Możliwość dofinansowania

Cyberbezpieczeństwo w pracy biurowej – usługa szkoleniowa

Numer usługi 2026/04/09/161638/3474882

6 519,00 PLN brutto
5 300,00 PLN netto
181,08 PLN brutto/h
147,22 PLN netto/h
261,33 PLN cena rynkowa

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,9 / 5

656 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
36:00 h
01.06.2026 do 05.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do: • pracowników biurowych, • specjalistów administracyjnych, • pracowników działów wsparcia, • koordynatorów, • menedżerów, • właścicieli firm • osób wykonujących obowiązki zawodowe z wykorzystaniem komputera, poczty elektronicznej, dokumentów cyfrowych, systemów online i narzędzi chmurowych. Szkolenie przeznaczone jest dla osób, które przetwarzają dane, korzystają z Internetu i komunikacji elektronicznej, obsługują dokumenty i zasoby cyfrowe oraz chcą lepiej rozumieć zagrożenia cyberbezpieczeństwa i zasady bezpiecznej pracy w środowisku biurowym. Od uczestników oczekuje się podstawowej umiejętności korzystania z komputera i Internetu oraz gotowości do aktywnego udziału w zajęciach.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	31-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Liczba godzin usługi	36
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do rozpoznawania podstawowych zagrożeń cyberbezpieczeństwa w pracy biurowej, identyfikowania ryzyka związanego z pocztą elektroniczną, hasłami, danymi, urządzeniami i pracą online, rozróżniania zasad bezpiecznego korzystania z narzędzi cyfrowych oraz doboru działań ograniczających ryzyko incydentów w środowisku zawodowym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje podstawowe pojęcia związane z cyberbezpieczeństwem w pracy biurowej.	wskazuje znaczenie pojęć związanych z cyberbezpieczeństwem.	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia podstawowe rodzaje zagrożeń cyfrowych.	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje przykłady incydentów bezpieczeństwa w środowisku biurowym.	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia najczęstsze metody ataków cybernetycznych stosowanych wobec użytkowników biurowych.	wskazuje cechy phishingu i innych popularnych ataków.	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia komunikaty bezpieczne i podejrzane na podstawie opisu sytuacji.	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje skutki cyberprzestępstw finansowych w przestrzeni cyfrowej.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje zasady bezpiecznego stosowania haseł i metod uwierzytelniania.	wskazuje zasady tworzenia haseł zgodnych z aktualnymi standardami bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia funkcje menedżera haseł i autoryzacji dwuskładnikowej.	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje przyczyny łamania haseł przez cyberprzestępców.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia zasady ochrony danych i zasobów cyfrowych w pracy biurowej.	wskazuje zasady ochrony danych osobowych zgodnie z RODO w środowisku pracy.	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia sposoby zabezpieczania plików, folderów i nośników danych.	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje zasady wykonywania kopii zapasowych danych.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje zasady bezpiecznego korzystania z urządzeń, chmury i narzędzi online.	wskazuje korzyści i ryzyka korzystania z chmury.	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia funkcje programów antywirusowych, firewalli, VPN i ustawień prywatności.	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje zasady ochrony prywatności podczas korzystania z Internetu.	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia zagrożenia wynikające z socjotechniki i wykorzystania AI przez cyberprzestępców.	wskazuje przykłady socjotechnik stosowanych przez cyberprzestępców.	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia sygnały ostrzegawcze związane z wykorzystaniem AI w oszustwach	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje działania zmniejszające ryzyko manipulacji użytkownikiem.	Test teoretyczny z wynikiem generowanym automatycznie
Definiuje zasady postępowania po wystąpieniu incydentu bezpieczeństwa.	wskazuje podstawowe działania po wykryciu incydentu.	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia elementy procedury formalnej i komunikacyjnej po ataku.	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje błędy w reagowaniu na incydent na podstawie opisu sytuacji.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Dzień 1

- **Data realizacji:** 01.06.2026
- **Godziny realizacji:** 09:00–16:45
- **Liczba godzin dydaktycznych:** 9
- **Przerwy:** 2 przerwy po 30 minut

Moduł 1. Wprowadzenie do szkolenia i audyt cyberbezpieczeństwa (90 min)

- cele i zakres szkolenia,
- znaczenie cyberbezpieczeństwa w pracy biurowej,
- identyfikowanie obszarów ryzyka,
- wstęp do audytu cyberbezpieczeństwa użytkownika.

