ZWIĄZEK BANKÓW POLSKICH

Materiał przyjęty przez Zarząd ZBP w dniu 7.05.2019 na podstawie rekomendacji Banków - Członków Komitetu Standardów Kwalifikacyjnych przy ZBP

Materiał ten został opracowany w Sekretariacie Systemu Standardów ZBP na bazie kwalifikacji przygotowanej przez Warszawski Instytut Bankowości we współpracy z ekspertami Prezydium Komitetu Cyberbezpieczeństwa Banków ZBP

Standard Kwalifikacyjny

Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych

/opis i wymagania/

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji:

Kwalifikacja jest skierowana do każdego pracownika instytucji finansowej oraz infrastruktury finansowej, tzn. banku, ubezpieczyciela, agenta rozliczeniowego i in., mającego kontakt z technologiami cyfrowymi, które mogą stwarzać cyberzagrożenie w środowisku własnym pracy oraz dla klientów. Kwalifikacja odpowiada także na potrzeby pracowników firm i instytucji infrastruktury sektora finansowego, takich jak Krajowa Izba Rozliczeniowa, Biuro Informacji Kredytowej, firmy-outsourcerzy banków, pracownicy pośredników finansowych i agregatorów płatności i in. Kwalifikacja może być także użyteczna dla pracowników, mających kontakt z reklamacjami i zgłoszeniami klientów, których działania mogą być narażone na cyberzagrożenia.

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]:

35 godzin (1 godzina dydaktyczna = 60 minut)

Instytucja szkoleniowa prowadząca proces szkoleniowy w formule e-learning:

Fundacja Warszawski Instytut Bankowości

Instytucja upoważniona do przeprowadzenia egzaminu zgodnie z zasadami Systemu Standardów ZBP, z wykorzystaniem zasad Zintegrowanego Systemu Kwalifikacji:

Związek Banków Polskich

Nazwa dokumentu potwierdzającego nadanie kwalifikacji:

Certyfikat sygnowany wspólnie przez ZBP i WIB

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności:

3 lata. Przedłużenie ważności kwalifikacji na podstawie potwierdzenia przez pracodawcę osoby posiadającej kwalifikację, że posiada zaktualizowane efekty uczenia się (wzór formularza potwierdzenia będzie dostępny na stronie www ZBP i WIB)

Zapotrzebowanie na kwalifikację

Jak wskazują najnowsze badania (Raport „Nadużycia w sektorze finansowym", KPF, EY, 2017), cyberprzestępczość jest najszybciej rosnącym zagrożeniem dla branży finansowej. Liczba cyberataków, w tym ataków od wewnątrz instytucji, wzrosła w ciągu ostatnich 2 lat o 160%.

Aktualnie trwają uzgodnienia projektu rozporządzenia Rady Ministrów w sprawie tzw. usług kluczowych. To akt wykonawczy do ustawy o krajowym systemie cyberbezpieczeństwa, która dotyczy implementacji dyrektywy Parlamentu Europejskiego i Rady (UE 2016/1148) z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (The Directive on security of network and information systems, NIS Directive). Projektowana ustawa wpisuje się w cel 5. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, zakładający osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów informatycznych istotnych dla funkcjonowania państwa. Konsultowane Rozporządzenie obejmie 67 podmiotów: 20 największych banków, po 10 największych banków spółdzielczych, SKOK-ów, ubezpieczycieli, instytucji płatniczych oraz NBP, BGK, GPW, PWPW, KDPW i CCP. Bezsprzecznie istotnym elementem przygotowań do skutecznego działania w krajowej sieci bezpieczeństwa, zgodnie z ww. regulacjami, będzie potwierdzenie transparentnymi certyfikatami wiedzy i umiejętności pracowników, którzy są ważnym ogniwem tej sieci. W tym kontekście warto przytoczyć rekomendację Europejskiego Kongresu Finansowego 2017 w obszarze cyberbezpieczeństwa sektora finansowego, która postuluje „zdefiniowanie i określenie potrzeb sektora finansowego w zakresie profilu kompetencyjnego z obszaru cyberbezpieczeństwa, wypracowanie oraz wdrożenie odpowiedniego programu edukacyjnego przy współpracy z organami oświaty i administracji publicznej"(http://www.efcongress.com/sites/default/files/cyberbezpieczestwo_sektora_finansowego.pdf). Wspomniany program edukacyjny powinien kończyć się potwierdzeniem kwalifikacji.

