МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП ТЕХНОЛОГО-ЕКОНОМІЧНИЙ ФАХОВИЙ КОЛЕДЖ БІЛОЦЕРКІВСЬКОГО НАУ

ПОГОДЖУЮ
Заступник директора
з навчальної роботи
___ ___О.М.Харчишина
«__»_____ 2021 р.

ЗАТВЕРДЖУЮ
Директор ВСП ТЕФК БНАУ
_____Л.П.Лендрик
«__»_____ 2021 р.

ЗАХИСТ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

ПРОГРАМА

навчальної дисципліни
для **підготовки фахівців ОКР «молодший спеціаліст»**

спеціальності 076 Підприємництво, торгівля та біржова діяльність (освітня програма «Інформаційна діяльність підприємства»)

Програму розглянуто і схвалено
циковою комісією
інформаційних технологій
Протокол № ____ від _____
Голова циклової комісії
_____ В.М. Бойко

БІЛА ЦЕРКВА 2021

Укладач Матусевич О.В., викладач ВСП Технолого-економічний фаховий коледж Білоцерківського НАУ

ПОЯСНЮВАЛЬНА ЗАПИСКА

Входження України у світовий інформаційний простір зумовлює швидке впровадження новітніх досягнень комп'ютерних і телекомунікаційних технологій. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У зв'язку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації. Захист інформації - це сукупність організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації. Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виключне право тої або іншої держави. Проте в останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різноманітних країн. Слідством цього процесу значно зросла потреба у фахівцях із захисту інформації.

Інформаційні технології охоплюють методи збору, обробки, перетворення, зберігання і розподілу інформації. Протягом тривалого часу ці технології розвивалися на мовній і "паперовій" буквено-цифровій основі. У цей час інформаційно-ділова активність людства зміщається в область кібернетичного простору. Цей простір стає реальністю світової спільноти і визначає перехід до "безпаперового, електронного" розвитку інформаційних технологій. Електронний обмін інформацією дешевше, швидше і надійніше "паперового".

Інформаційні процеси, що проходять повсюдно у світі, висувають на перший план, поряд із задачами ефективного опрацювання і передача інформації, найважливішу задачу забезпечення безпеки інформації. Це пояснюється особливою значимістю для розвитку держави Його інформаційних ресурсів, зростанням вартості інформації в умовах ринку, її високою уразливістю і нерідко значним збитком у результаті її несанкціонованого використання.

Предмет навчальної дисципліни

Предметом дисципліни є сучасні інформаційні технологій у галузі інформаційної безпеки та криптографічні методи захисту інформації.

Мета навчальної дисципліни

Метою вивчення дисципліни «Захист інформації в інформаційних системах» є формування теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення захисту програмної продукції.

Головна мета навчальної дисципліни “Захист інформації на підприємстві” – сформувати знання, вміння та навички в застосуванні засобів захисту інформаційних систем.

Навчальна дисципліна передбачає набуття навичок та вмінь для забезпечення

захисту комп'ютерної інформації, що реалізуються засобами обчислювальної техніки і забезпечують пошук, подання, перетворення та передавання інформації.

Основні завдання

Основні завдання дисципліни «Захист інформації в на підприємстві» - вивчення сучасних інформаційних технологій у галузі інформаційної безпеки та криптографічних методів захисту інформації. Ставлять за мету підготовку фахівців з розробки та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності, контролю передачі інформації, ідентифікації, аутентифікації, криптографії, інтегрованих систем, політики безпеки, менеджменту в галузі безпеки.

В результаті вивчення дисципліни студент повинен **знати**:

- основні поняття та терміни;
- причини знищення інформації та способи її відновлення;
- склад, структуру та принципи організації систем захисту інформації;
- принципи організації розділення доступу до інформації в обчислювальних системах.

В результаті вивчення предмета студент повинен **вміти**:

- аналізувати степінь інформаційної безпеки в обчислювальних системах.
- виконувати дублювання, оновлення та архівацію інформації;
- класифікувати та знищувати комп'ютерні віруси;
- організовувати комплекс заходів по розмежуванню доступу до інформації.