Moduł 2. Istota i podstawowe terminy w zakresie cyberbezpieczeństwa (90 min)

- podstawowe pojęcia związane z bezpieczeństwem cyfrowym,
- zagrożenia dla użytkownika biurowego,
- znaczenie incydentu bezpieczeństwa,
- rola użytkownika w ochronie informacji.

Moduł 3. Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA (90 min)

- podstawy prawne związane z bezpieczeństwem informacji,
- znaczenie wytycznych i dobrych praktyk,
- odpowiedzialność użytkownika,
- zalecenia ENISA w pracy biurowej.

Moduł 4. Najpopularniejsze ataki cybernetyczne (90 min)

- phishing, malware, ransomware i inne zagrożenia,
- przykłady ataków na użytkowników biurowych,
- skutki ataków,
- sygnały ostrzegawcze.

Moduł 5. Podsumowanie dnia szkoleniowego (45 min)

- uporządkowanie kluczowych zagadnień,
- omówienie podstawowych ryzyk,
- zebranie wniosków.

Dzień 2

- **Data realizacji:** 02.06.2026
- **Godziny realizacji:** 09:00–16:45
- **Liczba godzin dydaktycznych:** 9
- **Przerwy:** 2 przerwy po 30 minut

Moduł 6. Ćwiczenie: phishing i rozpoznawanie zagrożeń (90 min)

- cechy wiadomości phishingowych,
- elementy podejrzanych komunikatów,
- błędy użytkowników,
- zasady ostrożności.

Moduł 7. Przestępstwa finansowe w przestrzeni cyfrowej (90 min)

- oszustwa finansowe online,
- ryzyka związane z płatnościami i danymi dostępowymi,
- mechanizmy wyłudzania,
- ograniczanie ryzyka finansowego.

Moduł 8. Hasła zgodne ze standardami bezpieczeństwa cyfrowego (90 min)

- zasady tworzenia haseł,
- najczęstsze błędy użytkowników,
- bezpieczeństwo danych dostępowych,
- ochrona kont.

Moduł 9. Menedżer haseł i autoryzacja dwuskładnikowa w praktyce (90 min)

- jak działa menedżer haseł,
- jak wybrać rozwiązanie,
- dlaczego hasła są łamane,
- znaczenie 2FA.

Moduł 10. Podsumowanie dnia szkoleniowego (45 min)

- uporządkowanie zagadnień dotyczących phishingu i haseł,
- omówienie najważniejszych zasad ochrony dostępu,
- zebranie wniosków.

Dzień 3

- **Data realizacji:** 03.06.2026
- **Godziny realizacji:** 09:00–16:45
- **Liczba godzin dydaktycznych:** 9
- **Przerwy:** 2 przerwy po 30 minut

Moduł 11. Szyfrowanie plików, folderów i pendrive'ów w praktyce (90 min)

- znaczenie szyfrowania danych,
- zastosowania szyfrowania,
- ochrona nośników danych,
- ograniczanie ryzyka utraty informacji.

Moduł 12. Ochrona danych osobowych zgodnie z RODO i zastrzeganie PESEL (90 min)

- zasady ochrony danych osobowych,
- bezpieczeństwo danych w pracy biurowej,
- znaczenie ochrony tożsamości,
- zastrzeganie numeru PESEL.

Moduł 13. Jak robić backup danych? (90 min)

- znaczenie kopii zapasowych,
- rodzaje backupu,
- zasady planowania kopii bezpieczeństwa,
- błędy w przechowywaniu danych.

Moduł 14. Porządkowanie danych i bezpieczna organizacja informacji (90 min)

- organizacja plików i dokumentów,
- zasady ograniczania nieuprawnionego dostępu,
- bezpieczne przechowywanie informacji,
- dobre praktyki pracy z dokumentami cyfrowymi.

