



Силабус освітнього компонента Програма навчальної дисципліни



Менеджмент інформаційної безпеки

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

2

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseyev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем», «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Менеджмент інформаційної безпеки" є нормативною навчальною дисципліною. Дисципліна спрямована на набуття студентом теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки.

Мета та цілі дисципліни

Формування у студентів теоретичних знань основних принципів менеджменту управління інцидентами та ризиками на основі вимог міжнародних регуляторів.

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-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-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
- 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-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-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
- 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 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Інформаційна безпека держави, Основи побудови та захисту сучасних операційних систем, Комп'ютерні мережі.

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. Поняття інформаційної безпеки держави і складових національних інтересів України в інформаційній сфері.

Базові терміни і поняття ІБ . Еволюція кіберзагроз. Критично важливі інфраструктури держав України та США. Кібероперація «Олімпійські ігри». Кібератака на рівненську АЕС. Кібератака carbanaki мільярд доларів. звіт CISCO з інформаційної безпеки за перше півріччя 2017. Аналіз способів розгортання шкідливого ПО . Історія інцидентів – 2008, спекуляції?. Історія інцидентів – 2012. Чи реальні ризики? Загрози сьогодні. Поточна ситуація у безпеки АСУТП . Вразливості: людський фактор . Проблеми кібербезпеки в інтернеті речей . Основні причини кіберпорушень . Актуальність інцидент-менеджменту . Базові поняття інцидент-менеджменту. Вимоги до управління інцидентами згідно стандарту ISO/IEC 27001. Модель процесу управління інцидентами згідно стандарту ISO/IEC 27035 . Ознаки інцидентів ІБ . Цілі управління інцидентами. Стандарти, рекомендації та кращі практики у сфері управління інцидентами .

Тема 2. Менеджмент інциденту інформаційної безпеки.

Короткий огляд проблеми управління ризиками. Інтеграція управління ризиком у життєвий цикл розвитку систем (system development life cycle, sdlc). Стандарт ISO/IEC 27001 . Життєвий цикл IT-систем. Методологія оцінки ризику. Характеристика систем. Ідентифікація загроз. Ідентифікація вразливостей. Аналіз контролю (керування). Визначення можливості (можливості). Аналіз впливу (впливу). Визначення ризику. Рекомендації з контролю (керування). Документальне оформлення результатів. Зменшення ризиків. Загальна наслідність дій у методології зменшення ризиків . Аналіз рентабельності і залишковий ризик . Ключові фактори успішного управління ризиками .

Тема 3. Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL.

Концепція побудови, структура та функціональні особливості ефективної системи менеджменту інцидентів ІБ. Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL.

Тема 4. Поняття групи реагування на інциденти ІБ (CERT / CSIRT): історія розвитку та можливі вигоди перед- прийняттям.

Узагальнена класифікація груп CERT / CSIRT: сфера діяльності, цілі та потенційні клієнти.

Поняття групи реагування на інциденти ІБ (CERT / CSIRT): історія розвитку та можливі вигоди перед- прийняттям.

Тема 5. Інструментарій для ефективного функціонування груп реагування на інциденти ІБ.

Документаційне забезпечення процесу управління інцидентами ІБ. Діяльність різних груп реагування на інциденти ІБ. Інструментарій для ефективного функціонування груп реагування на інциденти ІБ.

Тема 6. Документаційне забезпечення процесу управління інцидентами ІБ.

Приклади документів: приватна (корпоративна) політика менеджменту ІБ . Діяльність груп реагування на інциденти ІБ (США) . Навіщо SOC потрібен компаніям. Як впровадити SOC в організації . Зберіть команду експертів . Будьте в курсі нових загроз . Забезпечте інфраструктуру для підтримки SOC . Моделі SOC у нотації NIST CYBERSECURITY FRAMEWORK. Інструменти і якості даних . Виявлення . Абстрактні інструменти забезпечення безпеки мереж . Вартість хибних проботувань . Кількість даних . Зразковий перелік питань при програмно-технічній експертизі ІС після дії інцидентів . Зразкові переліки після ураження інцидентами ІБ.

Тема 7. Аналіз ризиків в області захисту інформації.

Еволюція загроз. Рекомендації CISCO .

Тема 8. Управління ризиками та міжнародні стандарти.

Міжнародний стандарт iso 31000. Етапи процесу управління ризиками. Український державний центр радіочастот. Рамкова програма з кібербезпеки. Основа рамкової програми. Основні функції рамкової програми. Рівні впровадження рамкової програми. Рамкова програма з кібербезпеки. Встановлення або вдосконалення програми кібербезпеки.

Тема 9. Технології аналізу ризиків.

Аудит інформаційної безпеки. Обстеження вичислювальної системи ІТС. Обстеження інформаційного середовища ІТС. Обстеження фізичного середовища ІТС. Обстеження середовища користувачів. Тестування на вразливості ІТС. Аудит інформаційної безпеки банку. Методи оцінки ризиків. Практичний ризик-менеджмент. Методика CRAMM. Методика RiskWatch. Методика Microsoft.

Тема 10. Політики інформаційної безпеки.

Структура політики. Політика ІБ (приклад). Ідентифікація та оцінка активів. Аналіз джерел проблем. Ролі та обов'язки щодо ІБ. Розподіл обов'язків. Контакти з повноважними органами. Контакти з групами фахівців з певної проблематики. Приклад роботи з безпеки в угодах із третіми особами. ІБ в управлінні проектами. Мобільне обладнання та віддалена робота. Віддалена робота. Безпека персоналу. Терміни та умови найму. Відповідальність керівництва. Поінформованість, освіта й навчання щодо ІБ. Припинення чи зміна умов найму. Управління активами. Володіння активами СМІБ.

