**Силабус освітнього компонента**
Програма навчальної дисципліни

# Безпека в DEVOPS

**Шифр та назва спеціальності**
F5 – Кібербезпека та захист інформації

**Інститут**
ННІ комп`ютерних наук та інформаційних технологій

**Спеціалізація**

**Кафедра**
Кібербезпеки (328)

**Освітня програма**
Кібербезпека

**Тип дисципліни**
Вибіркова

**Рівень освіти**
Перший (бакалаврський)

**Форма навчання**
Денна, заочна

**Семестр**
5

**Мова викладання**
Українська, англійська

## Викладачі, розробники

**ГАВРИЛОВА Алла Андріївна**
alla.havrylova@khpi.edu.ua
PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 50, з них патентів на корисну модель 2, 5 монографії, з яких 3 – 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», «Безпека в DevOps», «Організація та безпека баз даних», «Управління ІТ-проєктами та їх безпека» у студентів бакалавріату
Детальніше про викладача на сайті кафедри

## Загальна інформація

### Анотація

Навчальна дисципліна "Безпека в DEVOPS" навчає інтегрувати безпеку на всіх етапах життєвого циклу розробки програмного забезпечення, що забезпечує створення безпечних продуктів без уповільнення процесу.

### Мета та цілі дисципліни

Формування системи теоретичних знань і набуття практичних умінь і навичок щодо забезпечення безпеки на протязі життєвого циклу існування веб-рішень, що виконуються на боці серверу; оволодіння навичками застосування сучасного програмного забезпечення щодо рішень завдань

DevOps і набуття компетенцій з використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та кібербезпеки.

## Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

## Компетентності

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

## Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації.
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

### Обсяг дисципліни

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

### Передумови вивчення дисципліни (пререквізити)

Програмування, Розробка та аналіз алгоритмів, Фізичні основи технічних засобів розвідки, Інформаційна безпека держави, Математичні основи криптології, Основи побудови та захисту сучасних операційних систем, Введення в мережі, Технології програмування, Основи побудови та захисту мікропроцесорних систем, Менеджмент інформаційної безпеки, Основи математичного моделювання систем безпеки, Основи криптографічного захисту, Безпека в інформаційно-комунікаційних системах, Інформаційні системи та інтернет технології, Комплексні системи захисту інформації, Безпека інтернет-речей.

### Особливості дисципліни, методи та технології навчання

Лекції проводяться інтерактивно з використанням мультимедійних технологій. Застосовуються активні форми проведення занять: лекція, лекційне опитування, практичні заняття, співбесіда, консультація. На заняттях використовується компетентністний підхід до навчання, акцентується увага на застосуванні он-лайн курсу з розгляду сучасних питань у галузі кібербезпеки.

## Програма навчальної дисципліни

### Навчальні заняття

#### Лекції

| Теми лекцій | Кількість годин |
|---|---|
| **Тема 1.** Інтеграція безпеки в DevOps.<br>1. Безпека як частина життєвого циклу<br>**2. Безпека в CI/CD** | 4 |
| **Тема 2.** Автоматизація безпеки.<br>1. Автоматизація перевірок безпеки<br>2. Автоматизація сканування коду<br>3. Тестування на вразливості<br>**4. Управління політиками** | 4 |
| **Тема 3.** Управління безпекою.<br>1. Управління вразливостями<br>2. Безпека інфраструктури як коду<br>3. Безпека контейнерів<br>**4. Безпека хмарних середовищ** | 4 |
| **Тема 4.** Операційна безпека.<br>1. Моніторинг та логування<br>2. Управління доступом<br>3. Захист даних | 4 |
| **Загальна кількість годин** | **16** |

## Лабораторні заняття

| Теми лабораторних занять | Кількість годин | Вагові коефіцієнти *a* |
|---|---|---|
| **Тема 1.** Аналіз нормативно-правової бази.<br>1. Огляд та порівняльний аналіз ключових законодавчих актів України щодо захисту інформації.<br>2. Огляд та порівняльний аналіз та міжнародних стандартів щодо захисту інформації. | 2 | 1 |
| **Тема 2.** Інвентаризація та класифікація активів<br>1. Складання переліку інформаційних активів (сервери, дані, ПЗ) для вибраної організації.<br>2. Визначення власників активів та їхня класифікація за ступенем конфіденційності, цілісності та доступності. | 2 | 1 |
| **Тема 3.** Оцінка ризиків.<br>1. Проведення якісної або кількісної оцінки ризиків для 3-5 визначених інформаційних активів.<br>2. Ідентифікація загроз та вразливостей.<br>3. Розрахунок рівня ризику. | 4 | 1 |
| **Тема 4.** Розробка політики безпеки.<br>1. Складання проекту "Загальної політики інформаційної безпеки" організації.<br>2. Визначення її структури, цілей та сфер застосування. | 2 | 1 |
| **Тема 5.** Політика управління доступом.<br>1. Розробка політики управління доступом (фізичним та логічним).<br>2. Визначення правил Role-Based Access Control (RBAC) для типових посад (адміністратор, менеджер, рядовий співробітник). | 2 | 1 |
| **Тема 6.** Політика паролів та автентифікації.<br>1. Складання політики керування паролями (вимоги до складності, терміну дії, правил зміни)<br>2. Складання рекомендацій щодо використання багатофакторної аутентифікації (MFA). | 4 | 1 |
| **Тема 7.** Реагування на інформаційні інциденти.<br>1. Розробка процедури (Плану) реагування на типовий інцидент безпеки.<br>2. Визначення етапів: виявлення, локалізація, усунення, відновлення. | 4 | 1 |
| **Тема 8.** План безперервності бізнесу (BCP).<br>1. Складання плану забезпечення безперервності бізнесу<br>2. Складання плану відновлення після катастроф для критичної бізнес-функції.<br>3. Визначення RTO (Recovery Time Objective) та RPO (Recovery Point Objective). | 4 | 1 |
| **Тема 9.** Організація фізичного захисту<br>1. Розробка схеми фізичного захисту критичного об'єкта.<br>2. Обґрунтування вибору засобів контролю доступу (шлагбауми, СКУД, відеоспостереження). | 4 | 1 |
| **Тема 10.** Програма навчання персоналу<br>1. Розробка структури навчальної програми для співробітників з питань інформаційної безпеки.<br>2. Розробка змісту навчальної програми для співробітників з питань інформаційної безпеки. | 4 | 1 |