Виконання в повному обсязі практичних занять, передбачених програмою, дає можливість студентам надалі самостійно використовувати програми у навчальному процесі та на виробництві.

Тематичний план, приведений у програмі, є орієнтовним. Викладачі можуть вносити відповідні зміни і доповнення до робочих навчальних програм в залежності від специфіки підготовки спеціалістів і матеріально-технічного забезпечення. Внесені в план зміни повинні бути обговорені на засіданні циклової комісії і затверджені заступником директора з навчальної роботи.

ТЕМАТИЧНИЙ ПЛАН

№	Назва розділу, теми	Кількість годин			
		всього	у тому числі		
			теоретичні	лабораторно-практичні	самостійне вивчення
		1	2	3	4
1.	Вступ. Безпека інформації на підприємстві: сутність, значення і завдання	6	4	-	2
2.	Інформаційна система підприємства як об’єкт захисту	2	-	-	2
3.	Класифікація загроз інформації на підприємстві	10	2	2	6
4.	Захист об’єктів інформаційної системи	4	2	-	2
5.	Технічний захист інформації	4	4	-	-
6.	Парольні системи захисту для операційних систем	8	2	4	2
7.	Нормативно-правові аспекти захисту інформації	4	-	-	4
8.	Захист від шкідливих програм	18	2	6	10
9.	Архівація даних і сховищ та їх захист	8	2	4	2
10.	Основні елементи онлайнової безпеки	14	2	6	6
11.	Управління системою захисту інформації	18	2	6	10
12.	Криптографічні методи захисту інформації	39	5	20	14
	Всього:	**146**	**36**	**46**	**64**

1. Вступ. Безпека інформації на підприємстві: сутність, значення і завдання
Вступ. Основні завдання захисту інформації. Поняття інформації та інформаційної безпеки. Об'єкти захисту інформації та їх властивості. Розподіл інформації за ступенем важливості

2. Інформаційна система підприємства як об'єкт захисту
Поняття інформаційної системи. Складові інформаційної системи. Поняття комерційна таємниця.

3. Класифікація загроз інформації на підприємстві
Поняття інформаційної загрози. Класифікація загроз. Основні загрози та канали витоку інформації. Типові вразливості систем і аналіз причин їх появи. Характеристика випадкових загроз інформації. Характеристика навмисних загроз інформації. Категорії порушників.
Практична робота №1
Модель порушника. Моделі загроз. Класифікації моделі загроз.

4. Захист об'єктів інформаційної системи
Методи захисту комп'ютерної інформації (правові, організаційні, технічні). Організаційні заходи захисту засобів комп'ютерної інформації.

5. Технічний захист інформації
Апаратний засіб захисту інформації. Завдання апаратного захисту. Програмний засіб захисту інформації. Поняття ідентифікації та аутентифікації. Системи оброблення конфіденційної інформації. Встановлення паролю на завантаження BIOS.

6. Парольні системи захисту для операційних систем
Встановлення паролю на завантаження ОС Windows. Захист файлів та папок в ОС Windows. Утиліти блокування доступом.
Практична робота №2
Активізація екранної заставки та встановлення пароля екранної заставки для захиста комп'ютера від несанкціонованого доступу.
Практична робота №3
Захист файлів та папок в ОС Windows.

7. Нормативно-правові аспекти захисту інформації
Призначення стандартів інформаційної безпеки. Законодавча і нормативна база захисту інформації в Україні. Оцінювання захищеності інформації, яку обробляють у комп'ютерних системах. Міжнародний стандарт ISO/IEC 15408.

8. Захист від шкідливих програм
Класифікація шкідливого програмного забезпечення. Комп'ютерні віруси та їх види. Програмні закладки. Файлові віруси. Завантажувальні віруси. Макровіруси.

Мережні хробаки та «трояни». Захист від комп'ютерних вірусів. Алгоритм роботи користувача з антивірусними програмами.

Практична робота №4

Види шкідливих програм та їх дія.

Практична робота №5

Робота з антивірусними програмами.

