Силабус освітнього компонента
Програма навчальної дисципліни

Безпека в інформаційно-комунікаційних системах

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
Спеціальна (фахова), Обов'язкова

Семестр
5

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтелліджанс» , «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека в інформаційно-комунікаційних системах" є обов`язковою навчальною дисципліною. Дисципліна спрямована на придбання студентами навичок з нейтралізації типових мережевих загроз, використання протоколу SNMP для захисту мережі, захисту від шкідливого програмного забезпечення та захист електронної пошти та веб-трафіку.

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 – залік.

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

Передумови вивчення дисципліни (пререквізити)

Основи криптографічного захисту. Основи математичного моделювання систем безпеки.

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. Сучасні загрози мережевої безпеки.
Огляд мережевих топологій. Інструменти хакерів. Шкідливе програмне забезпечення. Типові мережеві атаки. Захист мережі. Області мережевої безпеки. Архітектура Cisco SecureX. Нейтралізація типових мережевих загроз.
Тема 2. Забезпечення безпеки мережевих пристроїв.
Захист граничного маршрутизатора. Налаштування безпечного адміністративного доступу. Конфігурація розширених функцій безпеки для віртуального входу в систему. Конфігурація протоколу SSH. Призначення адміністративних ролей. Налаштування рівнів привілеїв. Налаштування CLI на основі ролей. Захист управління і звітності. Використання протоколу SNMP для захисту мережі.
Тема 3. Автентифікація, авторизація та облік.
Огляд AAA. Характеристики AAA. Локальна автентифікація AAA. Усунення помилок автентифікації AAA. Комунікаційні протоколи серверного AAA. Конфігурація серверної автентифікації AAA за допомогою інтерфейсу командного рядка (CLI). Усунення помилок серверної автентифікації AAA. Конфігурація серверної авторизації AAA.
Тема 4. Впровадження технологій брандмауера.
Налаштування стандартного і розширеного ACL-списків IPv4 з використанням інтерфейсу командного рядка (CLI). Нейтралізація атак за допомогою ACL-списків. ACL-списки IPv6. Захист мереж за допомогою міжмережевих екранів. Типи міжмережевих екранів.
Тема 5. Впровадження системи запобігання вторгнень.
Характеристики систем IDS и IPS. Мережеві реалізації IPS. Cisco Switched Port Analyzer. Характеристики сигнатур IPS. Дії сигнатури IPS. Управління та моніторинг IPS. Глобальна

кореляція IPS. Конфігурація Cisco IOS IPS з допомогою інтерфейсу командного рядка (CLI). Зміна сигнатур Cisco IOS IPS.
Тема 6. Забезпечення безпеки локальної мережі (LAN).
Знайомство з безпекою кінцевих пристроїв. Захист від шкідливого ПЗ. Захист електронної пошти та веб-трафіку. Контроль мережевого доступу. Загрози безпеці рівня 2. Атаки на таблиці CAM. Нейтралізація атаки на таблицю CAM. Нейтралізація атак на VLAN. Нейтралізація DHCP-атак. Нейтралізація ARP-атак. Нейтралізація атак спуфинга адрес. Нейтралізація STP-атак.
Тема 7. Криптографічні системи.
Захищені комунікації. Криптографія. Криптоаналіз. Криптографічні геш. Забезпечення цілісності за допомогою алгоритмів MD5, SHA-1 і SHA-2. Автентифікація за допомогою алгоритму HMAC. Шифрування. Стандарт шифрування даних (DES), AES. Альтернативні алгоритми шифрування. Обмін ключами Діффі-Геллмана. Цифровий підпис.
Тема 8. Впровадження віртуальних приватних мереж (VPN).
Огляд мереж VPN. Технології VPN. Знайомство з протоколом IPsec. Протоколи IPsec. Internet Key Exchange. Конфігурація IPsec VPN між двома пунктами (Site-to-Site). Політика ISAKMP. IPsec VPN.
Тема 9. Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA).
Рішення ASA. Базова конфігурація ASA. Конфігурація брандмауера ASA. Налаштування сервісів і параметрів управління. Групи об'єктів. ACLS. Сервісні політики в ASA.
Тема 10. Багатофункціональний пристрій безпеки Cisco ASA з розширеним функціоналом.
Меню майстрів ASDM. Налаштування сервісів і параметрів управління. Конфігурація розширених функцій ASDM. VPN між двома пунктами (Site-to-Site). VPN віддаленого доступу (Remote-Access). Конфігурація SSL VPN без використання клієнта. Конфігурація SSL VPN з використанням клієнта AnyConnect.
Тема 11. Управління безпечної мережею.
Техніки тестування безпеки мережі. Інструменти тестування безпеки мережі. Огляд політики безпеки. Структура політики безпеки. Стандарти, інструкції та процедури. Ролі та обов'язки. Обізнаність у питаннях безпеки і навчання. Реагування на компрометацію системи безпеки.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. (Cisco). Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак.
Тема 2. (Cisco). Захист маршрутизатора для адміністративного доступу.
Тема 3. (Cisco). Захист адміністративного доступу за допомогою AAA і RADIUS.
Тема 4. (Cisco). Налаштування розширених списків контролю доступу (ACL).
Тема 5. (Cisco). Налаштування зональних міжмережевих екранів.
Тема 6. (Cisco). Налаштування системи запобігання вторгнень (IPS).
Тема 7. (Cisco). Захист комутаторів 2-го рівня.
Тема 8. (Cisco). Вивчення методів ширування.
Тема 9. (Cisco). Налаштування мережі Site-to-Site VPN за допомогою Cisco IOS.

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:
Endpoint Security
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література:

1. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf.
2. 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
3. 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
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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література :

5. Безпека інформаційно-коммунікаційних систем. К. : Видавнича група BHV, 2009. – 608 с.
https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf
6. Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security - ESORICS 2016, Part I.
https://f.eruditor.link/file/2593296/

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;
• залік: 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