Moduł 15. Podsumowanie dnia szkoleniowego (45 min)

- uporządkowanie kluczowych zagadnień,
- omówienie zasad ochrony danych i kopii zapasowych,
- zebranie wniosków.

Dzień 4

- **Data realizacji:** 04.06.2026
- **Godziny realizacji:** 09:00–16:45
- **Liczba godzin dydaktycznych:** 9
- **Przerwy:** 2 przerwy po 30 minut

Moduł 16. Chmura, prywatność i bezpieczeństwo urządzeń (90 min)

- dlaczego warto korzystać z chmury,
- korzyści i ryzyka korzystania z chmury,
- programy antywirusowe, firewall, VPN, cookies i tryb incognito,
- zasady bezpiecznej konfiguracji środowiska pracy.

Moduł 17. AI i socjotechniki wykorzystywane przez cyberprzestępców (90 min)

- wykorzystanie AI w oszustwach cyfrowych,
- sygnały ostrzegawcze,
- socjotechniki wykorzystywane przez hakerów,
- ograniczanie ryzyka manipulacji.

Moduł 18. Co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna (90 min)

- działania po incydencie,
- procedura formalna i komunikacyjna,
- błędy w reagowaniu,
- zasady ograniczania skutków ataku.

Moduł 19. Podsumowanie szkolenia i przygotowanie do walidacji (90 min)

- uporządkowanie kluczowych zagadnień,
- omówienie najważniejszych zasad cyberbezpieczeństwa w pracy biurowej,
- przypomnienie zasad zaliczenia usługi,
- informacje końcowe.

Walidacja – test teoretyczny z wynikiem generowanym automatycznie (45 min)

1) Godziny i forma

Szkolenie odbywa się w godzinach dydaktycznych (1 godz. = 45 minut) łącznie 36 godzin dydaktycznych. Usługa realizowana jest zdalnie, w czasie rzeczywistym, na platformie Google Meet. Przerwy organizacyjne i obiadowe nie są wliczane do czasu szkolenia. Grupy: 1–30 osób.

2) Metoda prowadzenia

Zajęcia prowadzone są metodami interaktywnymi i aktywizującymi: krótkie wprowadzenia trenera, studia przypadków, ćwiczenia indywidualne i grupowe, symulacje sytuacji konfliktowych, warsztaty, dyskusje moderowane, analiza przykładów z praktyki zawodowej uczestników oraz praca nad indywidualnym planem rozwoju.

3) Grupa docelowa. Usługa skierowana jest do:

- pracowników biurowych,
- specjalistów administracyjnych,
- pracowników działów wsparcia,
- koordynatorów,

- menedżerów,
- właścicieli firm
- osób wykonujących obowiązki zawodowe z wykorzystaniem komputera, poczty elektronicznej, dokumentów cyfrowych, systemów online i narzędzi chmurowych.

4) Cel edukacyjny

Usługa przygotowuje uczestnika do rozpoznawania podstawowych zagrożeń cyberbezpieczeństwa w pracy biurowej, identyfikowania ryzyka związanego z pocztą elektroniczną, hasłami, danymi, urządzeniami i pracą online, rozróżniania zasad bezpiecznego korzystania z narzędzi cyfrowych oraz doboru działań ograniczających ryzyko incydentów w środowisku zawodowym.

5) Walidacja – zasady zaliczenia

Walidacja efektów uczenia się zostanie przeprowadzona w formie testu teoretycznego on-line z wynikiem generowanym automatycznie.

- Warunkiem zaliczenia walidacji jest uzyskanie co najmniej 80% poprawnych odpowiedzi w teście.
- Warunkiem otrzymania zaświadczenia o ukończeniu usługi jest:
- frekwencja na poziomie co najmniej 80% czasu szkolenia (bez przerw),
- uzyskanie wyniku co najmniej 80% poprawnych odpowiedzi w teście walidacyjnym.

W ramach tej metody walidacji ocenie podlega wyłącznie poprawność odpowiedzi udzielonych przez uczestnika w teście.

