**Силабус освітнього компонента**
Програма навчальної дисципліни

# Інформаційна безпека держави

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
1

Мова викладання
Українська

## Викладачі, розробники

**КОРОЛЬ Ольга Григорівна**
olha.korol@khpi.edu.ua
кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з яких 14 навчальних посібників, 48 статтей у закордонних виданнях та фахових виданнях України, 8 патентів на корисну модель, 9 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави» , «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків»», у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

## Загальна інформація

### Анотація

Навчальна дисципліна "Інформаційна безпека держави" є нормативною навчальною дисципліною. Дисципліна спрямована на дослідження способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні та їх своєчасного виявлення, запобігання і нейтралізації.

### Мета та цілі дисципліни

Формування теоретичних основ законодавчої бази України та міжнародного суспільства в галузі національної та інформаційної безпеки держави, визначення основних вимог щодо формування підтримки та удосконалення систем управління інформаційної безпеки критичних інформаційно-комунікаційних систем, а також визначення місця і ролі інформаційної безпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави.

## Формат занять

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

## Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–5. Здатність спілкуватися іноземною мовою.
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-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
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.

## 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-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
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-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 інфораційною 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-мунікаційних 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. (6 кредитів ECTS): лекції – 32 год., лабораторні роботи – 48 год., самостійна робота – 100 год.

### Передумови вивчення дисципліни (пререквізити)

Вступ до спеціальності. Ознайомча практика.

### 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. Вступ.
Цілі та завдання навчальної дисципліни «Інформаційна безпека держави». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Поняття інформаційної безпеки держави та складових національних інтересів України в інформаційній сфері.
Тема 2. Основні положення інформаційної безпеки.
Основні складові інформаційної безпеки держави. Класифікація видів інформаційної безпеки держави. Види інформаційної безпеки. Загрози інформаційній безпеці України. Доктрина інформаційної безпеки України. Пріоритети державної політики в інформаційній сфері.
Тема 3. Загрози безпеці інформації.
Дестабілізуючі фактори інформаційної безпеки. Класифікація загроз інформаційній безпеці. Актуальні загрози національній безпеці України. Маніпулювання свідомістю, сутність та види маніпуляції. Роль та місце маніпулювання в національних системах державного управління та політичних системах, а також у формуванні та здійсненні міжнародних стосунків. Сутність та прояви інформаційного насильства. Проблемні питання правового запобігання здійсненню інформаційного насильства.
Тема 4. Основи інформаційного протиборства.
Основні поняття інформаційного протиборства. Концепція інформаційної війни. Основи, форми та принципи кібернетичної розвідки. Основи кібернетичного впливу.
Тема 5. Кібернетична зброя.
Класифікація кібернетичної зброї. Основні завдання, що покладаються на кібернетичну зброю. Об'єкт кібернетичного впливу та його складові елементи. Методи та засоби застосування кібернетичної зброї.
Тема 6. Психологічна війна та інформаційно-психологічна безпека держави.
Основні поняття, цілі та завдання психологічної війни. Види психологічного впливу. Форми психологічної війни. Особливі способи та прийоми психологічної війни. Основи інформаційно-психологічної безпеки держави. Принципи безпеки у психосфері. Сили та засоби інформаційно-психологічної безпеки.
Тема 7. Інтернет та інформаційна безпека.
Особливості встановлення та проблеми реалізації інформаційних правовідносин в мережі Інтернет. Сутність, витоки та механізми трансформаційних процесів забезпечення національної та міжнародної безпеки. Сутність, витоки та механізми глобалізації інформаційного простору. Життєво важливі інтереси людини та суспільства в інформаційній сфері. Національні інтереси в інформаційній сфері. Поняття та сутність інформаційного суверенітету. Сучасні та потенційні проблемні питання правового забезпечення інформаційного суверенітету та можливі шляхи їх вирішення. Проблемні питання правового реагування на трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення. Витоки та

сутність кіберсоціалізації. Соціальні мережі. Мережева мобілізація: питання демократії та безпеки. Наслідки кіберсоціалізації.
Сутність поняття «кіберцивілізація».
Потенційні загрози кіберцивілізації для людства.
Поняття кіберзлочинності.
Про кіберзлочинність: Конвенція Ради Європи від 23.11.01 р. № 994-575.
Сутність та визначення поняття «кібертероризм».
Відображення кібертероризму в законодавстві України.
Тема 8. Види персональних даних у державі. Принципи захисту персональних даних у державі.
Нормативні документи захисту даних.
Конфіденційність персональних даних.
Захист персональної інформації.
Європейська система захисту персональних даних.
Тема 9. Доктринальні, концептуальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.
Основні ознаки відмінностей індустріального та постіндустріального суспільств.
Тенденції розвитку постіндустріального суспільства.
Трансформація правовідносин у постіндустріальному суспільстві.
Реальні та потенційні загрози в інформаційній сфері у постіндустріальному суспільстві.
Характеристика основних положень: - Воєнної доктрини України; - Доктрини інформаційної безпеки України; - Концепції розвитку сектору безпеки і оборони України. - Стратегії національної безпеки України; - Стратегії кібербезпеки України Характеристика основних положень Закону України «Про основні засади забезпечення кібербезпеки України».
Тема 10. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки.
Адміністративна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. Кримінальна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. Цивільна відповідальність за правопорушення в системі забезпечення інформаційної безпеки.
Тема 11. Основні законодавчі положення у сфері забезпечення інформаційної безпеки, кібербезпеки.
Основні законодавчі положення у сфері: - забезпечення захисту інформації; - убезпечення від «шкідливої» інформації людину, суспільство, державу; захисту персональних даних.

### Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

### Теми лабораторних робіт

Тема 1. Порівняння даних за допомогою хешу.
Тема 2. Методи та шляхи збору та обробки інформації. Що було зроблено?.
Тема 3. Створення та збереження надійних паролей.
Тема 4. Резервне копіювання даних до зовнішнього сховища.
Тема 5. Інформаційне протиборство. Хто володіє Вашими даними?.
Тема 6. Аналітичне забезпечення інформаційної безпеки. Дослідіть ризики своєї поведінки в Інтернеті (командна робота).
Тема 7. Класифікація програмних та криптографічних засобів забезпечення інформаційної безпеки.
Тема 8. Електронна ідентифікація користувачів. Нормативне забезпечення інформаційної безпеки. Загрози безпеки.
Тема 9. Системна класифікація та характеристика технічних засобів забезпечення інформаційної безпеки.
Тема 10. Міжнародні стандарти та рекомендації в галузі забезпечення інформаційної безпеки.

### 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:
Cyber Ess
https://www.netacad.com/catalogs/learn?category=course.

## Література та навчальні матеріали

### Основна література

1. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
2. Богуш В. М., Юдін О. К. Інформаційна безпека держави. – К.: "МК-Прес", 2005. – 432с.
3. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
4. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0. https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf.
5. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%d0%86%d0%bd%d1%84%d0%be%d1%80%d0%bc.%20%d0%b1%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%d0%b0%20%d0%b4%d0%b5%d1%80%d0%b6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y.

### Додаткова література

6. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
7. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 6 травня 2015 року № 287/2015. Дата оновлення: 16.09.2020. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text
9. Про національну безпеку: Закон України від 21.06.2018 № 2469-VIII. Дата оновлення: 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
10. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: https://www.iso.org/ru/contents/data/standard/08/28/82875.html
11. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html
12. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html.

13. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
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. URL: 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;
•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