



Силабус освітнього компонента

Програма навчальної дисципліни



Бізнес інтеллідженс

Шифр та назва спеціальності

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Національна безпека у сфері кіберзахисту

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

7

Мова викладання

Українська

Викладачі, розробники

**КОРОЛЬОВ Роман Володимирович**

korolevrv01@ukr.net

Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХП».

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтеллідженс», «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Бізнес інтеллідженс" є обов'язковою навчальною дисципліною.

Дисципліна спрямована на придбання студентами навичок з створення бізнес звітів в сучасних системах бізнес-аналізу QlikView, Qlik Sense, Microsoft Power BI.

Мета та цілі дисципліни

Надання студентам знань та вмінь щодо застосування ефективних інструментальних засобів обробки бізнес-даних та сприяння системному уявленню архітектури відповідних технологічних платформ на основі веб-рішень та хмарних обчислень.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ-7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
ФК-2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
ФК-8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

ФК-11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-4. Вільно спілкуватися державною мовою.

ПРН-7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

ПРН-8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ПРН-10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ПРН-12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.

ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.

ПРН-17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Організація і безпека баз даних.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання,

які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Основні терміни та визначення.

Особливості технологій глибинного аналізу даних (Data Mining), сховищ даних (Data Warehousing), бізнес-аналітики (Business Analytics) та місце BI у сучасних бізнес-процесах підприємств та організацій.

Тема 2. Основи стратегічного менеджмента.

Інструментарій стратегічного менеджмента. Базові інструменти стратегічного менеджмента. Шляхи досягнення стратегічних цілей.

Тема 3. Фінансові критерії для прийняття бізнес рішень.

Фінансова звітність компанії як універсальна мова спілкування всіх менеджерів. Поточний бюджет як контракт між власником та командою менеджерів.

Тема 4. Управляти бізнесом – управляти ризиками.

Стратегічні ризики компанії: чого слід уникнути, а чим скористатися. Основні ризики бізнесу. Упорядкування основних ризиків бізнесу.

Тема 5. Система бізнес-аналізу QlikView.

Введення в термінологію. Поняття асоціативної моделі. Огляд компонентів QlikView. Джерела даних для моделей QlikView.

Тема 6. Система бізнес аналізу QlikSense.

Введення в термінологію. Поняття асоціативної моделі. Огляд компонентів QlikSense. Джерела даних для моделей QlikSense.

Тема 7. Інструментальні засоби BI. Приклад застосування Microsoft Power BI для візуалізації бізнес-даних та створення звітів.

Особливості технологій хмарних обчислень у рішенні завдань BI. Введення в термінологію. Поняття асоціативної моделі. Огляд компонентів Microsoft Power BI. Джерела даних для моделей Microsoft Power BI.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Збір та аналіз даних. Створення презентації в PowerPoint. Представлення проєкту.

Тема 2. Багатовимірний аналіз даних (OLAP-технології) за допомогою табличного процесора Excel.

Тема 3. Робота із середовищем QlikView.

Тема 4. Робота із середовищем QlikSense.

Тема 5. Робота із середовищем Microsoft Power BI.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surli.pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література:

1. Савчук В.П. Оцифрований менеджмент: Business Intelligence для ТОПів. К.: "Баланс Бізнес Букс", 2017. - 504 с.
https://kniga.biz.ua/pdf/7640-ocifrovanniy-management.pdf?srsId=AfmBOoqcpOrriV27YNt0brY-VIGd6sqfcqha6-Il4v-FReg88pWm_cVI
2. Величко О.М Основи системного аналізу і прийняття оптимальних рішень підручник /О.М. Величко, Т.Б. Гордієнко. – К: Олді, 2021. – 672 с.
4. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
<http://kist.ntu.edu.ua/textPhD/tzi.pdf>
5. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсєєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
6. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсєєв, О.В. Мілов, С.Е. Остапов, О.В. Северінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>.

Додаткова література :

7. A Guide to the Business Analysis Body of Knowledge (BABOK Guide). – 3rd Edition. – IIBA. – 2015. – 502 p.
[https://www.google.com.ua/books/edition/A+Guide+to+the+Business+Analysis+Body+of+Knowledge+\(BABOK+Guide\).+%E2%80%933rd+Edition.+%E2%80%93IIBA.+%E2%80%932015.+%E2%80%93502+p.&printsec=frontcover](https://www.google.com.ua/books/edition/A+Guide+to+the+Business+Analysis+Body+of+Knowledge+(BABOK+Guide).+%E2%80%933rd+Edition.+%E2%80%93IIBA.+%E2%80%932015.+%E2%80%93502+p.&printsec=frontcover)
8. Ferrari A. Introducing Microsoft Power BI / Alberto Ferrari and Marco Russo // Microsoft Press, 2016. – 189 p.
<https://f.eruditor.link/file/1991775/>
9. Collier Michael S. Microsoft Azure Essentials: Fundamentals of Azure, Second Edition / Michael S. Collier and Robin E. Shahan // Microsoft Press, 2016. – 246 p.
https://books.google.com.ua/books/about/Microsoft+Azure+Essentials+Fundamentals.html?hl=el&id=EfFxBgAAQBAJ&redir_esc=y
10. Barnes J. Microsoft Azure Essentials: Azure Machine Learning / Jeff Barnes // Microsoft Press, 2015. – 237 p.
https://books.google.com.ua/books/about/Microsoft+Azure+Essentials+Azure+Machine.html?id=fserCAAQBAJ&redir_esc=y
11. Browne D. IBM Cognos Business Intelligence V10.1 Handbook / Dean Browne, Brecht Desmeijter, Rodrigo Frealdo Dumont, Armin Kamal and others // An IBM Redbooks publication, 2010. – 572 p.
<https://www.redbooks.ibm.com/redbooks/pdfs/sg247912.pdf>
12. Guide to the Business Analysis Body of Knowledge (BABOK Guide). – 3rd Edition. – IIBA. – 2015. – 502 p.
<https://www.twirpx.com/file/1690179/>
13. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
<http://monograph.com.ua/pctc/catalog/view/64/52/231-1>
14. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
<http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2>
15. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
<http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2>.

16. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсєєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с.
<http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/.pdf2.pdf>.
17. Євсєєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсєєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.
<http://repository.hneu.edu.ua/bitstream/123456789/24508/1/2020-%d0%84%d0%b2%d1%81%d0%b5%d1%94%d0%b2%20%d0%a1%20%d0%9f%2c%20%d0%9c%d1%96%d0%bb%d0%be%d0%b2%20%d0%9e%20%d0%92%2c%20%d0%9a%d0%be%d1%80%d0%be%d0%bb%d1%8c%20%d0%9e%20%d0%93.pdf>.
18. Security of Linux operating system: laboratory workshop / S. Yevseiev, S. Pogasiy, A. Goloskokova, O. Shmatko, M. Melnik (Кібербезпека: безпека операційної системи Linux: лабораторний практикум: навчальний посібник для студентів вищих навчальних закладів англійською мовою / Євсєєв С.П., Погасій С.С., Голоскокова А.О., Шматко О.В., Мельник М.О. – Львів: Видавництво «Новий Світ – 2000», 2021. – 256 с.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- залік: 40% семестрової оцінки

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

28.08.2024



Завідувач кафедри

Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП

Андрій ТКАЧОВ