Harmonogram

Liczba pozycji harmonogramu: 28

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 28 Moduł 1. Wprowadzenie do szkolenia i audyt cyberbezpieczeństwa – wideokonferencja	WOJCIECH GRACZYK	01-06-2026	09:00	10:30	01:30
2 z 28 Przerwa	WOJCIECH GRACZYK	01-06-2026	10:30	11:00	00:30
3 z 28 Moduł 2. Istota i podstawowe terminy w zakresie cyberbezpieczeństwa – wideokonferencja	WOJCIECH GRACZYK	01-06-2026	11:00	12:30	01:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 28 Moduł 3. Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA – ćwiczenia	WOJCIECH GRACZYK	01-06-2026	12:30	14:00	01:30
5 z 28 Przerwa	WOJCIECH GRACZYK	01-06-2026	14:00	14:30	00:30
6 z 28 Moduł 4. Najpopularniejsze ataki cybernetyczne – wideokonferencja	WOJCIECH GRACZYK	01-06-2026	14:30	16:00	01:30
7 z 28 Moduł 5. Podsumowanie dnia szkoleniowego – wideokonferencja	WOJCIECH GRACZYK	01-06-2026	16:00	16:45	00:45
8 z 28 Moduł 6. Ćwiczenie: phishing i rozpoznawanie zagrożeń – ćwiczenia	WOJCIECH GRACZYK	02-06-2026	09:00	10:30	01:30
9 z 28 Przerwa	WOJCIECH GRACZYK	02-06-2026	10:30	11:00	00:30
10 z 28 Moduł 7. Przestępstwa finansowe w przestrzeni cyfrowej – wideokonferencja	WOJCIECH GRACZYK	02-06-2026	11:00	12:30	01:30
11 z 28 Moduł 8. Hasła zgodne ze standardami bezpieczeństwa cyfrowego – ćwiczenia	WOJCIECH GRACZYK	02-06-2026	12:30	14:00	01:30
12 z 28 Przerwa	WOJCIECH GRACZYK	02-06-2026	14:00	14:30	00:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 28 Moduł 9. Menedżer haseł i autoryzacja dwuskładnikowa w praktyce – wideokonferencja	WOJCIECH GRACZYK	02-06-2026	14:30	16:00	01:30
14 z 28 Moduł 10. Podsumowanie dnia szkoleniowego – wideokonferencja	WOJCIECH GRACZYK	02-06-2026	16:00	16:45	00:45
15 z 28 Moduł 11. Szyfrowanie plików, folderów i pendrive'ów w praktyce – ćwiczenia	WOJCIECH GRACZYK	03-06-2026	09:00	10:30	01:30
16 z 28 Przerwa	WOJCIECH GRACZYK	03-06-2026	10:30	11:00	00:30
17 z 28 Moduł 12. Ochrona danych osobowych zgodnie z RODO i zastrzeganie PESEL – wideokonferencja	WOJCIECH GRACZYK	03-06-2026	11:00	12:30	01:30
18 z 28 Moduł 13. Jak robić backup danych? – ćwiczenia	WOJCIECH GRACZYK	03-06-2026	12:30	14:00	01:30
19 z 28 Przerwa	WOJCIECH GRACZYK	03-06-2026	14:00	14:30	00:30
20 z 28 Moduł 14. Porządkowanie danych i bezpieczna organizacja informacji – wideokonferencja	WOJCIECH GRACZYK	03-06-2026	14:30	16:00	01:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 28 Moduł 15. Podsumowanie dnia szkoleniowego – wideokonferencja	WOJCIECH GRACZYK	03-06-2026	16:00	16:45	00:45
22 z 28 Moduł 16. Chmura, prywatność i bezpieczeństwo urządzeń – wideokonferencja	WOJCIECH GRACZYK	05-06-2026	09:00	10:30	01:30
23 z 28 Przerwa	WOJCIECH GRACZYK	05-06-2026	10:30	11:00	00:30
24 z 28 Moduł 17. AI i socjotechniki wykorzystywane przez cyberprzestępców – ćwiczenia	WOJCIECH GRACZYK	05-06-2026	11:00	12:30	01:30
25 z 28 Moduł 18. Co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna – wideokonferencja	WOJCIECH GRACZYK	05-06-2026	12:30	14:00	01:30
26 z 28 Przerwa	WOJCIECH GRACZYK	05-06-2026	14:00	14:30	00:30
27 z 28 Moduł 19. Podsumowanie szkolenia i przygotowanie do walidacji – ćwiczenia	WOJCIECH GRACZYK	05-06-2026	14:30	16:00	01:30
28 z 28 Walidacja – test teoretyczny z wynikiem generowanym automatycznie	WOJCIECH GRACZYK	05-06-2026	16:00	16:45	00:45

