Силабус освітнього компонента
Програма навчальної дисципліни

Організаційне забезпечення захисту інформації

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
Профільна підготовка, Вибіркова

Семестр
7

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

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

Кількість наукових публікацій: понад 30, з них патентів на корисну модель 2, 3 монографії, з яких 1 – 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» у студентів бакалавріата
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Організаційне забезпечення захисту інформації" є вибірковою навчальною дисципліною. Дисципліна призначена для набуття теоретичних знань з захисту інформації та практичних навичок з організації забезпечення захисту інформації. Студенти вивчають основні напрямки, принципи та умови організаційного захисту; основні підходи, вимоги, методи та засоби.

Мета та цілі дисципліни

Формування теоретичних знань щодо проведення аналізу і оцінки загроз інформаційній безпеці об'єкта, оцінки збитків внаслідок протиправного розкриття інформації обмеженого доступу, організації і забезпечення режиму таємності, підбору, розстановки і роботи з кадрами.

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)

Антивірусний захист інформації , Інформаційно-комунікаційні системи у сфері національної безпеки, знання механізмів роботи з MS Word, MS Excel.

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. Завдання організаційного забезпечення захисту інформації.
Роль організаційних заходів в створенні надійного механізму захисту інформації. Завдання, які вирішуються на організаційному рівні для забезпечення безпеки функціонування інформації.
Тема 2. Аналіз і оцінка загроз інформаційної безпеки об'єкта.

Класифікація загроз щодо інформаційної безпеки за базовими ознаками. Три основних види загроз.
Тема 3. Оцінка збитків внаслідок протиправного розкриття інформації обмеженого доступу і заходи щодо його локалізації.
Перелік інформації з обмеженим доступом: державна, комерційна, банківська, професійна, службова таємниці, персональні дані і інтелектуальна власність. Огляд способів несанкціонованого доступу. Умови, що сприяють неправомірному оволодінню конфіденційною інформацією. Показник критерію ступеня відсутності або наявності завданої об’єкту матеріальної та моральної шкоди. Параметри вартості ризику від настання події.
Тема 4. Служба безпеки об'єкта.
Основні завдання служби безпеки. Принципи системи безпеки підприємства. Функції служби захисту інформації підприємства. Перелік підрозділів служби безпеки об'єкта обробки інформації або підприємства і їх функції.
Тема 5. Підбір, розстановка і робота з кадрами.
Етапи процедури відбору персоналу. Перевірка персоналу на благонадійність. Процес перевірки керівних кадрів. Укладання контрактів та угод про секретності. Особливості звільнення співробітників, які володіють конфіденційною інформацією. Підбір, розстановка і робота з кадрами служби безпеки. Дотримання трудової дисципліни і законності, зміцнення фізичного розвитку, здоров'я, підвищення культури. Соціальний захист персоналу служби безпеки.
Тема 6. Організація і забезпечення режиму таємності.
Особливості режиму секретності. Порядок організації режиму секретності. Закриті роботи режиму секретності. Документи, регламентуючі роботу підрозділів із захисту державної таємниці. Права працівників підрозділів із захисту державної таємниці. Основні завдання постійно діючих технічних комісій. Структура і зміст переліку відомостей, що становлять конфіденційну інформацію підприємства. Порядок допуску співробітників до відомостей, що становлять комерційну таємницю. Життєвий цикл документів, які містять комерційну таємницю.
Тема 7. Організація пропускного, внутрішньооб'єктового і протипожежного режиму.
Заходи, які регламентує пропускний режим. Встановлення відповідальності за забезпечення пропускного режиму і збереження матеріальних цінностей у структурних підрозділах. Документація з пропускного режиму. Заходи внутрішньооб'єктового режиму. Забезпечення протипожежного режиму.
Тема 8. Захист інформації при аваріях та інших екстремальних ситуаціях.
Особливості інформаційного впливу в екстремальних умовах. Превентивні заходи. Питання, які вирішуються і документуються при складанні попереджувального плану дій. Перелік відомостей плану дій.
Тема 9. Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва.
Канали поширення конфіденційної інформації.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Шаблони документів.
Тема 2. Створення конструкційної сітки документа складної структури.
Тема 3. Використання колонтитулів під час створення бланків документів.
Тема 4. Використання стилів у електронних документах.
Тема 5. Основи створення документів з обчислюваними реквізитами.
Тема 6. Автоматизація створення та розсилання однотипних документів.
Тема 7. Створення переліків відомостей інформації з обмеженим доступом.
Тема 8. Складання та оформлення організаційно-розпорядчих документів.
Тема 9. Ведення документів, що містять інформацію з грифом. Формування справ.
Тема 10. Відбирання та передавання документів на знищення.

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.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. Поточна редакція від 27.07.2023.
URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Про науково-технічну інформацію: Закони України від 25 червня 1993 року № 3322-XII . Поточна редакція від 19.04.2014.
URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text
3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Поточна редакція від 01.01.2024.
URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII // ВВР України. Поточна редакція від 01.01.2024.
URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.
5. Про захист персональних даних: Закон України від 09.02.2010 №2297–VI // ВВР України. Поточна редакція від 27.10.2022.
URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
6. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226с. URL:
https://moodle.znu.edu.ua/pluginfile.php/1142772/mod_resource/content/1/Zahyst_informacii_ASU.PDF
7. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518. Поточна редакція від 07.09.2022.
URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
8. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.
URL: https://pdf.lib.vntu.edu.ua/books/IRVC/Yaremchuk_2018_118.pdf
9. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.
URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/6dbd7fae-06f3-4afd-b2f7-871688668ea0/content
10. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf

Додаткова література

1. Бурячок В.Л., Толюпа С.В., Семко В.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ. ДУТ-КНУ, 2016. 178 с.

https://duikt.edu.ua/uploads/p_303_92597962.pdf
2. Яремчук Ю. Є. Дослідження комбінаційних характеристик вітчизняних радіо непрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. №3 – С. 56-65.
http://nbuv.gov.ua/UJRN/rzod_2015_17_3_8
3. Яремчук Ю. Є. Дослідження характеристик вітчизняних радіо непрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю. Є. Яремчук, В. С. Катаєв, М. Ю. Гижко, П. В. Павловський // Реєстрація, зберігання та обробка даних. – 2016. – Том 18, № 1. – С. 42-51.
https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34773/93691.pdf?sequence=2&isAllowed=y.

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