ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «ВИШИЙ НАВЧАЛЬНИЙ ЗАКЛАД «МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»

МАУП

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

ЩОДО ЗАБЕЗПЕЧЕННЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

З ДИСЦИПЛІНИ

“ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПАТЕНТОЗНАВСТВО”

(для бакалаврів)

Київ 2018

Підготовлено доцентом кафедри комп'ютерних інформаційних систем та технологій О.Г. Чолишкіна.
Затверджено на засіданні кафедри комп'ютерних інформаційних систем та технологій (Протокол № 1 від 23 серпня 2018 р.)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Чолишкіна О.Г. Методичні рекомендації щодо забезпечення самостійної роботи студентів з дисципліни "Технології захисту інформації та патентознавство" (для освітньо-кваліфікаційного рівня «бакалавр»). — К.: МАУП, 2018—21 с.

Методичні рекомендації містять пояснювальну записку**,** тематичний план, зміст дисципліни, теми лабораторних робіт , тематику контрольних робіт, вказівки до виконання контрольних робіт, питання для самоконтролю, список літератури.

© ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», 2018

ПОЯСНЮВАЛЬНА ЗАПИСКА

У сучасних умовах інформація, яка забезпечує життєво й історично важливі напрями діяльності людини, перетворюється в цінний продукт і основний товар, вартість якого поступово наближається до вартості продуктів матеріального виробництва, що робить її (інформацію) об'єктом інтересів різного характеру (комерційного, соціального, кримінального та ін.). Одним словом, виникнення індустрії обробки інформації привело до необхідності розвитку індустрії засобів захисту інформації.

Об'єктами посягань можуть бути технічні засоби (комп'ютери і периферія) як матеріальні об'єкти, програмне забезпечення і бази даних, для яких технічні засоби є оточенням. У цьому сенсі комп'ютер може бути як предметом посягань, так й інструментом. Можливе об'єднання зазначених понять, коли комп'ютер одночасно і інструмент, і предмет. Зокрема, до цієї ситуації належить факт розкрадання машинної інформації, видалення її, порушення нормального процесу функціонування ЕОМ і мереж. Якщо це пов'язане із втратою матеріальних і фінансових цінностей, то цей факт можна кваліфікувати як злочин. Також якщо із цим фактом пов'язуються порушення інтересів національної безпеки, авторства, то кримінальна відповідальність прямо передбачена відповідно до законів України.

Особливу тривогу викликає те, що організовані злочинні формування активно використовують здобутки інформатики для досягнення злочинних цілей. Аналіз наявної емпіричної бази світового досвіду показує, що спостерігається тенденція, коли транснаціональна організована комп'ютерна злочинність становить загрозу не тільки національній безпеці окремої країни, а й загрожує всьому світовому порядку. Це стосується сфери економічної безпеки. Світовий "кіберпростір" у галузі економічних відносин активно освоюється криміналітетом. За експертними оцінками, обсяги операцій при електронній обробці та передаванні через комп'ютерні мережі грошових ресурсів вказують на те, що потенційні втрати можуть бути вищі, ніж при тих самих операціях з використанням звичайних

паперових технологій. Втрати ж окремо взятої держави в таких випадках за лічені хвилини можуть досягати значних розмірів.

У результаті вивчення навчальної дисципліни “Технології захисту інформації та патентознавство” студенти повинні:

- знати про джерела і способи дії загроз на об’єкти інформаційної безпеки установ; про правові і нормативні акти, які визначають систему захисту інформації в державі; про керівні документи, що визначають рівень захищеності комп’ютерних систем; про методи проведення аналізу надійності системи захисту інформації в комп’ютерних системах; про основні методи, технологію, принципи і правила побудови захисту електронних обчислювальних машин, у тому числі персональних комп’ютерів, їх елементів і об’єктів комп’ютерних мереж;
- мати достатньо повне уявлення про алгоритми створення сучасних програм; про алгоритми кодування та застосування стандартного програмного забезпечення захисту; про методи та технологію захисту операційних систем, текстових редакторів, табличних процесорів, системи управління базами даних в локальних, корпоративних та глобальних комп’ютерних мережах банків та інших фінансових установ; на основі вивчених алгоритмів вміти розробляти нові програмні складові захисту в майбутньому;
- набути практичних навичок роботи з концептуальними моделями розробки, розподілу, обробки, використання та зберігання конфіденціальних документів; з системами й методами визначення захищеності носіїв інформації; створення засобами стандартного програмного забезпечення елементів захисту інформації; формулювання завдань з питань захисту інформації та визначення шляхів їх вирішення.

