МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ «УМАНСЬКИЙ ФАХОВИЙ КОЛЕДЖ ТЕХНОЛОГІЙ ТА БІЗНЕСУ УМАНСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ САДІВНИЦТВА»

Циклова комісія комп'ютерних дисциплін

ЗАТВЕРДЖУЮ"
Заступник директора
з навчальної роботи
Н. П. Николюк
„01" 09 2023 року

НАВЧАЛЬНА ПРОГРАМА

Технологія захисту інформації

Галузь знань	0501 "Інформатика та обчислювальна техніка"
Спеціальність	122 "Комп'ютерні науки"
Освітньо – професійна програма	"Комп'ютерні науки"
Освітньо-кваліфікаційний рівень	Фаховий молодший бакалавр

2023

Розробник: Вічкань О.М., викладач комп'ютерних дисциплін, спеціаліст вищої кваліфікаційної категорії

Програма затверджена на засіданні циклової комісії комп'ютерних дисциплін.

Протокол № 1 від "01" вересня 2023 року

Голова циклової комісії комп'ютерних дисциплін

_____ Н.О. Цяпута

Вступ

Навчальна програма «Технологія захисту інформації» для студентів за напрямом підготовки «122 "Комп'ютерні науки», спеціальністю «Комп'ютерні науки» є невід'ємною частиною циклу професійно-орієнтованої підготовки.

Розглянуто основи сучасного захисту інформації в комп'ютерних системах, не пов'язаних із державною таємницею. Викладено основні поняття та визначення захисту інформації, формування політики безпеки, критерії оцінки захищеності комп'ютерних систем, основи криптографічного захисту інформації, захисту інформації від несанкціонованого доступу в сучасних операційних системах, а також описано комплексні системи захисту в корпоративних інформаційних системах..

1. Мета, завдання навчальної дисципліни, компетентності та очікувані результати навчання

1.1 Предметом навчальної дисципліни: є методи організації технічного та технологічного захисту інформації.

1.2 Метою викладання дисципліни є надання студентам системних знань з принципів побудови систем криптографічного захисту інформації, освоєння ними необхідних знань та отримання навиків з організації та забезпечення захисту інформації в інформаційно-телекомунікаційних системах.

1.2 Основними завданнями вивчення дисципліни є: освоєння принципів побудови ТЗІ в комп'ютерних системах, а також формування умінь використовувати на практиці набуті знання для аналізу захищеності сучасного обладнання та програмного забезпечення, проектування та експлуатації ефективної системи захисту інформації від несанкціонованого доступу. Формування професійних навиків у студентів

В ході вивчення дисципліни у студента повинні формуватися наступні компетентності.

Інтегральна компетентність.

Здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій або у процесі навчання, що вимагає застосування положень і методів комп'ютерних наук та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях.

Загальні компетентності:

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК4. Здатність застосовувати знання у практичних ситуаціях.

ЗК6. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК7. Здатність спілкуватися іноземною мовою.

ЗК8. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні компетентності:

СК1. Здатність використовувати основні поняття, ідеї та методи фундаментальних наук під час розв'язання складних спеціалізованих задач з комп'ютерних наук в галузі інформаційних технологій.

СК2. Здатність використовувати теоретичні та фундаментальні знання в галузі комп'ютерних наук та інформаційних технологій для вирішення різноманітних проблем.

СК3. Здатність розробляти, аналізувати та застосовувати ефективні алгоритми для розв'язання конкретних професійних задач залежно від предметного середовища.

СК5. Здатність застосовувати принципи і методи побудови та використання мережевих технологій.

СК6. Здатність застосовувати методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу в умовах супроводження та експлуатації програмних систем і комплексів.

Результати навчання:

РН2. Вільно спілкуватися усно і письмово державною та іноземною мовами, у тому числі з професійних питань.

РН3. Використовувати професійно-профільовані знання і практичні навички методів фундаментальної та прикладної математики під час розв'язання стандартних задач і задач прикладного характеру в галузі комп'ютерних наук.

РН13. Здійснювати моніторинг роботи програмних систем і комплексів.

РН14. Організовувати конфігураційне та програмне налагодження інформаційних систем у процесі їх супроводження та експлуатації.

2. Інформаційний обсяг навчальної дисципліни

Розділ 1. Захист інформації. Традиційні криптографічні системи.

Організація, структура, цілісність. Інформаційна безпека, захист інформації, інформація, що обробляється в АС, права власників цієї інформації та власників АС, права користувача. Конфіденційність, цілісність та доступність. Неспростовність, автентичність, достовірність, адекватність.