9. Архівація даних і сховищ та їх захист

Резервне копіювання. Архівування, відновлення та зберігання даних. Сховище даних та основні вимоги до нього.

Практична робота №6

Резервне копіювання даних.

Практична робота №7

Архівація даних.

10. Основні елементи онлайнової безпеки

Засоби захисту інформації в мережі. Характеристика процесу ідентифікації та аутентифікації користувачів. Аудит користувачів обчислювальних систем. Міжмережні екрани. Системи виявлення атак.

Практична робота № 8

Настроювання параметрів безпеки браузера. Настроювання та використання брандмауера

Практична робота № 9

Робота з онлайновими антивірусними програмами.

Практична робота № 10

Захист електронної пошти.

11. Управління системою захисту інформації

Безпека ОС Windows: засоби захисту в операційній системі Windows. Основні підсистеми комплексу засобів захисту інформації. Захист інформаційних ресурсів від несанкціонованого доступу. Використання методу забезпечення захисту інформації керування доступом.

Практична робота № 11.

Захист електронної інформації від несанкціонованого доступу з використанням параметрів доступу.

Практична робота № 12 .

Парольний захист БД Access. Захист на рівні користувача.

Практична робота № 13.

Адміністрування баз даних. Шифрування БД.

12. Криптографічні методи захисту інформації

Поняття криптографії, шифрування, криптоаналізу, криптології, стенографії.

Способи симетричного шифрування (перестановка, заміна, комбінування). Асиметричне шифрування. Стійкість криптоалгоритмів. Криптоаналітичні методи розкриття.

Практична робота №14.
Створення нової пари ключів з використанням утиліти PGPkeys.
Практична робота №15 (4 год).
Дослідження алгоритму шифрування Цезаря.
Практична робота №16 (4 год).
Шифрування повідомлень за допомогою алгоритму RSA.
Практична робота №17 (4 год).
Система шифрування Віженера.
Практична робота №18.
Систематичні групові коди.
Практична робота №19.
Використання коригувальних кодів для захисту інформації. Код Хеммінга. Циклічний код.
Практична робота №20.
Використання функції хешування.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

ОСНОВНА ЛІТЕРАТУРА

1. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони. Підручник.-О.:ОНАЗ ім..О.С.Попова, 2019.-320с.
2. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних сичтемах та мережах. Навчальний посібник.-Х.: НТУ «ХПІ», 2014.-252с.
3. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації. Навчальний посібник.-Х.: ХНЕУ, 2013.- 479с.

ДОПОМІЖНА ЛІТЕРАТУРА

4. Грайворонський М.В., Новіков О.М., Безпека інформаційно-комунікаційних систем: підручник. - К. : BHV, 2009. - 608 с.: іл.
5. В.Д. Руденко, О.М. Макарчук, М.О. Патланжоглу. Базовий курс інформатики. Книга 1. Основи інформатики. — К., Видавнича група BHV, 2005 — 320 с.
6. Анин, Б. Защита компьютерной информации : БХВ - Петербург, 2000. - 376 с.
7. Информационная безопасность и защита информации : учеб. пособие для студ. высш. учеб. заведений / В. П. Мельников, С.А.Клейменов, А.М.Петраков ; под. ред. С.А.Клейменова. — 3-е изд., стер. — М. : Издательский центр «Академия», 2008. — 336 с.
8. Аграновский А. В. , Хади Р. А. Практическая криптография: М.: СОЛОН - ПРЕСС, 2009. - 256 с.
9. Кормич Б.А. Інформаційне право: підручник – Харків: БУРУН і К, 2011. – 334с.
10. Мельников В.В. Защита информации в компьютерных системах. -М.: Финансы и статистика, 1997. 368 с.: ил.
11. Филин С.А. Информационная безопасность: Учебное пособие. — М.: Издательство «Альфа-Пресс», 2006. — 412 с.

Інтернет – ресурси

1. http://zakon4.rada.gov.ua/laws/show/505/98
2. http://buklib.net/books/28747/
3. http://www.nbuv.gov.ua/node/208