiedzy i umiejętności) osób kształconych w tym zakresie,
- raportu *Cybersecurity Curricula 2017*, opracowanego przez Joint Task Force on Cybersecurity Education: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on, Information Security Education (IFIP WG 11.8), December 2017;
www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

Wzięto również pod uwagę efekty uczenia się (student outcomes), określone w kryteriach akredytacji przyjętych przez Accreditation Board for Engineering and Technology (USA) – patrz punkt „Efekty uczenia się”.

W procesie przygotowywania się do opracowania programu studiów dokonano analizy literatury dotyczącej kształcenia w zakresie cyberbezpieczeństwa (głównie materiałów o charakterze przeglądowym) oraz kilku programów oferowanych przez uczelnie zagraniczne. W szczególności wykorzystano pełną dokumentację programu studiów „Cyber Security Engineering”, prowadzonego od roku 2014 w Volgenau School of Engineering, George Mason University, USA – instytucję dobrze znaną pracownikom Zakładu Cyberbezpieczeństwa z racji osobistych kontaktów i wzajemnych wizyt.

Międzynarodowe doświadczenia dydaktyczne w zakresie cyberbezpieczeństwa związane są także z udziałem pracowników Wydziału w realizacji projektu PaRIS (Partnership in Information Security) finansowanego z programu Erasmus+, w którym partnerami PW są University of Luxembourg - Faculty of Sciences, University of Lisbon oraz National Technical University of Ukraine “Kyiv Polytechnic Institute”. W ramach tego projektu przygotowywane zostały: *International Joint Master's Programme in Information Security* oraz 5-dniowy *Intensive Study Programme in Information Security*.

2. SPOSÓB UWZGLĘDNIENIA WYNIKÓW MONITOROWANIA KARIER ABSOLWENTÓW

Przy opracowaniu ogólnych założeń i koncepcji programu studiów, w tym definiowaniu zestawu efektów uczenia się odnoszących się do kompetencji ogólnych, niezależnych od kierunku studiów, wykorzystano wyniki projektu „Monitoring karier zawodowych absolwentów Politechniki Warszawskiej”, realizowanego przez Dział Badań i Analiz Centrum Zarządzania Innowacjami i Transferem Technologii PW, a w szczególności suplement do raportu z roku 2016 r., zawierający szczegółowe dane – w postaci arkusza programu Excel – odnoszące się do Wydziału Elektroniki i Technik Informacyjnych oraz wybranych kierunków studiów prowadzonych na Wydziale.

Wyniki te posłużyły do sformułowania przez Komisję ds. Kształcenia Rady Wydziału zestawu postulatów dotyczących opracowywania nowych/doskonalenia dotychczas prowadzonych programów studiów w ramach projektów NERW.

W efekcie powstał projekt programu studiów I stopnia na kierunku Cyberbezpieczeństwo, który charakteryzuje się:

- znacznym komponentem zajęć dotyczących pozatechnicznych aspektów pracy inżyniera oraz służących kształtowaniu kompetencji „miękkich”,
- ograniczeniem liczby przedmiotów (w odpowiedzi na negatywną ocenę fragmentacji wiedzy absolwentów i trudności w postrzeganiu relacji między wiedzą zdobywaną na poszczególnych przedmiotach),
- dobrą synchronizacją treści poszczególnych przedmiotów,
- znaczną elastycznością (możliwością kształtowania indywidualnego programu i planu studiów, z wykorzystaniem zajęć prowadzonych na innych wydziałach PW i innych uczelniach),
- znacznym udziałem zajęć prowadzonych w formach aktywizujących studentów, w tym zajęć o tym charakterze na I roku studiów.

Ze względu na to, że kierunek Cyberbezpieczeństwo jest nowym elementem oferty Wydziału, nie ma danych dotyczących karier absolwentów studiów na tym kierunku. Zebrano natomiast wiele informacji dotyczących oczekiwanego przez rynek pracy modelu absolwenta. Są one przedstawione w kolejnym punkcie

3. SPOSÓB UWZGLĘDNIENIA WYNIKÓW ANALIZY ZGODNOŚCI ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ/EFEKTÓW KSZTAŁCENIA Z POTRZEBAMI RYNKU PRACY - SPOSÓB WSPÓŁDZIAŁANIA Z INTERESARIUSZAMI ZEWNĘTRZNYMI

Doświadczenia związane z uruchomieniem w roku akademickim 2017/2018 w ramach studiów II stopnia na kierunku *Telekomunikacja* specjalności *Teleinformatyka i Cyberbezpieczeństwo*, a zwłaszcza opinie zebrane z kilkunastu instytucji z otoczenia społeczno-gospodarczego, zainteresowanych zatrudnieniem absolwentów tych studiów, stanowiły zachętę do skierowania do tych i innych instytucji rozbudowanej ankiety dotyczącej:

- ogólnego profilu kompetencyjnego absolwenta,
- pożądanych kompetencji absolwenta, w tym kompetencji miękkich,
- zagadnień z zakresu cyberbezpieczeństwa i innych obszarów wiedzy, które powinny odpowiednio wyeksponowane w programie studiów.

