



Силабус освітнього компонента
Програма навчальної дисципліни



**Розробка корпоративних
інформаційних систем**

Шифр та назва спеціальності

257 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Управління інформаційною безпекою

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

4,5

Мова викладання

Українська

Викладачі, розробники



ГАВРИЛОВА Алла Андріївна

alla.havrylova@khpi.edu.ua

PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 30, з них патентів на корисну модель 2, 3 монографії, з яких 1 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з дисциплін: «Вступ до спеціальності. Ознайомча практика», «Організаційне забезпечення захисту інформації» у студентів бакалавріата

[Детальніше про викладача на сайті кафедри](#)



ТКАЧОВ Андрій Михайлович

andrii.tkachov@khpi.edu.ua

Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: «Мережне програмування», «Розробка та аналіз алгоритмів», «Технології програмування», «Інструментальні засоби програмування», «Веб безпека», «Основи технічного захисту інформації», у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна «Розробка корпоративних інформаційних систем» є навчальною дисципліною з циклу професійної вибіркової підготовки блоку 03 “Innovation Campus” для формування у студентів теоретичних та практичних вмінь з програмної розробки інформаційних систем, що захищаються. Вона викладається у четвертому та п'ятому семестрах. У курсі передбачено два змістових модулі та дві контрольні роботи.

Мета та цілі дисципліни

Отримання студентами поглиблених знань з теорії та навичок практичної розробки інформаційних систем для забезпечення роботи великих підприємств, корпорацій та інших бізнес-структур будь-якої галузі економіки та форми власності.

Формат занять

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

Компетентності

КЗ-6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

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-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційною безпекою.

ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

ПРН-17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

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

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 180 год.: лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 116 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Іноземна мова, Основи програмування, Розробка та аналіз алгоритмів, Структури даних, Технології програмування, Інструментальні засоби програмування.

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, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Семестр 1

Тема 1. Основні поняття корпоративних інформаційних систем.

Перелік питань.

Тема 2. Принципи організації корпоративних інформаційних систем.

Перелік питань.

Тема 3. Особливості архітектури корпоративних інформаційних систем.

Перелік питань.

Тема 4. Проектування корпоративних інформаційних систем.

Перелік питань.

Тема 5. Особливості розробки корпоративних інформаційних систем.

Перелік питань.

Семестр 2

Тема 6. Впровадження корпоративних інформаційних систем.

Перелік питань.

Тема 7. Міграція в корпоративних інформаційних системах.

Перелік питань.

Тема 8. Забезпечення якості корпоративних інформаційних систем.

Перелік питань.

Тема 9. Підтримка та супровід корпоративної інформаційної системи.

Перелік питань.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Семестр 1

Тема 1. Аналіз предметної області та формування вимог до корпоративної інформаційної системи.

Тема 2. Проектування та розробка модулів корпоративної інформаційної системи.

Тема 3. Розробка прототипу користувацького інтерфейсу.

Семестр 2

Тема 4. Розробка моделі бази даних відповідно до архітектури корпоративної інформаційної системи.

Тема 5. Розробка тестів для аналізу роботи корпоративної інформаційної системи.

Тема 6. Розробка довідкової системи корпоративної інформаційної системи.

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://surl.li/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. Татарчук М.І. (2014) Корпоративні інформаційні системи. Підручник. Київ: КНЕУ.
<https://javalibre.com.ua/java-book/book/2908519>
2. Langer A. M. Guide to Software Development: Designing and Managing the Life Cycle. Second Edition Springer.
https://www.google.com.ua/books/edition/Guide_to_Software_Development/I9kyDQAAQBAJ?hl=ru&gbpv=1&dq=Langer+A.+M.+Guide+to+Software+Development:+Designing+and+Managing+the+Life+Cycle.+Second+Edition+Springer.&printsec=frontcover
3. Ушакова І. О. (2015) Проектування інформаційних систем. Практикум Харків : Вид. ХНЕУ
<http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/10473/1/2015-%d0%a3%d1%88%d0%b0%d0%ba%d0%be%d0%b2%d0%b0%20%d0%86.%d0%9e.pdf>
4. Greasley A., Hickie, S, P. (2018) Business Information Systems: Technology, Development and Management for the Modern Business 6th edition Pearson Education UK:

https://books.google.com.ua/books?id=jSTmRXVaOjQC&printsec=frontcover&hl=ru&source=gb_s_ggmmmary_r&cad=0#v=onepage&q&f=false