Według wyników najnowszego Sektorowego Badania Kompetencji Sektora Finansowego wśród stanowisk i kompetencji, na które w najbliższym czasie będzie rosło zapotrzebowanie w sektorze, znajduje się obszar cyberbezpieczeństwa (Raport SBKL 2018, SRK SF, dostępny na stronie internetowej Rady, www.rada.wib.org.pl).

Jak podaje GUS (Zatrudnienie i wynagrodzenia w gospodarce narodowej w I kwartale 2018 r., GUS 2018,

http://stat.gov.pl/obszary-tematyczne/rynek-pracy/pracujacy-zatrudnieni-wynagrodzenia-koszty-pracy/zatrudnienie-i-wynagrodzenia-w-gospodarce-narodowej-w-pierwszym-kwartale-2018-r-,1,30.html), wielkość zatrudnienia w działalności finansowej i ubezpieczeniowej wynosiła na koniec marca 2018 r. 275,5 tysiąca. Ta wielkość wyznacza prognozę zapotrzebowania na proponowaną kwalifikację, a na pewno na posiadanie efektów uczenia się zawartych w przedkładanej kwalifikacji.

W świetle powyższych procesów, trendów i prognoz, odczuwanej potrzeby zatrudniania pracowników posiadających aktualne umiejętności z zakresu stosowania zasad cyberbezpieczeństwa należy uznać, że efekty uczenia się zawarte w proponowanej kwalifikacji

odpowiadają wprost na kluczowe potrzeby sektora finansowego, jego podmiotów i pracowników. Ich znaczenie będzie rosło w kolejnych latach, stając się ważnym elementem wzmacniania bezpieczeństwa systemu finansowego w Polsce.

Źródła:

- Raport *Nadużycia w sektorze finansowym* z dn.24.10.2017, *Konferencja* Przedsiębiorstw Finansowych i EY. Raport dostępny:

http://www.ey.media.pl/pr/373780/cyberprzestepczosc-najszybciej-rosnacym-zagrozeniem-wedlug-branzy-fina

- https://legislacja.rcl.gov.pl/projekt/12312201/katalog/12512907#12512907
- https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
- http://www.efcongress.com/sites/default/files/cyberbezpieczestwo_sektora_finansowego.pdf

Raport Sektorowego Badania Kompetencji Sektora Finansowego (Sektorowa Rada ds. Kompetencji Sektora Finansowego) http://stat.gov.pl/obszary-tematyczne/rynek-pracy/pracujacy-zatrudnieni-wynagrodzenia-koszty-pracy/zatrudnienie-i-wynagrodzenia-w-gospodarce-narodowej-w-pierwszym-kwartale-2018-r-,1,30.html)

Typowe możliwości wykorzystania kwalifikacji

Osoba posiadająca kwalifikację "Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych", posiadając równocześnie wykształcenie kierunkowe związane z obszarem bankowości i finansów, może pracować w banku, bądź innej instytucji finansowej, a także instytucjach i firmach infrastruktury sektora finansowego, takich jak Krajowa Izba Rozliczeniowa, Biuro Informacji Kredytowej, firmy-outsourcerzy banków. Może też aplikować na stanowiska związane z bezpośrednią obsługą klienta, przyjmowaniem zgłoszeń klientów, a także wszędzie tam, gdzie jednym z zadań jest edukowanie klientów w zakresie podstaw cyberbezpieczeństwa: uświadamianie o zagrożeniach wynikających z funkcjonowania w cyberprzestrzeni oraz propagowanie zasady bezpiecznego korzystania z urządzeń i systemów teleinformatycznych.

Syntetyczna charakterystyka efektów uczenia się

Osoba posiadająca kwalifikację „Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych” jest przygotowana do realizacji swoich obowiązków w instytucji finansowej zgodnie z zasadami cyberbezpieczeństwa. Bezpiecznie funkcjonuje w środowisku teleinformatycznym i korzysta w sposób bezpieczny z narzędzi i technologii funkcjonujących w bankach i instytucjach finansowych. Identyfikuje zagrożenia, przeciwdziała ryzyku cyberzagrożenia, sygnalizuje sytuacje podejrzane i raportuje naruszenia. Ponadto, może też edukować klientów w zakresie podstaw cyberbezpieczeństwa: uświadamiać o zagrożeniach wynikających z funkcjonowania w cyberprzestrzeni oraz propagować zasady bezpiecznego korzystania z urządzeń i systemów teleinformatycznych.