Formularz ankiety stanowi załącznik 8.

Uzyskano kompletne zestawy odpowiedzi z następujących instytucji:

- Asseco
- Centralne Laboratorium Kryminalistyczne Policji
- Cert Polska
- Cryptomage
- IBM
- KPMG
- Narodowe Centrum Kryptologii
- Orange
- PKO BP
- Play
- T-Mobile
- VT Cyber
- WB Electronics

Bezpośredni udział w pracach programowych wzięła ponadto grupa najwyższej klasy ekspertów z zakresu cyberbezpieczeństwa:

- dr inż. Andrzej Bartosiewicz: Dyrektor dr. infrastruktury krytycznej i cyberbezpieczeństwa, Thales Polska,
- Robert Kośla: Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji (poprzednio dyrektor sektora bezpieczeństwa narodowego i obronności na region Europy Środkowej i Wschodniej w Microsoft Europe),
- Mirosław Maj: prezes Fundacji Bezpieczna Cyberprzestrzeń, wiceprezes zarządu ComCERT SA,
- prof. Ewa Niewiadomska-Szyrkiewicz: Zastępca Dyrektora NASK do Spraw Naukowych

Wyniki ankietowania oraz opinie ekspertów miały istotny wpływ na kształt programu, a w szczególności spowodowały:

- wprowadzenie do programu 1. semestru „dużego” przedmiotu „Wprowadzenie do cyberbezpieczeństwa”, że znacznym komponentem zajęć praktycznych,
- istotne zmiany – w porównaniu z pierwszą wersją programu – treści i sekwencji przedmiotów w klasie Cyberbezpieczeństwo, wymuszające z kolei odpowiednie zmiany w treści i sekwencji innych przedmiotów.

W procesie projektowania istotną rolę odegrali studenci delegowani przez Wydziałową Radę Samorządu, w większości przypadków mający już doświadczenie w pracy zawodowej. Uczestniczyli oni w regularnie odbywających się od czerwca 2018 r. mniej więcej co dwa tygodnie spotkaniach zespołu opracowującego projekt programu, przekazując opinie dotyczące m.in. mankamentów obecnie prowadzonych programów studiów i postulaty dotyczące pożądanych (i – co równie ważne – niepożądanych) treści i form kształcenia.

4. UDOKUMENTOWANIE, ŻE LICZBA PUNKTÓW ECTS, KTÓRĄ STUDENT MUSI UZYSKAĆ NA ZAJĘCIACH WYMAGAJĄCYCH BEZPOŚREDNIEGO UDZIAŁU NAUCZYCIELI AKADEMICKICH LUB INNYCH OSÓB PROWADZĄCYCH ZAJĘCIA, WYNOSI CO NAJMNIEJ POŁOWĘ PUNKTÓW ECTS DLA PROGRAMU

Udokumentowanie znajduje się w załączniku 5.

5. UDOKUMENTOWANIE, ŻE PROGRAM STUDIÓW UMOŻLIWIA STUDENTOWI WYBÓR ZAJĘĆ, KTÓRYM PRZYPISANO PUNKTY ECTS W WYMIARZE NIE MNIEJSZYM NIŻ 30% PUNKTÓW ECTS DLA PROGRAMU.

Udokumentowanie znajduje się w załączniku 5.

6. STOSOWANE METODY KSZTAŁCENIA UMOŻLIWIAJĄCE STUDENTOM OSIĄGANIE ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ, W TYM CO NAJMNIEJ PRZYGOTOWANIE DO PROWADZENIA BADAŃ

Przyjęta koncepcja programowa zakłada odejście – na ile to możliwe i uzasadnione – od kształcenia masowego, opartego na biernym uczestnictwie w zajęciach (narzucającym pozyskiwanie wiedzy teoretycznej i pasywne jej odtwarzanie na sprawdzianach) na rzecz stosowania metod kształcenia opartego na rozwiązywaniu problemów i realizacji projektów oraz innych form prowadzenia zajęć aktywizujących studentów (więcej na ten temat – w kolejnym punkcie). Powoduje to, że matryca pokrycia efektów uczenia się (załącznik 4) jest szczególnie „gęsta” w obszarze kształtowania umiejętności i kompetencji społecznych.