Тема 11. Політика системи менеджменту інформаційної безпеки.

Система менеджменту інформаційної безпеки. Орієнтовна послідовність дій при розробці СМІБ. Обов'язкові документи СМІБ. Загальна політика інформаційної безпеки може включати наступну інформацію. Приклад структури (загальної і детальних) політик безпеки організації (для забезпечення мережевої безпеки). Приклад політики інформаційної безпеки. Приклади невдалих політик. Інші ознаки поганих документів. Фактори, що визначають ефективність політики безпеки. Content of standard 27001:2013. Контекст організації. Лідерство. Планування. Оцінка ризиків інформаційної безпеки. Обробка ризиків інформаційної безпеки. Заява (декларація) про можливість застосування засобів контролю (statement of applicability). Цільові показники в сфері інформаційної безпеки та планування їх досягнення. Забезпечення. Документована інформація. Що повинно бути задокументовано? Управління документованою інформацією. Функціонування. Оцінка результатів діяльності. Поліпшення.

Тема 12. Аудит безпеки і аналіз ризиків.

Взаємозв'язок понять. Якісна оцінка СМІБ. Зміст процесу управління інцидентами. Причини виникнення інцидентів. Специфічні питання управління інцидентами інформаційної безпеки розглядаються в наступних документах. Планування і підготовка. Група розслідування

інцидентів. Структура команди з розслідування інцидентів ІБ. Розробка нормативних документів з управління інцидентами. Принципи ефективної політики реагування на інциденти ІБ. Політика розслідування інцидентів інформаційної безпеки. Ресурси і інструментарій розслідування інцидентів інформаційної безпеки. Превентивні заходи. Виявлення та аналіз інцидентів інформаційної безпеки. Ознаки інциденту інформаційної безпеки. Аналіз інцидентів інформаційної безпеки. Документування інциденту інформаційної безпеки. Розсилка повідомлень про інцидент інформаційної безпеки. Протидія поширенню інциденту. Процедура ліквідації наслідків інциденту ІБ.

Тема 13. Захист та аналіз кінцевих пристроїв.

Захист від шкідливих програм. Захист від вторгнень нарівні хоста. Безпека додатків. Профілювання мережі і сервера. Загальна система оцінки вразливостей. Загальна система оцінки вразливостей (CVSS). Архітектури забезпечення відповідності. Безпечне управління пристроями. Системи управління інформаційною безпекою.

Тема 14. Моніторинг безпеки.

Моніторинг найпоширеніших протоколів. Технології забезпечення безпеки. Типи даних безпеки. Дані сеансу і транзакцій. Журнали кінцевих пристроїв. Мережеві журнали.

Тема 15. Аналіз даних вторгнень.

Джерела попереджень. Огляд оцінки попереджень. Загальна платформа даних. Дослідження мережевих даних. Підвищення ефективності роботи аналітиків з кібербезпеки. Обробка доказів та атрибуція атак.

Тема 16. Реагування на інциденти та їх опрацювання.

Моделі реагування на інциденти. Обробка інцидентів.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та систем.

Тема 2. Інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі.

Тема 3. Дослідження вразливостей систем та веб ресурсів за допомогою спеціалізованих сканерів вразливостей (Nessus, Vega).

Тема 4. Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega.

Тема 5. Пошук вразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego.

Тема 6. Збір технічної та чуттєвої інформації за допомогою ПЗ класу – сніфери.

Тема 7. Засіб дослідження вразливостей безпроводних мереж Wi-Fi – Aircrack-ng.

Тема 8. Правила Snort та правила міжмережевого екрану.

Тема 9. Вилучення виконуваного файлу з PCA.

Тема 10. Інтерпретація даних HTTP та DNS для ізоляції зловмисника.

Тема 11. Обробка інцидентів.

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 Threat Management

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

Література та навчальні матеріали

Основна література

1. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.
<http://ir.stu.cn.ua/bitstream/handle/123456789/19244/%d0%9c%d0%b5%d0%bd%d0%b5%d0%b4%d0%b6%d0%bc%d0%b5%d0%bd%d1%82%20%d1%96%d0%bd%d1%84%d0%be%d1%80%d0%bc.%20%d0%b1%d0%b5%d0%b7%d0%bf.%20New%20booklet%201.pdf?sequence=1&isAllowed=y>
2. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
<https://drive.google.com/drive/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>
3. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlov, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
<https://drive.google.com/drive/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>
4. 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.
<https://drive.google.com/drive/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>.

Додаткова література

5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems.
<https://www.iso.org/ru/standard/27001>
6. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України/ [Електронний ресурс].
<https://zakon.rada.gov.ua/laws/show/v0365500-11#Text>
7. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Електронний ресурс].
<http://lindex.net.ua/ua/shop/bibl/500/doc/11423>
8. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з управління безпекою інформаційних технологій. [Електронний ресурс].
<http://www.premier-hs.com.ua/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinih-tiekhnologhii> Дата звернення: Декабрь. 7.2017.
9. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 3. Методи управління захистом інформаційних технологій. [Електронний ресурс].
<http://lindex.net.ua/ua/shop/bibl/500/doc/11425>
10. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибір засобів захисту. [Електронний ресурс].
<http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005>
11. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережевою безпекою. [Електронний ресурс].
<http://lindex.net.ua/ua/shop/bibl/500/doc/11427>.

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