Efekty uczenia się zawarte w kwalifikacji potwierdzają:

- podstawy wiedzy z zakresu bezpieczeństwa w cyberprzestrzeni, w tym w szczególny sposób w sektorze finansowym,
- umiejętność wykonywania prostych czynności w środowisku teleinformatycznym, zgodnie z instrukcjami, że identyfikuje elementarne uwarunkowania pracy z użyciem nowoczesnych technologii w instytucji finansowej.

Wyodrębnione zestawy efektów uczenia się

1. Bezpieczne korzystanie z urządzeń i systemów teleinformatycznych przez pracowników instytucji finansowych, 17 godzin.
2. Edukowanie klientów instytucji finansowych w zakresie bezpiecznego korzystania z bankowości internetowej, mobilnej i kart płatniczych, 6 godzin
3. Ochrona tożsamości swojej i klientów instytucji finansowej, 3 godziny
4. Stosowanie uniwersalnych przepisów zapewniających bezpieczeństwo informacji, infrastruktury teleinformatycznej, pracowników oraz klientów w instytucji finansowej, 9 godzin

Zestaw efektów uczenia się:	**01. Bezpieczne korzystanie z urządzeń i systemów teleinformatycznych przez pracowników instytucji finansowych**
Efekty uczenia się	**Kryteria weryfikacji**
Posługuje się hasłami do systemów informatycznych zgodnie z zasadami bezpieczeństwa	● Tworzy bezpieczne hasło ● Wymienia zasady przechowywania haseł ● Opisuje zasady ochrony haseł przed nieuprawnionym dostępem przez inne osoby ● Wyjaśnia powody i częstotliwość okresowej zmiany haseł ● Definiuje metodę dwuskładnikowego uwierzytelniania ● Wymienia zasady posługiwania się urządzeniami kryptograficznymi typu token/karta kryptograficzna ● Opisuje zagrożenia wynikające ze stosowania tych samych lub pokrewnych haseł w różnych serwisach
Używa komputera zachowując zasady bezpieczeństwa	● Wymienia zasady ochrony komputera przed dostępem osób niepowołanych ● Omawia powody aktualizacji systemu operacyjnego i aplikacji ● Sprawdza poprawność ustawień dotyczących aktualizacji systemu operacyjnego i aplikacji ● Wymienia powody oraz zasady wykorzystywania oprogramowania antywirusowego ● Sprawdza poprawność działania programu antywirusowego i ustawienia aktualizacji bazy sygnatur wirusów ● Podaje objawy infekcji komputera przez złośliwe oprogramowanie ● Omawia zasady reagowania w przypadku podjęcia podejrzenia o obecności wrogiego oprogramowania ● Objaśnia zasady bezpiecznego korzystania z publicznych i niezaufanych sieci komputerowych ● Przedstawia powody, zasady tworzenia i przechowywania kopii zapasowych ważnych plików oraz techniki archiwizowania informacji ● Podaje zasady bezpiecznego użytkowania nośników danych i przenośnych urządzeń teleinformatycznych

Korzysta ze smartfona zgodnie z zasadami bezpieczeństwa	● Objaśnia zasady instalowania i aktualizacji oprogramowania na smartfonie ● Opisuje objawy infekcji smartfona oraz cechy złośliwego oprogramowania ● Wymienia zasady ochrony smartfona i danych na nim przechowywanych ● Rozpoznaje zagrożenia związane z różnymi obszarami działalności na tym samym urządzeniu, np. współistnienie gier niewiadomego pochodzenia oraz operacji finansowych ● Objaśnia, że tzw. zaufane źródło takie jak np. Google Play nie gwarantuje nieobecności wrogiego kodu w aplikacji ● Opisuje zasady zarządzania uprawnieniami dla aplikacji, w szczególności wykrywania podejrzanych żądań o uprawnieniach
Korzysta z poczty elektronicznej z zachowaniem zasad bezpieczeństwa	● Rozpoznaje cechy charakterystyczne spamu, malware i phishingu ● Podaje sposoby reagowania na wymienione zagrożenia ● Stosuje zasady adresowania e-maili, zapewniające poufność korespondencji ● Stosuje zabezpieczenia komunikacji elektronicznej wysyłanej na zewnątrz, zapewniające poufność i integralność informacji ● Objaśnia, że metody sztucznej inteligencji mogą prowadzić do coraz lepszej personalizacji ataków i trudności z rozpoznaniem sfałszowanego emaila
Zestaw efektów uczenia się:	**02. Edukowanie klientów instytucji finansowych w zakresie bezpiecznego korzystania z bankowości internetowej, mobilnej i kart płatniczych**
Efekty uczenia się	**Kryteria weryfikacji**
Informuje, jak korzystać z bankowości internetowej i mobilnej zgodnie z zasadami bezpieczeństwa	● Objaśnia zasady bezpiecznego logowania się do bankowych serwisów internetowych ● Wymienia zasady dokonywania płatności w internecie i autoryzacji transakcji
Wyjaśnia, jak korzystać z kart płatniczych zgodnie z zasadami bezpieczeństwa	● Tworzy bezpieczny PIN do karty płatniczej ● Omawia zasady bezpiecznego przechowywania kart płatniczych i PINów do kart ● Przedstawia zasady korzystania z kart płatniczych przy płatnościach w terminalu, bankomacie i internecie, a w szczególności ochrony PINu do kart