ІНДИВІДУАЛЬНО-КОНСУЛЬТАЦІЙНА РОБОТА

Індивідуально-консультативна робота з дисципліни «Технології захисту інформації та патентознавство» організовуються та здійснюється у формі консультацій на кафедрі комп'ютерних інформаційних систем і технологій у відповідності до затвердженого графіку консультацій (одна консультація на два тижні).

На консультаціях студентам надаються пояснення з виконання самостійної роботи, підготовки до практичних занять, перевірка та захист завдань, винесених на поточний контроль тощо.

ТЕМАТИЧНИЙ ПЛАН ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПАТЕНТОЗНАВСТВО»

№/п.п.	Назва змістового модуля та теми
Змістовий модуль 1. **Менеджмент інформаційної безпеки**	
Тема 1	Категорії інформаційної безпеки з точки зору інформації та інформаційних систем
Тема 2	Абстрактні моделі захисту інформації. Огляд найпоширеніших методів “злому”
Тема 3	Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації
Тема 4	Класифікація криптоалгоритмів
Тема 5	Системи шифрування даних, які передаються в мережах
Тема 6	Засоби управління криптографічними ключами
Змістовий модуль 2. **Основи кодування інформації в каналах зв’язку**	
Тема 7	Сучасна ситуація у сфері інформаційної безпеки. Рівні мережних атак
Тема 8	Апаратні та програмні засоби захисту інформації в мережах
Тема 9	Термінали захищеної інформаційної системи. Отримання пароля на основі помилок
	Разом годин : 90

ЗМІСТ ДИСЦИПЛІНИ

Змістовий модуль І. Менеджмент інформаційної безпеки

Тема 1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем

Етапи розвитку систем захисту. Основні загрози інформаційній безпеці. Категорії безпеки інформації та інформаційних систем. “Помаранчева книга” США.

Література [1; 3–5; 8; 10; 36; 40; 41]

Тема 2. Абстрактні моделі захисту інформації.

Огляд найпоширеніших методів “злому”. Абстрактні моделі захисту інформації. Побудова моделі захисту системи, визначення затрат часу, ресурсів та засобів.

Огляд найпоширеніших методів “злому”. Комплексний пошук можливих методів доступу.

Термінали захищеної інформаційної системи.

Література [1; 3–5; 8; 10; 36; 40; 41]

Тема 3. Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації

Класи безпеки інформації та інформаційних систем. Класифікація систем за критеріями інформаційної безпеки. Вимоги до роботи з конфіденційною інформацією. Створення політики інформаційної безпеки.

Електромагнітні та електричні канали витоку інформації. Параметричні канали витоку інформації.

Література [1; 3–5; 8; 10; 22; 25–27; 35; 36; 40–42]

Тема 4. Класифікація криптоалгоритмів

Тайнопис, криптографія з ключем. Симетричні та асиметричні криптоалгоритми.

Література [4; 5; 11; 14; 15; 30; 34]

Тема 5. Системи шифрування даних, які передаються в мережах

Канальне шифрування. Абонементне шифрування.

Література [4; 5; 11; 14; 15; 30; 34]

Тема 6. Засоби управління криптографічними ключами

Генерація ключів. Зберігання і розподілення ключів.

Література [4; 5; 11; 14; 15; 30; 34]

Змістовий модуль ІІ. Менеджмент безпеки інформаційних систем

Тема 7. Сучасна ситуація у сфері інформаційної безпеки. Рівні мережних атак

Рівні мережних атак згідно із моделлю OSI. Захист систем передавання інформації.

Література [1–8; 12; 13; 16–23; 25–27; 29; 33; 37–42]

Тема 8. Апаратні та програмні засоби захисту інформації в мережах

Системи ідентифікації й аутентифікації користувача (традиційні та біометричні параметри).

Система FireWall-1/VPN-1. Система OmniGuard/Enterprise Security Manager компанії Axent. Брандмауери. Мережний екран PIX Firewall.

Апаратно-програмний комплекс захисту інформації “ШИП”, “Dallas Lock”. Криптографічний адаптер. Процесор безпеки мережі. Локатори ліній зв’язку.

Сканер NetRecon. Аналізатор телефонних ліній SP-18/T “Багер-01”.