Правові аспекти захисту інформації: законодавчо-правовий, адміністративний (організаційний), програмно-технічний.

Криптографія, криптосистема, криптографічне перетворення, шифрування, розшифрування, крипто аналіз, простий шифр маршрутної перестановки, простий перестановочний шифр, шифр зсуву, шифр заміни, поліалфавітний шифри заміни, модифікований шифр Цезаря, шифр Віженера. Криптографічна стійкість шифрів

Розділ 2. Блокові шифри як основа сучасних криптосистем

Блокові алгоритми і режими шифрування, режим електронної кодової книги (ECB), Режим зціплення блоків по криптотексту (CBC). Режим з оберненим зв'язком по криптотексту (CFB). Режим з оберненим зв'язком по виходу (OFB). Режим з лічильником (CTR). SP-мережа. Мережі Фейстеля. Криптосистема DES, загальна характеристика. Алгоритм шифрування. Структура функції F. Стійкість DES. Похідні від DES шифри. DES і шифрована файлова система EFS.

Сучасні симетричні криптосистеми. ДСТУ ГОСТ 28147:2009. AES (Advanced Encryption Standard). Програмна реалізація криптографічних алгоритмів засобами NET. Модель асиметричної системи. Модель криптосистеми з публічними ключами.

3. Список рекомендованої літератури

Основна

1. Основна література 1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2015. – 104 с.

2. Методи та засоби інженерно-технічного захисту інформації навч. посіб. / В.В. Богданов, О.В.Волков, О.В.Жук, В.В.Мартинюк – К.: ВІТІ НТУУ «КПІ», 2013.

3. Захист інформації обмеженого доступу: навч. посіб. / Г.А. Бузов – М.: Гаряча лінія - Телеком, 2014.

4. «Про захист інформації в інформаційно-телекомунікаційних системах» Закон України від 05.07.1994 № 80/94-ВР (В редакції Закону від 31.05.2005 № 2594-IУ).

5. Конституція України: редакція від 01.01.2020 р./ Відомості Верховної Ради України, № 254к/96-ВР, ст.141

6. «Про основи національної безпеки України» Закон України від 19.06.2003р.. № 964-IV, ВВР, 2003, №39, ст.351 (редакція станом на 08.07.2018),.

7. «Про інформацію» Закон України від 02.10.1992 р., №2657-XII, ВВР, 1992, №48, ст.650 (редакція станом на 16.07.2020).

8. «Про державну таємницю» Закон України від 21.01.1994 р., № 3855-XII, ВВР, 1994, № 16, ст.93 (редакція станом на 24.10.2020).

9. «Про власність» Закон України в редакції від 20.06.2007 р. № 697-XII, ВВР, 2007, №33, ст. 440.

10. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. [Чинний від 1997-01-01]. Київ, Держстандарт України, 1997, ст. 20.

11. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. [Чинний від 1997-07-01]. Київ Держстандарт, 1997, ст. 6.

12. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. [Чинний від 1998-01-01]. Київ, Держстандарт України, 1997, ст. 12.

13. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. [чинний від 1997- 01-01, в редакції від 2005-08-23]. Київ. Держстандарт. 2005, ст. 13.

14. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. [Чинний від 1997-01-01]. Київ, Держстандарт України, 1997, ст. 20.

15. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. [Чинний від 1997-07-01]. Київ Держстандарт, 1997, ст. 6.

16. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. [Чинний від 1998-01-01]. Київ, Держстандарт України, 1997, ст. 12.

17. Захист інформації обмеженого доступу: навч. посіб. / Г.А. Бузов – М.: Гаряча лінія - Телеком, 2014.

18. Звід відомостей, що становлять державну таємницю (затверджено наказом служби безпеки України від 12.08.2005 № 440, із змінами).

Додаткова

1.ДСТУ 4163-03 Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів. [Чинний від 2003-09-01]. Київ, Держстандарт, 2003, ст. 40.

2. Постанова Кабінету Міністрів України від 18 грудня 2013 № 939 «Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, підприємствах, в установах і організаціях».

Ресурси мережі Інтернет

1. hhttps://zakon.rada.gov.ua/laws/show/z0362-14#Text
2. https://zakon.help/article/nacionalnii-standart-dstu-41632020-derzhavna?menu=82

4.Форма підсумкового контролю успішності навчання

Контроль знань і умінь студентів з дисципліни здійснюється відповідно до системи організації освітнього процесу. Формою підсумкового контролю є іспит.

5. Засоби діагностики успішності навчання

Для підсумкової діагностики успішності навчання використовується усний, письмовий, тестовий та програмований контроль, практична перевірка, а також методи самоконтролю і самооцінки.