Силабус освітнього компонента
Програма навчальної дисципліни

Основи професійної психології

Шифр та назва спеціальності
125 - Кібербезпека та захист інформації

Інститут
Соціально-гуманітарних технологій

Освітня програма
Освітньо-професійна програма Кібербезпека

Кафедра
Педагогіки та психології управління соціальними системами імені акад. І.А. Зязюна)

Рівень освіти
Магістр

Тип дисципліни
Загальна підготовка, вибіркова

Семестр
Третій

Мова викладання
Українська

Викладачі, розробники

ПІДБУЦЬКА Ніна Вікторівна

Nina.Pidbutska@khpi.edu.ua
Доктор психологічних наук, професор, завідувач кафедри педагогіки та психології управління соціальними системами імені акад. І.А. Зязюна НТУ «ХПІ», автор понад 100 наукових та науково-методичних праць. Провідний лектор з дисципліни: «Основи професійної психології».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна спрямована на розгляд широкого кола питань щодо ознайомлення здобувачів із знаннями про загальну природу психічного, психологічних властивостей професійної діяльності фахівця. Особливу увагу в курсі приділено практичним знанням з прикладних аспектів професійної діяльності (мотивації, конфліктів та ін.).

Мета та цілі дисципліни

Забезпечення теоретичної підготовки з психологічних властивостей професійної діяльності фахівця, а також практичних знань з прикладних аспектів професійної діяльності (мотивації, конфліктів та ін.).

Формат занять

Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., практичні (семінарські) заняття – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Не передбачені освітньою програмою.

Особливості дисципліни, методи та технології навчання

Під час вивчення дисципліни використовується брейм-стормінг, діалогове навчання, ігрові (ділові ігри);документальні (психобіографічний аналіз, складання документів); проблемні (кейси);інтерактивні(ментальні карти, виступи-презентації);самостійні (творчі завдання. опрацювання літератури);тренінгові (рефлексія, обговорення)

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Поняття про особистість, її структуру.
Загальна характеристика поняття особистості. Філогенез людини. Співвідношення індивід, індивідуальність, особистість. Структура особистості.
Тема 2. Особливості психіки людини, її структура.
Загальна характеристика психіки. Структура психіки людини. Психічні процеси, стани, властивості особистості.
Тема 3. Професіограма та психограма фахівця.
Загальна характеристика професіограми фахівця. Професіограма та психограма фахівця. Професійно важливі якості фахівця.
Тема 4. Психологічні особливості професійного становлення фахівця.
Загальна характеристика професійного становлення. Етапи професійного становлення фахівців. Професійна придатність фахівця. Професійна готовність фахівця.
Тема 5. Професійна мотивація, шляхи її розвитку.
Загальна характеристика мотивації. Класифікація теорій мотивацій. Особливості професійної мотивації. Шляхи розвитку професійної мотивації.
Тема 6. Психологічні аспекти ділового спілкування.
Загальна характеристика та структура феномену спілкування. Бар'єри спілкування. Поняття ділового спілкування. Умови успішного ділового спілкування.
Тема 7. Психологічні аспекти вирішення конфліктів.
Загальна характеристика конфліктів. Класифікація конфліктів. Умови попередження та вирішення конфліктів.
Тема 8. Соціально-психологічний клімат, способи його формування.

Загальна характеристика соціально-психологічного клімату. Етапи формування соціально-психологічного клімату. Умови побудови гармонійного соціально-психологічного клімату

Теми практичних занять

Тема 1. Професіограма та психограма фахівця з маркетингу.
Загальна характеристика професіограми фахівця. Професіограма та психограма фахівця. Професійно важливі якості фахівця з маркетингу. Побудова Професіограма та психограма фахівця.
Тема 2. Психологічні особливості професійного становлення фахівця.
Загальна характеристика професійного становлення фахівця. Етапи професійного становлення фахівця. Професійна придатність фахівця. Професійна готовність фахівця.
Тема 3. Професійна мотивація, шляхи її розвитку.
Класифікація теорій мотивацій. Особливості професійної мотивації. Розробка шляхів розвитку професійної мотивації фахівця.
Тема 4. Психологічні аспекти ділового спілкування.
Загальна характеристика та структура феномену спілкування. Бар'єри спілкування у професійній діяльності фахівця. Поняття ділового спілкування. Умови успішного ділового спілкування фахівця.

Теми лабораторних робіт

немає

Самостійна робота

Курс передбачає виконання завдань за темами: "Моя професійна придатність", "Професіограма та психограма фахівця ", "Шляхи підвищення мотивації до професійної діяльності" , "Шляхи підвищення рівня комунікативної компетеності фахівця".
Студентам також рекомендуються додаткові матеріали (відео, фільми) для самостійного вивчення та аналізу.

Література та навчальні матеріали

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Підбуцька Н. В. Психологічні основи професіоналізму інженера: структура, динаміка та закономірності розвитку : [монографія] / Н. В. Підбуцька; М-во освіти і науки України, Нац. техн. ун-т «Харків. політехн. ін-т». – Харків : «Діса плюс», 2016. – 295 с. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/f922a271-fccc-4d29-8597-4b3f669d3439/content
2. Романовський О. Г. Конфліктне спілкування в інженерній діяльності : навч. посібник / О. Г. Романовський, О. С. Пономарьов, Н. В. Підбуцька ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2013. – 292 с. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/51c91ae5-d59f-48d2-ba5d-58a3a9326f2a/content

Базова література

3. Кокун О. М. Психологія професійного становлення сучасного фахівця : монографія / Кокун О. М. ; Ін–т психології ім. Г. С. Костюка НАПН України. — Київ : ДП «Інформ. — аналіт. агенство», 2012. — 200 с. URL: https://lib.iitta.gov.ua/id/eprint/1651/1/%D0%9A%D0%BE%D0%BA%D1%83%D0%BD_%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80_12.pdf
4. Ложкін Г. В. Психологія праці : навч. посібник для студ. вищ. навч. закладів / Ложкін Г. В., Волянюк Н. Ю., Солтик О. О. — Хмельницький, 2013. — С. 147–153. URL: https://psy.kpi.ua/lozhkin/posibniki/
5. Орбан-Лембрик, Лідія Ернестівна. Психологія професійної комунікації [Текст] : монографія / Л. Е. Орбан-Лембрик. - Чернівці : Книги - ХХІ, 2019. - 527 с. URL: https://catalog.lounb.org.ua/bib/390561

6. Психологія праці у звичайних та екстримальних умовах [Текст] : навч. посіб. для студентів ВНЗ / [М. С. Корольчук, В. М. Корольчук, С. М. Миронець та ін. ; заг. ред. М. С. Корольчук] ; Київ. нац. торг.-екон. ун-т. - Київ : Київ. нац. торг.-екон. ун-т, 2015. - 651 с.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

100% підсумкової оцінки складаються з результатів оцінювання у вигляді заліку (20%) та поточного оцінювання (80%). Залік: усна відповідь. Поточне оцінювання: активна участь у обговореннях відбувається за лекційним матеріалом та матеріалом самостійної роботи (30%), практичні завдання (20%), написання контрольних робіт (10%).

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено

Дата погодження, підпис
28.08.2024

Завідувач кафедри
Ніна ПІДБУЦЬКА

Дата погодження, підпис
28.08.2024

Гарант ОП
Ольга КОРОЛЬ