Liczne projekty badawcze realizowane m.in. w ZCB (patrz punkt V), a także w innych zespołach działających na Wydziale stanowią podstawę do formułowania tematów i realizacji przez studentów badań w ramach prac dyplomowych, a także w ramach projektów związanych z występującymi w programie studiów przedmiotami z zakresu

teleinformatyki i cyberbezpieczeństwa. Realizacja prac dyplomowych, ale także projektów w ramach poszczególnych przedmiotów obejmuje najczęściej:

- sformułowanie problemu,
- dobór metod i narzędzi badawczych,
- opracowanie i prezentację wyników badań.

7. STOSOWANE METODY KSZTAŁCENIA UWZGLĘDNIAJĄCE SAMODZIELNE UCZENIE SIĘ STUDENTÓW, AKTYWIZUJĄCE FORMY PRACY ZE STUDENTAMI ORAZ UMOŻLIWIAJĄCE STUDENTOM OSIĄGANIE ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ

W zestawie przedmiotów tworzących program studiów występują przedmioty, w których wykorzystane są m.in. następujące formy prowadzenia zajęć:

- projekty i zajęcia laboratoryjne, realizowane indywidualnie i w zespołach,
- zajęcia projektowe prowadzone zgodnie z koncepcją „design thinking”,
- zajęcia obejmujące szybkie prototypowanie,
- projekty i zajęcia laboratoryjne – także na przedmiotach prowadzonych tradycyjnie w inny sposób, np. na przedmiotach z zakresu matematyki,
- samodzielne uczenie się studentów (zdobywanie wiedzy wykraczającej poza materiał wykładowy) i prezentacja wyników tego samokształcenia na zajęciach grupowych,
- zajęcia wymagające formułowania i rozwiązywania problemów „otwartych”, w tym problemów o charakterze badawczym,
- zajęcia warsztatowo-treningowe,
- samoocena oraz wzajemna ocena studentów przez studentów.

Ww. formy prowadzenia zajęć i metody kształcenia występują w przedmiotach opisanych w załączniku 3.

Dobrym wskaźnikiem stopnia wykorzystania w proponowanym programie metod kształcenia uwzględniających samodzielne uczenie się studentów oraz aktywizujących form pracy ze studentami jest znaczne ograniczenie udziału wykładów jako formy prowadzenia zajęć w ogólnym bilansie „godzin kontaktowych”. W przedmiotach obowiązkowych występujących w planie studiów (bez dyplomowania) wykłady stanowią jedynie 39.0% godzin zajęć kontaktowych – wyraźnie mniej niż w przypadku innych programów studiów prowadzonych na Wydziale i na Uczelni. Szczególnie warta uwagi jest w tym kontekście nowa koncepcja nauczania matematyki, w której jedynie 35.3% zajęć ma formę wykładów, a pozostałe formy to ćwiczenia (23.5% zajęć), laboratoria (17.7% zajęć) i projekty (23.5% zajęć).

VII. PODSUMOWANIE

Uruchomienie programu studiów na kierunku Cyberbezpieczeństwo odpowiada na od dawna artykułowane oczekiwania podstawowych interesariuszy: wewnętrznych (studentów) i zewnętrznych (pracodawcy). Ich przedstawiciele brali aktywny udział w opracowaniu programu studiów.

Przedstawiona propozycja charakteryzuje się – jak się wydaje – kilkoma oryginalnymi, niezbyt powszechnie występującymi w praktyce polskich uczelni technicznych rozwiązaniami:

1. Zestaw kompetencji absolwenta (efektów uczenia się) uwzględnia nie tylko wymagania obowiązujących aktów prawnych, lecz także wymagania najbardziej rozpoznawalnej w świecie agencji akredytującej programy studiów technicznych – Accreditation Board for Engineering and Technology (ABET).
2. Zestaw zajęć na 1. semestrze został zaprojektowany z myślą o ułatwieniu „aklimatyzacji” nowo przyjętym studentom, ich wzajemnej integracji, wzmocnieniu zainteresowania studiami technicznymi, motywacji do studiowania na Wydziale, w szczególności na kierunku Cyberbezpieczeństwo, a zarazem z intencją wyposażenia ich w istotne kompetencje uniwersalne, przydatne w dalszym kształceniu. Obejmuje on m.in. następujące przedmioty/moduły zajęć:
 - *Szybkie prototypowanie inżynierskie*: zajęcia, w trakcie których studenci, początkowo indywidualnie, a następnie w zespołach, konstruują mini-roboty, rywalizując o osiągnięcie jak najlepszych parametrów swoich projektów;
 - *Pozatechniczne aspekty pracy inżyniera*: w trakcie zajęć, prowadzonych przez pracowników Wydziału Administracji i Nauk Społecznych oraz Wydziału Elektroniki i Technik Informacyjnych, mających charakter warsztatowo-treningowy, studenci rozwiązują problemy, analizując studia przypadku, biorąc pod uwagę społeczne, ekonomiczne, prawne, etyczne i inne pozatechniczne uwarunkowania działalności zawodowej inżyniera, pogłębiają wiedzę poprzez samodzielne wyszukanie i analizę treści odpowiednich materiałów źródłowych i przedstawiają wyniki swoich prac w formie opracowań i prezentacji, przygotowanych zgodnie omówionymi na zajęciach zasadami;
 - *Matematyka 1 – Wstęp do matematyki*: przedmiot obejmujący m.in. zajęcia projektowe – prezentację zagadnień związanych z praktycznymi zastosowaniami matematyki, wykraczających poza treści omawiane na wykładach;
 - *Matematyka 2 – Analiza*: przedmiot obejmujący m.in. zajęcia projektowe oraz zajęcia laboratoryjne realizowane z wykorzystaniem programu Mathematica, systemu zeszyt.online oraz portalu Khan Academy;
 - *Wprowadzenie do cyberbezpieczeństwa*: przedmiot zrywający z „tradycją” przedmiotów o wymiarze 1-2 punktów ECTS wprowadzających do studiów na danym kierunku, mających w znacznym stopniu charakter przewodnika po kierunku studiów ilustrowanego przykładami (pokazami), na rzecz „dużego” przedmiotu, w trakcie którego studenci współdziałają z prowadzącymi, realizując projekty związane z zagadnieniami cyberbezpieczeństwa;
 - *Podstawy techniki cyfrowej*: w trakcie zajęć praktycznych (projekt + laboratorium) studenci projektują, wykorzystując narzędzia firmy Intel oraz narzędzia typu open-source, oraz realizują w sprzęcie w nowoczesnym laboratorium proste układy cyfrowe.