| | | |
|---|---|---|
| **Загальна кількість годин** | **32** | $\sum_{i=1}^{n} a_i = 10$ |

### Контрольні роботи

| Теми контрольних робіт | Вагові коефіцієнти $b$ |
|---|---|
| **Тема 1. Впровадження безпеки в CI/CD** | 2 |
| **Тема 2. Управління доступом та секретами** | 2 |
| **Тема 3. Автоматизоване тестування безпеки** | 2 |
| **Загалом** | $\sum_{i=1}^{m} b_i=6$ |

### Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

### Опрацювання теоретичного матеріал

| Теми для самостійного вивчення | Кількість годин |
|---|---|
| **Тема 1. Ключові концепції та принципи DevSecOps** | 24 |
| **Тема 2. Безпека на етапах CI/CD пайплайну** | 24 |
| **Тема 3. Безпека інфраструктури та операцій** | 24 |
| **Загальна кількість годин** | **72** |

## Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості..

### Рекомендовані курси, тренінги, стажування

## Література, навчальні матеріали та інформаційні ресурси

### Основна література

1. DevOps Revealed 3rd edition. International DevOps Certification Academy.- 94 p. [Electronic resource]. –Access mode https://www.devops-certification.org/.
2. Розробка безпечних хмарних додатків [Електронний ресурс] / Роби Сен. IBM developerWorks, 2016. – Режим доступу : http://www.ibm.com/ developerworks/ru/library/cl-develop-secure-cloud-aware-applications/index.html.
3. Хмарні стандарти: сумісність додатків у хмарі [Електронний ресурс] / Кэйн Скарлетт. IBM developerWorks, 2016. – Режим доступу : http://www.ibm.com/ developerworks/ ru/library /cl-tools-to-ensure-cloud-application-interoperability/index.html.
4. Create REST applications with the Slim micro-framework [Electronic resource] / Vikram Vaswani. IBM developerWorks, 2012. – Access mode : http://www.ibm.com/developerworks/library/x-slim-rest/.

5. Get started with Azure [Електронний ресурс]. – Режим доступу: https://azure.microsoft.com/en-us/get-started/#explore-azure.
6. Web Application Security [Electronic resource]. – Access mode: https://www.nginx.com/resources/library/web-application-security/?utm_medium=cpc&utm_source=google&utm_campaign=emea_ne-nx_sec&utm_content=eb-textad-kywd&_bt=499136631724&_bk=devsecops&_bm=p&_bn=g&_bg=123463179768&gclid=Cj0KCQiA3rKQBhCNARIsACUEW_a0bLksBM_gH0gLf8pP0gP2z-iwk46QLUjUMDkDtq3NLHBwvANtnZYaAiEYEALw_wcB#download.
7. Tutorials Library [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/index.htm.

### Додаткова література

1. Oracle Linux [Електронний ресурс]. – Режим доступу: https://www.oracle.com/linux/.
2. NIST Roadmap for Improving Critical Infrastructure Cybersecurity V [Електронний ресурс]. – Режим доступу: https://www.nist.gov/system/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf

## Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників $k$:

| Поточний контроль (практичні, семінарські, лабораторні заняття), $k_1$ | Контрольні роботи (за наявності), $k_2$ | Індивідуальне завдання (за наявності), $k_3$ | Підсумковий контроль (для ОК з іспитом), $k_4$ |
|---|---|---|---|
| 0,6 | 0,4 | | |

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
$K$ – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: $a_i$ - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: $b_i$ - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, $K$, І,... ) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої

### Шкала оцінювання

| Сума балів | Національна оцінка | ECTS |
|---|---|---|
| 90–100 | Відмінно | A |
| 82–89 | Добре | B |

освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

| | | |
|---|---|---|
| 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

Здобувач вищої освіти 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 | 30.08.2025 | | **Завідувач кафедри**<br>Сергій ЄВСЕЄВ |
| | 30.08.2025 | | **Гарант ОП**<br>Сергій ЄВСЕЄВ |