Детектор електромагнітного поля Д-006.

Література [1–8; 12; 13; 16–23; 25–27; 29; 33; 37–42]

Тема 9. Термінали захищеної інформаційної системи. Отримання пароля на основі помилок

Термінали захищеної інформаційної системи. Отримання пароля на основі помилок адміністратора та користувача. Отримання пароля на основі помилок у реалізації. Соціальна психологія й інші способи отримання пароля.

Література [1–8; 12; 13; 16–23; 25–27; 29; 33; 37–42]

ТЕМАТИКА ЛАБОРАТОРНИХ ЗАНЯТЬ

Лабораторне заняття – це організаційна форма навчального заняття, на якому студенти під керівництвом викладача формують уміння й навички з практичного застосування основних теоретичних положень навчальної дисципліни шляхом виконання завдань до лабораторних робіт. Лабораторні заняття з дисципліни «Технології захисту інформації та патентознавство» проводяться в спеціально обладнаній навчальній аудиторії з використанням комп'ютерного устаткування пристосованого до начального процесу.

За результатами виконаної на занятті лабораторної роботи студенти оформлюють індивідуальні звіти з її виконання та захищають ці звіти перед викладачем. Результати виконання лабораторних досліджень оцінюються викладачем.

Тематика проведення лабораторних занять наведена у таблиці нижче:

№	Назва теми
1	Побудова моделі захисту системи, визначення затрат часу, ресурсів та засобів.
2	Класифікація систем за критеріями інформаційної безпеки.
3	Тайнопис, криптографія з ключем.
4	Симетричні та асиметричні криптоалгоритми
5	Канальне шифрування. Абонементне шифрування.
6	Генерація ключів. Зберігання і розподілення ключів.
7	Захист систем передавання інформації.
8	Системи ідентифікації й аутентифікації користувача.
9	Отримання пароля на основі помилок адміністратора та користувача. Отримання пароля на основі помилок у реалізації.

ТЕМАТИКА КОНТРОЛЬНИХ РОБІТ.

1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем.
2. Класифікація криптоалгоритмів.
3. Технічні, програмно-апаратні та адміністративні засоби захисту інформації
4. Установлення та зміна паролів, контроль доступу в систему, права користувачів
5. Системи аутентифікації електронних даних (імітовставка, електронний підпис).
6. Сучасна ситуація у сфері інформаційної безпеки
7. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access.conf
8. Ідентифікація й аутентифікація. Механізми підзвітності та аудиту.
9. Система пошуку та захисту від вторгнення LIDS
10. Критерії інформаційної безпеки
11. Класифікація інформації за рівнем конфіденційності
12. Термінали захищеної інформаційної системи
13. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування)

ВАРІАНТИ КОНТРОЛЬНИХ РОБІТ

Варіант 1

1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем.
2. Класифікація криптоалгоритмів.
3. Стратегія захисту інформації у фінансово-економічних інформаційних системах.

Варіант 2

1. Технічні, програмно-апаратні та адміністративні засоби захисту інформації.
2. Комплекс технічних і програмних засобів захисту інформації.
3. Установлення та зміна паролів, контроль доступу в систему, права користувачів.

Варіант 3

1. Визначення об’єкта захисту та можливих загроз.
2. Системи аутентифікації електронних даних (імітовставка, електронний підпис).
3. Служби, які можуть захищати від кібероблав.

Варіант 4

1. Принцип розімкнутого управління, компенсації, зворотного зв’язку.
2. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
3. Додавання користувача та встановлення його прав.

Варіант 5

1. Сучасна ситуація у сфері інформаційної безпеки.
2. Відповідальність за протиправні дії згідно із законодавством України.
3. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access.conf.

Варіант 6

1. Ідентифікація й аутентифікація. Механізми підзвітності та аудиту.
2. Типи атак.
3. Система пошуку та захисту від вторгнення LIDS.

Варіант 7

1. Класи безпеки.
2. Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.
3. Побудова моделі захисту системи, визначення затрат часу, ресурсів та засобів.

Варіант 8

1. Критерії інформаційної безпеки.
2. Рівні мережних атак (фізичний, канальний, мережний, транспортний, сеансовий) згідно із моделлю OSI.
3. Отримання пароля на основі помилок у реалізації. Соціальна психологія й інші способи отримання пароля.

Варіант 9

1. Канали витоку інформації.
2. Вимоги при роботі з конфіденційною інформацією.
3. Отримання пароля на основі помилок адміністратора та користувача.