5. Harper R. (2016) Practical Foundation of Programming Languages. Second edition Carnegie Mellon University,

[https://www.google.com.ua/books/edition/Practical_Foundations_for_Programming_La/I2KcCwAAQBAI?hl=ru&gbpv=1&dq=Harper+R.+\(2016\)++Practical+Foundation+of+Programming+Languages.+Second+edition+Carnegie+Mellon+University.&printsec=frontcover](https://www.google.com.ua/books/edition/Practical_Foundations_for_Programming_La/I2KcCwAAQBAI?hl=ru&gbpv=1&dq=Harper+R.+(2016)++Practical+Foundation+of+Programming+Languages.+Second+edition+Carnegie+Mellon+University.&printsec=frontcover)

6. Ledin J. (2020) Modern Computer Architecture and Organization / J. Ledin. Packt Publishing,

[https://www.google.com.ua/books/edition/Modern_Computer_Architecture_and_Organiz/eCLhDwAAQBAI?hl=ru&gbpv=1&dq=Ledin+J.+\(2020\)+Modern+Computer+Architecture+and+Organization+/+J.+Ledin.+++Packt+Publishing.&printsec=frontcover](https://www.google.com.ua/books/edition/Modern_Computer_Architecture_and_Organiz/eCLhDwAAQBAI?hl=ru&gbpv=1&dq=Ledin+J.+(2020)+Modern+Computer+Architecture+and+Organization+/+J.+Ledin.+++Packt+Publishing.&printsec=frontcover)

7. Gregory P., Lassenius C., Wang, X. (2021) Agile Processes in Software Engineering and Extreme Programming. Kruchten. Springer,

[https://www.google.com.ua/books/edition/Agile_Processes_in_Software_Engineering/uLsyEAAAQBAI?hl=ru&gbpv=1&dq=Gregory+P.,+Lassenius+C.,+Wang,+X.+\(2021\)+Agile+Processes+in+Software+Engineering+and+Extreme+Programming.+Kruchten.+Springer.&printsec=frontcover](https://www.google.com.ua/books/edition/Agile_Processes_in_Software_Engineering/uLsyEAAAQBAI?hl=ru&gbpv=1&dq=Gregory+P.,+Lassenius+C.,+Wang,+X.+(2021)+Agile+Processes+in+Software+Engineering+and+Extreme+Programming.+Kruchten.+Springer.&printsec=frontcover)

8. Freeman E., Robson. E. (2020) Head First Design Patterns: Building Extensible and Maintainable Object-Oriented Software 2nd

[https://www.google.com.ua/books/edition/Head_First_Design_Patterns/GGpXN9SMELMC?hl=ru&gbpv=1&dq=Freeman+E.,+Robson.+E.+\(2020\)+Head+First+Design+Patterns:+Building+Extensible+and+Maintainable+Object-Oriented+Software+2nd&printsec=frontcover](https://www.google.com.ua/books/edition/Head_First_Design_Patterns/GGpXN9SMELMC?hl=ru&gbpv=1&dq=Freeman+E.,+Robson.+E.+(2020)+Head+First+Design+Patterns:+Building+Extensible+and+Maintainable+Object-Oriented+Software+2nd&printsec=frontcover)

Додаткова література :

9. The modern approach to building corporate information systems (ERP/CRM) /Retrieved from:

<https://www.purelogics.net/blog/the-modern-approach-to-building-corporate-information-systems-erpcrm/>

10. Microsoft Project - The Complete Guide for Project Managers Retrieved from:

<https://www.udemy.com/course/microsoft-project-the-complete-project-lifecycle/>

11. Microsoft Project Full Tutorial For Beginners Retrieved from:

https://www.youtube.com/watch?v=iUqbhkJWt_4

12. Основи тестування програмного забезпечення Retrieved

from:https://courses.prometheus.org.ua/courses/course-v1:LITS+115+2017_T4/about.

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;
- іспит: 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
Роман КОРОЛЬОВ