Міністерство освіти і науки України
Таврійський державний агротехнологічний університет
імені Дмитра Моторного

ЮЛІЯ ХОЛОДНЯК, МИКОЛА МІРОШНИЧЕНКО

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

КУРС ЛЕКЦІЙ

для здобувачів ступеня вищої освіти «Бакалавр»
зі спеціальності 122 «Комп'ютерні науки»

Запоріжжя
2023

УДК 004.056.5:003.26.09

Укладачі:
Холодняк Ю. В., доцент кафедри комп'ютерних наук Таврійського державного агротехнологічного університету імені Дмитра Моторного
Мірошниченко М. Ю., старший викладач кафедри комп'ютерних наук Таврійського державного агротехнологічного університету імені Дмитра Моторного

Дозвіл до впровадження та видання надано Вченою радою факультету енергетики і комп'ютерних технологій Таврійського державного агротехнологічного університету імені Дмитра Моторного (протокол № 10 від 24 травня 2023 р.)

Рецензенти:
Дереза О. О., к.т.н., доцент, доцент кафедри інженерної механіки та комп'ютерного проектування Таврійського державного агротехнологічного університету імені Дмитра Моторного
Попова І. О., к.т.н., доцент, доцент кафедри електротехніки і електромеханіки імені професора В.В. Овчарова Таврійського державного агротехнологічного університету імені Дмитра Моторного

Холодняк Ю. В., Мірошниченко М. Ю.
Технології захисту інформації: курс лекцій для здобувачів ступеня вищої освіти «Бакалавр» зі спеціальності 122 «Комп'ютерні науки» / Ю. В. Холодняк, М. Ю. Мірошниченко. Запоріжжя, 2023. 150 с.

В курсі лекцій зібраний, систематизований та викладений матеріал, який охоплює теоретичні питання дисципліни «Технології захисту інформації». Розглядаються основні поняття інформаційної безпеки і компоненти системи захисту інформації. Описуються заходи та засоби законодавчого, адміністративного, організаційного та інженерно-технічного рівнів забезпечення захисту інформації в організаціях та установах. Окрему увагу приділено програмно-технічному захисту інформаційних систем.

Зміст видання відповідає освітньо-професійній програмі підготовки бакалаврів зі спеціальності 122 «Комп'ютерні науки».

© Холодняк Ю. В., Мірошниченко М. Ю.,
© Таврійський державний агротехнологічний університет імені Дмитра Моторного, 2023

ЗМІСТ

ВСТУП.....6
ТЕМА 1. ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....7
1.1 Вступ до дисципліни.....7
1.2 Основні складові інформаційної безпеки.....10
1.3 Класифікація загроз інформаційної безпеки.....11
1.4 Вимоги до моделі інформаційної безпеки.....16
1.5 Об'єктно-орієнтований підхід до інформаційної безпеки.....29
1.6 Українське законодавство в галузі інформаційної безпеки.....36
Контрольні питання.....39

ТЕМА 2. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ. КЕРУВАННЯ ДОСТУПОМ.....40
2.1 Основні поняття і концепції.....40
2.2 Ідентифікація і механізми підтвердження достовірності користувача.....43
2.2.1 Одноразові паролі.....46
2.2.3 Сервер автентифікації Kerberos.....47
2.2.4 Ідентифікація за допомогою біометричних даних.....48
2.3 Взаємна автентифікація користувачів.....50
2.4 Протоколи ідентифікації з нульовою передачею знань.....54
2.4.1 Спрощена схема ідентифікації з нульовою передачею знань.....54
2.4.2 Паралельна схема ідентифікації з нульовою передачею знань.....56
2.4.3 Схема ідентифікації Гіллоу-Куіскуотера.....57
2.5 Керування доступом.....58
2.5.1 Основні поняття.....58
2.5.2 Рольове керування доступом.....61
Контрольні питання.....65

ТЕМА 3. ЗАГРОЗИ ІНФОРМАЦІЇ. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.....66
3.1 Найпоширеніші загрози доступності.....66
3.2 Шкідливе програмне забезпечення.....69
3.3 Основні загрози цілісності.....72
3.4 Основні загрози конфіденційності.....73