Варіант 10

1. Класифікація інформації за рівнем конфіденційності.
2. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).
3. Термінали захищеної інформаційної системи.

ВКАЗІВКИ ДО ВИКОНАННЯ КОНТРОЛЬНИХ РОБІТ

Задачами контрольної роботи є:

- систематизація і закріплення теоретичних та практичних фахових знань, виявлення уміння студента застосовувати ці знання при вирішенні конкретних наукових, технічних, економічних і виробничих задач;
- перевірка уміння студента самостійно освоювати та використовувати сучасні інформаційні технології, програмно-апаратні засоби обчислювальної техніки;
- розвинення у студента навичок ведення самостійного науково-практичного пошуку, оволодіння методикою дослідження й експериментування при вирішенні проблем і питань, поставлених на курсове проектування;
- закріплення знань і навичок виконання графічних робіт та інших конструкторських документів у відповідності до вимог і правил, встановлених державними стандартами, Єдиною системою конструкторської документації (ЄСКД), Єдиною системою проектної документації (ЄСПД), іншими чинними нормативно-технічними документами;

Головна мета контрольної роботи – визначення рівня теоретичної та практичної підготовки студента з курсу „Технології захисту інформації та патентознавство”.

Контрольна робота сприяє розвиткові у студента творчої ініціативи і самостійності в проведенні аналізу, добору й обґрунтування найбільш раціональних інженерних рішень.

Контрольна робота надає студентові таких навичок виконання виробничих завдань, які допоможуть йому швидко адаптуватися до умов праці у професійному колективі.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем.
2. Технічні засоби захисту інформації.
3. Програмно-апаратні засоби захисту інформації.
4. Адміністративні засоби захисту інформації.
5. Визначення об’єкта захисту та можливих загроз.
6. Принцип розімкнутого управління захистом інформації.
7. Принцип зворотного зв’язку при захисті інформації.
8. Відповідальність за протиправні дії згідно із законодавством України.
9. Ідентифікація й аутентифікація.
10. Механізми підзвітності та аудиту.
11. Класи безпеки.
12. Критерії інформаційної безпеки.
13. Канали витоку інформації.
14. Класифікація інформації за рівнем конфіденційності.
15. Класифікація криптоалгоритмів.
16. Тайнопис, криптографія з ключем.
17. Симетричні криптоалгоритми.
18. Асиметричні криптоалгоритми.
19. Скремблери.
20. Мережа Фейстеля.
21. Переставні криптоалгоритми.
22. Підставні криптоалгоритми.
23. Поточні, блочні шифри. Одиниці кодування.
24. Системи шифрування дискових даних (системи прозорого та спеціального видів шифрування).
25. Системи шифрування даних, які передаються в мережах (канальне та абонементне шифрування).

26. Системи аутентифікації електронних даних: імітовставка.

27. Системи аутентифікації електронних даних: електронний підпис.

28. Засоби управління криптографічними ключами: генерація, зберігання і розподілення ключів.

29. Стратегія захисту інформації у фінансово-економічних інформаційних системах.

30. Комплекс технічних засобів захисту інформації.

31. Комплекс програмних засобів захисту інформації.

32. Сучасна ситуація у сфері інформаційної безпеки.

33. Рівні мережних атак (фізичний, канальний) згідно із моделлю OSI.

34. Рівні мережних атак (мережний, транспортний, сеансовий) згідно із моделлю OSI.

35. Типи атак.

36. Вимоги при роботі з конфіденційною інформацією.

37. Політика ролей.

38. Технології цифрових підписів.

39. Стратегія вибору систем виявлення атак.

40. Термінали захищеної інформаційної системи.

41. Отримання пароля на основі помилок адміністратора та користувача.

42. Отримання пароля на основі помилок у реалізації.

43. Соціальна психологія й інші способи отримання пароля.

44. Побудова моделі захисту системи, визначення затрат часу, ресурсів та засобів.

45. Система пошуку та захисту від вторгнення LIDS.

46. Створення дерева каталогів із правами доступу. Зміна змісту каталогу access.conf.

47. Добавлення користувача та встановлення його прав.

48. Служби, які можуть захищати від кібероблав.

49. Установлення та зміна паролів, контроль доступу в систему, права користувачів.

50. Завдання моніторингу систем інформаційної безпеки.

51. Поясніть модель оптимізації режиму моніторингу систем інформаційної безпеки.