Zestaw efektów uczenia się:	**03. Ochrona tożsamości swojej i klientów instytucji finansowej**
Efekty uczenia się	**Kryteria weryfikacji**
Chroni dane identyfikacyjne swoje i klientów przed ujawnieniem osobom niepowołanym	● Definiuje, co to są dane identyfikacyjne składające się na tożsamość danej osoby ● Opisuje zasady ograniczania ryzyka ujawnienia danych identyfikacyjnych w życiu prywatnym i w internecie ● Wymienia zasady i warunki udostępniania danych identyfikacyjnych swoich lub klienta innym osobom ● Wymienia zasady postępowania z dokumentami papierowymi i elektronicznymi, zawierającymi jakiekolwiek dane identyfikacyjne
Korzysta z serwisów internetowych i społecznościowych w sposób minimalizujący utratę tożsamości	● Wymienia zasady i warunki umieszczania informacji zawierających dane identyfikacyjne swoje lub klientów w ogólnodostępnych serwisach internetowych ● Opisuje sytuacje, w których może dojść do utraty tożsamości w serwisach internetowych i jak ujawnione dane mogą być wykorzystane przez osoby niepowołane
Zapewnia bezpieczeństwo dokumentów identyfikacyjnych	● Wyjaśnia, jak bezpiecznie przechowywać dokumenty identyfikacyjne (np. dowód osobisty, prawo jazdy, paszport) ● Opisuje procedury zgłaszania utraty dokumentu zawierającego dane identyfikacyjne ● Opisuje ryzyko związane ze skanowaniem, kopiowaniem i fotografowaniem dokumentów identyfikacyjnych ● Wymienia zasady postępowania z kopiami fizycznymi i elektronicznymi dokumentów identyfikacyjnych ● Opisuje zasady korzystania z dokumentów tożsamości z funkcjami elektronicznymi, w tym ochrony PINu do tych dokumentów
Zestaw efektów uczenia się:	**04. Stosowanie uniwersalnych przepisów zapewniających bezpieczeństwo informacji, infrastruktury teleinformatycznej, pracowników oraz klientów w instytucji finansowej**
Efekty uczenia się	**Kryteria weryfikacji**
Stosuje politykę bezpieczeństwa	● Uzasadnia potrzebę klasyfikacji informacji i stosowania adekwatnych do danej klasyfikacji zasad ochrony i postępowania ● Wymienia powody oraz zasady bezpiecznego niszczenia dokumentów papierowych i elektronicznych oraz nośników danych

	● Opisuje zasady usuwania informacji z pamięci komputera bez niszczenia nośnika fizycznego oraz zagrożenia wynikające z zawodności takich procedur ● Wymienia zasady ochrony dostępu do informacji przed osobami niepowołanymi ● Opisuje przykładową procedurę zgłaszania incydentów bezpieczeństwa ● Omawia zasady dostępu do pomieszczeń ● Objaśnia zasady "czystego biurka" (Clean Desk Policy) w miejscu pracy ● Opisuje zasadę niezbędnej wiedzy/informacji (tzw. Chinese Wall) ● Charakteryzuje generalne zasady kontaktu z mediami/klientami
Reaguje w sytuacjach próby popełnienia oszustwa przez cyberprzestępców	● Opisuje najbardziej popularne oszustwa wykorzystujące metody socjotechniczne, na które narażone są instytucje finansowe i klienci, w tym wykorzystujące sztuczną inteligencję ● Wymienia symptomy próby oszustwa lub manipulacji ● Wymienia sposoby zapobiegania przestępstwom socjotechnicznym i postępowania w przypadku stwierdzenia oszustwa