Warto zwrócić uwagę, że już ma 1. semestrze student projektuje i konstruuje fizyczne obiekty, odnosząc w ten sposób pierwsze „realne” sukcesy w karierze inżyniera, którymi może pochwalić się (zdjęcia, film) w swoim środowisku.

3. Jednym z głównych celów programu jest rozwinięcie wśród studentów poczucia konieczności i umiejętności stałego aktualizowania i wzbogacania posiadanej wiedzy przez samokształcenie. Realizacji tego celu służy taka koncepcja prowadzenia przedmiotów, w której samodzielne poszukiwanie i analizowanie przez studenta różnego rodzaju materiałów źródłowych jest niezbędne dla wykonania zadań przewidzianych w programie przedmiotu. W opracowanym programie studiów występuje wiele przedmiotów, w których opisie w sposób jawny uwidoczniło się umiejętności samokształcenia jako warunku realizacji zadań, zwykle zadań o charakterze projektowym. Przykładami takich przedmiotów, prowadzonych na 1. semestrze, kiedy zdobycie umiejętności samokształcenia i zrozumienie potrzeby stałego wzbogacania posiadanej wiedzy ma szczególnie istotne znaczenie, są:
- *Pozatechniczne aspekty pracy inżyniera,*
 - *Szybkie prototypowanie inżynierskie,*
 - *Matematyka 1 oraz Matematyka 2,*
 - *Wprowadzenie do cyberbezpieczeństwa*

Program studiów na kierunku Cyberbezpieczeństwo spełnia ponadto postulaty sformułowane w kontekście prac programowych związanych z realizacją zadań w projekcie NERW PW, wynikające m.in. z analizy karier opinii studentów, absolwentów i pracodawców, m.in.:

- ograniczenie liczby przedmiotów w poszczególnych semestrach i w całym cyklu studiów, łączenie przedmiotów w większe, spójne merytorycznie moduły,
- względnie mały udział w programie studiów zajęć w formie tradycyjnie – bez interakcji ze studentami – prowadzonych wykładów,
- znacznym udziałem zajęć prowadzonych w formach aktywizujących studentów, nastawionych na zdobywanie wiedzy i umiejętności poprzez rozwiązywanie problemów,
- znaczna elastyczność (możliwość kształtowania indywidualnego programu i planu studiów, z wykorzystaniem zajęć prowadzonych na innych wydziałach PW i innych uczelniach).

Program powstawał we współpracy i „pod stałym nadzorem” najwyższej klasy ekspertów w zakresie cyberbezpieczeństwa, reprezentujących instytucje silnie zainteresowane zatrudnieniem absolwentów studiów na tym kierunku.

IX. ZAŁĄCZNIKI

1. Efekty uczenia się dla programu studiów I stopnia na kierunku Cyberbezpieczeństwo
2. Efekty uczenia się dla programów studiów I stopnia (undergraduate programs) określone w kryteriach akredytacji przyjętych przez Accreditation Board for Engineering and Technology
3. Opis przedmiotów
4. Matryca efektów uczenia się
5. Wskaźniki ilościowe
6. Wzorcowy plan studiów
7. Wymagania programowe
8. Formularz ankiety skierowanej do instytucji z otoczenia społeczno-gospodarczego