



## Силабус освітнього компонента

Програма навчальної дисципліни



# Архітектура корпоративних інформаційних систем

### Шифр та назва спеціальності

125 – Кібербезпека та захист інформації

### Інститут

ННІ Комп'ютерних наук та інформаційних технологій

### Освітня програма

Кібербезпека

### Кафедра

Кібербезпеки (328)

### Рівень освіти

Бакалавр

### Тип дисципліни

Профільна підготовка, Вибіркова

### Семестр

7

### Мова викладання

Українська, англійська

## Викладачі, розробники



### ПОГАСІЙ Сергій Сергійович

[Serhii.Pohasii@khpi.edu.ua](mailto:Serhii.Pohasii@khpi.edu.ua)

Кандидат економічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.

[Детальніше про викладача на сайті кафедри](#)

## Загальна інформація

### Анотація

Дисципліна «Архітектура корпоративних інформаційних систем» завершує цикл дисциплін по розробці, впровадженню та підтримці інформаційних систем рівня корпорацій. Студенти отримають розуміння архітектурних концепцій та інтеграції хмарних рішень, що допоможе їм стати компетентними фахівцями у сфері розробки та впровадження інформаційних систем для сучасного бізнесу.

Курс викладається практикуючим фахівцем, що зумовлює практичну спрямованість дисципліни та використання досвіду реальних проєктів IT-компанії Academy Smart.

## Мета та цілі дисципліни

Формування у студентів поглиблених знань з теорії та навичок практичної розробки архітектури програмного забезпечення для великих підприємств, корпорацій та інших бізнес-структур будь-якої галузі економіки та форми власності.

## Формат занять

Лекції, лабораторні роботи, самостійна робота. Підсумковий контроль — іспит.

## Компетентності

КЗ-2. Знання та розуміння предметної області та розуміння професії.

КЗ-5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

## Результати навчання

РН-1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

РН-2. організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН-3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН-4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН-5. Адаптуватися в умовах частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН-6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН-7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

РН-8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

РН-10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

РН-11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

РН-12. Розробляти моделі загроз та порушника.

РН-13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

РН-14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

- РН-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
- РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
- РН-17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
- РН-18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
- РН-19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
- РН-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
- РН-21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
- РН-23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
- РН-25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
- РН-26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
- РН-27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
- РН-29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
- РН-30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
- РН-31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
- РН-32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
- РН-33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
- РН-34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
- РН-35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних

та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки.

РН-36. Виявляти небезпечні сигнали технічних засобів.

РН-37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

РН-40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

РН-42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

РН-43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.

РН-44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

РН-45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

РН-46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

РН-48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

РН-49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

РН-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

РН-51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

РН-52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

РН-53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

РН-54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

## **Обсяг дисципліни**

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

## **Передумови вивчення дисципліни (пререквізити)**

Бази даних корпоративних інформаційних систем

## 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 проекти, майстер-класи.

## Програма навчальної дисципліни

### Теми лекційних занять

Тема 1. Основні поняття архітектури корпоративних інформаційних систем

Тема 2. Моделі надання програм споживачам

Тема 3. Роль форматів обміну даними у корпоративних інформаційних системах

Тема 4. Особливості клієнт-серверної архітектури в корпоративних інформаційних системах

Тема 5. Безпека передачі даних у корпоративних інформаційних системах

### Теми практичних занять

Практичні заняття в рамках дисципліни не передбачені.

### Теми лабораторних робіт

Тема 1. Розгортання мікросервісної архітектури в AWS

Тема 2. Використання Firebase у корпоративних інформаційних системах

Тема 3. Використання JSON для обміну даними між сервісами

### 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.

Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:

CCNA2

<https://www.netacad.com/catalogs/learn?category=course>

## Література та навчальні матеріали

### Основна література

1. Richards, M., Ford N. (2020). Fundamentals of Software Architecture: An Engineering Approach. O'Reilly Media, 432 p.

[https://books.google.com.ua/books?id=xa7MDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs\\_ge\\_summary\\_r&cad=0#v=onepage&q&f=false](https://books.google.com.ua/books?id=xa7MDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)

2. Newman, S. (2021). Building Microservices: Designing Fine-Grained Systems. 2nd ed. O'Reilly Media, 616 p.

<https://h.twirpx.link/file/3802294/>

3. Blokdyk, G. (2011). Client Server Complete Self-Assessment Guide. 5STARCook, 311 p.

[https://books.google.com.ua/books/about/Client\\_Server\\_Complete\\_Self\\_Assessment\\_G.html?id=dSJb0AEACAAJ&redir\\_esc=y](https://books.google.com.ua/books/about/Client_Server_Complete_Self_Assessment_G.html?id=dSJb0AEACAAJ&redir_esc=y)



4. Newman, S. (2019). Monolith to Microservices: Evolutionary Patterns to Transform Your Monolith. 1st ed. O'Reilly Media, 272 p.  
<https://www.google.com.ua/books/edition/Monolith+to+Microservices+Evolutionary+Patterns+to+Transform+Your+Monolith.1st+ed.+O%27Reilly+Media,+272+%D1%80.&printsec=frontcover>

### Додаткова література

5. Hohpe, G. (2020). The Software Architect Elevator: Redefining the Architect's Role in the Digital Enterprise. 1st ed. O'Reilly Media, 368 p.  
<https://www.google.com.ua/books/edition/The+Software+Architect+Elevator/X-bDwAAQBAJ?hl=ru&gbpv=1&dq=Hohpe,+G.+The+Software+Architect+Elevator:+Redefining+the+Architect%27s+Role+in+the+Digital+Enterprise&printsec=frontcover>  
 6. Introducing JSON. [Electronic resource]. – Access mode : <https://www.json.org/json-en.html>

## Система оцінювання

### Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 20% 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<br>(потрібне додаткове вивчення) | FX   |
| 1–34       | Незадовільно<br>(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

Сергій ЄВСЕЄВ