52. Критерії оптимізації режиму моніторингу систем інформаційної безпеки.

53. Як розрахувати необхідний рівень захисту програмного продукту від несанкціонованого використання?

Відповідність підсумкової семестрової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	***Відмінно***	**A**	**Відмінно** (відмінне виконання лише з незначною кількістю помилок)
82 – 89	**Добре**	**B**	**Дуже добре** (вище середнього рівня з кількома помилками)
75 – 81		**C**	**Добре** (в загальному вірне виконання з певною кількістю суттєвих помилок)
67 – 74	**Задовільно**	**D**	**Задовільно** (непогано, але зі значною кількістю недоліків)
60 – 66		**E**	**Достатньо** (виконання задовольняє мінімальним критеріям)
35 – 59	**Незадовільно**	**FX**	**Незадовільно** (з можливістю повторного складання)
1 – 34		**F**	Незадовільно **(з обов'язковим повторним курсом)**

Підсумкова семестрова рейтингова оцінка в балах, за національною шкалою та шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента.

Підсумкова семестрова рейтингова оцінка заноситься до залікової книжки та навчальної картки студента, наприклад, так: ***92/Відм./A, 87/Добре/B, 79/Добре/C, 68/Задов./D, 65/Задов./E*** тощо..

Підсумкова рейтингова оцінка з дисципліни визначається як середньоарифметична оцінка з підсумкових семестрових рейтингових оцінок у балах (з цієї дисципліни – за перший та другий семестри) з наступним її переведенням в оцінки за національною шкалою та шкалою ECTS.

СПИСОК ЛІТЕРАТУРИ

Основна

1. Домарев В. В. Безопасность информационных технологий. — СПб.: DiaSoft, 2002. — 688 с.
2. Защита компьютерных систем от разрушающих программных воздействий: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 128 с.
3. Зегжда Д. П., Калинин М. О., Степанов П. Г. Теоретические основы информационной безопасности. Защищенные операционные системы: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 69 с.
4. Конев И., Беляев А. Информационная безопасность предприятия. — СПб.: БХВ Петербург, 2003. — 752 с.
5. Методы и средства защиты информации / Под ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.

Додаткова

6. О вирусах, червях, троянцах и бомбах. Защита информации. Переводы. — М.: Знание, 1990. — (Новое в жизни, науке и технике. Сер. “Вычислительная техника и ее применение”). — С. 9.
7. Касперський Е. “Дыры” в MS-DOS и программы защиты информации // КомпьютерПресс. — 1991. — № 10.
8. Баранов А. П., Зегжда Д. П., Зегжда П. Д., Ивашко А. М., Корт С. С. Теоретические основы информационной безопасности (Дополнительные главы): Учеб. пособие. — СПб., 1998. — 173 с.
9. Мельников В. Криптография от папируса до компьютера. — М.: ABF, 1996.
10. Галатенко В. А., Гагин А. В. Информационная безопасность: Обзор основных положений: Ч. 1–3. Jet INFO, № 1, 2, 3, 1996.

11. Герасименко В. А., Размахнин М. К. Криптографические методы в автоматизированных системах // Зарубежная радиоэлектроника. — 1982. — № 8.
12. Головкин Б. А. Надежное программное обеспечение (обзор) // Зарубежная радиоэлектроника. — 1978. — № 12. — С. 3–61.
13. Давыдовский А. И. Использование средств автоматизации, заслуживающих доверие // Защита информации. — 1992. — № 1. — С. 63–71.
14. Дж. Л. Месси. Введение в современную криптологию // ТИИЭР. — М.: Мир, 1988. — Т. 76, № 5, Май. — С. 24–42.
15. Джефф П. Р. Шифрование данных методом гаммирования // Электроника. — 1973. — Т. 46. — № 1.
16. Защита программного обеспечения / Д. Гроувер, Р. Сатер, Дж. Фипс и др. / Под ред. Д. Гроувера: Пер. с англ. — М.: Мир, 1992. — 285 с.
17. Зегжда Д. П., Корт С. С., Каулио В. В. Теоретические основы информационной безопасности: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 34 с.
18. Защита информации в компьютерных системах: Лабораторный практикум / П. Д. Зегжда, Д. Ю. Копылов, С. С. Корт, И. Д. Медведовский и др.; Под ред. проф. П. Д. Зегжды. — СПб., 1996. — 89 с.