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 519,00 PLN
Koszt przypadający na 1 uczestnika netto	5 300,00 PLN
Koszt osobogodziny brutto	181,08 PLN
Koszt osobogodziny netto	147,22 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

WOJCIECH GRACZYK

Wojciech Graczyk — szkoleniowiec i walidator, Prezes Zarządu KORYCKI & GRACZYK CONSULTING GROUP sp. z o.o. Posiada ponad 3000 udokumentowanych godzin prowadzenia szkoleń oraz doświadczenie w realizacji ponad 200 procesów walidacyjnych. W ciągu ostatnich pięciu lat przeprowadził ponad 500 godzin zegarowych szkoleń w zakresie bezpieczeństwa cyfrowego w różnym stopniu zaawansowania.

Posiada trzy certyfikaty trenerskie potwierdzające kompetencje do prowadzenia szkoleń dla osób dorosłych, liczne certyfikaty w obszarze kompetencji menedżerskich oraz zarządzania. Obecnie jest administratorem danych osobowych w spółce pod firmą KORYCKI & GRACZYK CONSULTING GROUP sp. z o.o. oraz jest odpowiedzialny za zabezpieczanie systemów, danych oraz informacji w infrastrukturze firmowej. Ukończył specjalistyczne szkolenia w zakresie zaawansowanych technik cyberbezpieczeństwa ze szczególnym uwzględnieniem prawnych aspektów cyberbezpieczeństwa oraz ustalania haseł. Dodatkowo ukończył kurs w zakresie ochrony danych osobowych na wydziale psychologii i prawa Uniwersytetu SWPS w Poznaniu.

Aktualnie studiuje na V roku prawa, pogłębiając wiedzę z zakresu prawa w biznesie. Łączy perspektywę merytoryczną trenera z podejściem procesowym i najwyższą starannością operacyjną, kładąc nacisk na zgodność, transparentność i efekt dla klienta.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Komplet materiałów zostanie wysłany w wiadomości e-mail przed rozpoczęciem szkolenia do każdego z Uczestników. Będzie to skrypt wraz z prezentacją (w formacie PDF).

Warunki uczestnictwa

Ukończony 18 rok życia.

Informacje dodatkowe

1. Podstawa prawna zwolnienia przedmiotowego z podatku VAT: §3 ust.1 pkt 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U. z 2015 r., poz.736). W przypadku gdy Uczestnik realizuje szkolenie bez dofinansowania (komercyjnie) lub wartość dofinansowania jest mniejsza niż 70% wartości szkolenia, to do ceny netto dodaje się należny podatek VAT w wysokości 23%.

2. Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub Partnera Operatora w danym projekcie PSF lub w którymkolwiek Regionalnym Programie lub FERS albo przez podmiot powiązany z Operatorem lub Partnerem kapitałowo lub osobowo.

Warunki techniczne

1. Platforma komunikacyjna – Google Meet.

2. Wymagania sprzętowe: komputer z aktualnym systemem (Windows 10 lub nowszy / macOS 12 lub nowszy / aktualna dystrybucja Linux), aktualną przeglądarkę (Chrome/Edge/Firefox/Safari – co najmniej dwie ostatnie wersje), stabilne łącze internetowe o przepustowości min. 10 Mb/s (pobieranie) i 2 Mb/s (wysyłanie), sprawną kamerę komputerową i mikrofon, sprawne słuchawki/ głośniki.

3. Okres ważności linku: od godziny zegarowej przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny zegarowej po zakończeniu szkolenia w dniu ostatnim.

Kontakt

Sylwia Dworzyńska

E-mail sylwia.dworzynska@hameracapital.eu
Telefon (+48) 661 336 370