3.5 Види атак на криптосистеми 75
3.6 Криптографічні засоби захисту інформації 78
3.6.1 Симетрична (секретна) методологія 80
3.6.2 Асиметрична (відкрита) методологія 81
3.7 Поширення ключів 85
3.8 Алгоритми шифрування 88
3.8.1. Симетричне шифрування 88
3.8.2. Асиметричне шифрування 93
3.9 Стійкість шифру 94
3.10 Хеш-функція 95
3.11 Електронний цифровий підпис 97
Контрольні питання 101

ТЕМА 4. СТАНДАРТИ І СПЕЦИФІКАЦІЇ В ОБЛАСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 102
4.1 Оцінні стандарти і технічні специфікації. «Помаранчева книга» як оцінний стандарт 102
4.1.1 Основні поняття 103
4.1.2 Механізми безпеки 105
4.1.3 Класи безпеки 107
4.2 Інформаційна безпека розподілених систем. Рекомендації X.800 . 111
4.2.1 Мережеві сервіси безпеки 111
4.2.2 Мережеві механізми безпеки 113
4.2.3 Адміністрування засобів безпеки 114
4.3 Стандарт ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій» 116
4.3.1 Основні поняття 116
4.3.2 Функціональні вимоги 118
4.3.3 Вимоги довіри безпеці 121
4.4 Гармонізовані критерії європейських країн 122
4.5 Інтерпретація «Помаранчевої книги» для мережних конфігурацій 124
Контрольні питання 126

ТЕМА 5. КЕРУВАННЯ РИЗИКАМИ. ТЕХНОЛОГІЇ ЗАХИСТУ ПРИВАТНИХ МЕРЕЖ 128
5.1 Основні поняття 128

5.2 Підготовчі етапи керування ризиками 130
5.3 Основні етапи керування ризиками 132
5.4 Технології захисту приватних мереж. Брандмауери 135
5.4.1 Різновиди брандмауерів 136
5.4.2 Схеми підключення 138
5.4.3 Адміністрування 140
5.5 Віртуальні приватні мережі 142
5.5.1 Концепція побудови захищених віртуальних приватних мереж VPN 142
5.5.2 Сутність і зміст технології віртуальних приватних мереж 143
5.5.3 Тунелювання 145
5.5.4 Технічні й економічні особливості впровадження технологій VPN у корпоративні мережі 146
Контрольні питання 147

СПИСОК ЛІТЕРАТУРИ 149

ВСТУП

Дисципліна «Технології захисту інформації» призначена для вивчення основних положень та принципів побудови та використання програмних та апаратно-програмних засобів забезпечення безпеки програм та даних у комп'ютерних системах та мережах. Опанування сучасних технологій роботи із даними на рівні створення та налагодження програмного забезпечення, засвоєння та використання методів захисту даних та програмного забезпечення є необхідним компонентом підготовки кваліфікованого інженера-програміста (Software Engineer), системного архітектора (System Architect), архітектора програмного забезпечення (Software Architect).

Метою вивчення дисципліни є набуття студентами здатності забезпечувати захист інформації, що обробляється в інформаційних системах і комп'ютерних мережах з метою реалізації встановленої політики інформаційної безпеки. Це досягається вивченням теоретичних основ побудови і практики застосування методів та засобів захисту інформації в інформаційних системах з метою запобігання несанкціонованому доступу, витоку, руйнації, знищення і модифікації інформації різної категорії шляхом реалізації політики і створення комплексних корпоративних систем захисту інформації.

В курсі лекцій викладено основні положення законодавчої бази в сфері захисту інформації в інформаційних системах; склад організаційних, технічних та програмно-апаратних засобів комплексної системи захисту корпоративної інформації; канали витоку корпоративної інформації; загрози інформації в інформаційних системах; принципи побудови, дії та захисту від комп'ютерних вірусів; методи, етапи способи та засоби здійснення кібернетичних атак на комп'ютерні системи; методи, алгоритми і технології криптографічного захисту інформації в інформаційних системах; методи і засоби автентифікації та ідентифікації; принципи керування доступом; стандарти і технічні специфікації в області інформаційної безпеки.

Даний курс лекцій включає теми змістовних модулів курсу «Технології захисту інформації», який викладається для здобувачів вищої освіти, що навчаються за спеціальністю 122 «Комп'ютерні науки».