МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
Кафедра інформаційних систем і технологій

«МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ТРАНСПОРТНОЇ ГАЛУЗІ»

НАВЧАЛЬНО-МЕТОДИЧНИЙ КОМПЛЕКС

навчальної дисципліни

підготовки доктора філософії
(назва освітньо-кваліфікаційного рівня)
за спеціальністю 122 «Комп'ютерні науки та інформаційні технології»

Київ
2016

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
Кафедра інформаційних систем і технологій

«МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ТРАНСПОРТНОЇ ГАЛУЗІ»

ПРОГРАМА
навчальної дисципліни

підготовки доктора філософії
(назва освітньо-кваліфікаційного рівня)
за спеціальністю 122 «Комп'ютерні науки та інформаційні технології»

Київ
2016

РОЗРОБЛЕНО ТА ВНЕСЕНО: Національний транспортний університет

(повне найменування вищого навчального закладу)

РОЗРОБНИКИ ПРОГРАМИ: професор кафедри інформаційних систем і технологій, д.т.н., професор Баранов Г.Л., доцент кафедри інформаційних систем і технологій, к.т.н., доцент Міронова В.Л., доцент кафедри інформаційних систем і технологій, к.т.н. Косенко В.Р.

Робочу програму схвалено на засіданні Ради факультету транспортних та інформаційних технологій

Протокол № __ від «__» _____ 2016 року

ВСТУП

Навчальна дисципліна «Методи та засоби захисту інформації на об'єктах транспортної галузі» є невід'ємною частиною циклу комп'ютерних дисциплін, необхідних фахівцям-аналітикам які, використовуючи сучасні комп'ютерні і телекомунікаційні технології, проводять теоретичну та практичну підготовку по проектуванню й застосуванню на транспорті з різноманітними транспортними засобами навичок в області захисту інформації й інформаційної безпеки..

Мета *навчальної дисципліни* – ознайомити PhD-студентів із сучасними інформаційними технологіями побудови і дослідження систем та практичними навичками використання методів та засобів захисту інформації на об'єктах транспортної галузі.

Предмет навчальної дисципліни – методологія захисту інформації, методи і процеси дослідження систем транспортної галузі, а також сучасні засоби і технології захисту інформації на об'єктах транспортної галузі.

Вивчення дисципліни дозволяє PhD-студентам за спеціальністю 122 «Комп'ютерні науки та інформаційні технології» оволодіти знаннями та навичками використання сучасних інформаційних систем і технологій в області захисту інформації й інформаційної безпеки; забезпечення вивчення основних програмно-апаратних засобів захисту комп'ютерів і програм; практичного використання сучасних методів, засобів та технологій забезпечення інформаційної безпеки при роботі в мережі. Дисципліна викладається на другому році навчання, що дозволяє PhD-студентам застосувати отримані знання і навички при написанні дисертаційної роботи.

Завдання:

- оволодіння теоретичними знаннями в області інформаційних технологій і забезпечення їхньої безпеки, а також керування інформаційними ресурсами;
- придбання прикладних знань в області створення систем захисту інформації, а також оптимізації моделей складних процесів бізнесу;
- оволодіння навичками самостійного використання відповідних інструментальних програмних систем.

У результаті вивчення навчальної дисципліни PhD-студент повинен ***знати:***

- загальні характеристики системності та системного підходу;
- питання адміністративного й організаційно-правового забезпечення захисту інформації;
- основні системи захисту інформації в Україні й у провідних закордонних країнах;
- основні методологічні положення захисту інформації;
- основні програмно-апаратні засоби захисту комп'ютерів і програм;
- загальні питання забезпечення інформаційної безпеки при роботі в мережі;
- особливості захисту інформації в СУБД.

У результаті вивчення навчальної дисципліни PhD-студент повинен ***вміти:***

- обмежувати використання ресурсів комп'ютера на основі роздільного доступу користувачів в операційну систему;
- організовувати реєстрацію користувачів в мережній операційній системі;
- організовувати захист інформації в локальній мережі на рівнях входу в мережу й системи прав доступу;
- організовувати безпечну роботу в Інтернет і відправлення поштових повідомлень у глобальній мережі;
- використовувати засоби захисту даних від руйнуючих програмних впливів комп'ютерних вірусів.

1. Програма навчальної дисципліни

Модуль 1. Проблеми інформаційної безпеки та технології захисту даних.

Змістовий модуль 1. Проблеми інформаційної безпеки.

Тема 1. Основні поняття захисту інформації та інформаційної безпеки. Аналіз загроз інформаційної безпеки. Введення у мережевий інформаційний обмін. Аналіз загроз мережевої безпеки. Забезпечення інформаційної безпеки мереж.

Тема 2. Основні поняття політики безпеки. Структура політики безпеки організації. Розробка політики безпеки організації. Роль стандартів інформаційної безпеки. Міжнародні стандарти інформаційної безпеки. Вітчизняні стандарти безпеки інформаційних технологій.

Змістовий модуль 2. Технології захисту даних.

Тема 3. Основні поняття криптографічного захисту інформації. Симетричні криптосистеми шифрування. Асиметричні криптосистеми шифрування. Функція хешування. Електронний цифровий підпис. Управління криптоключами..

Тема 4. Автентифікація, авторизація, і адміністрування дій користувачів. Методи автентифікації, що використовують паролі та PIN-коди. Строга автентифікація. Біометрична автентифікація користувача. Апаратно-програмні системи ідентифікації та автентифікації.

Модуль 2 Багаторівневий захист корпоративних мереж, технологія виявлення вторгнень та управління засобами захисту інформації.

Змістовий модуль 3. Багаторівневий захист корпоративних мереж.

Тема 5. Проблеми забезпечення безпеки ОС. Архітектура підсистеми захисту ОС. Захист в ОС UNIX. Засоби безпеки ОС Windows XP.

Тема 6. Функції міжмережевих екранів. Концепція побудови віртуальних захищених мереж VPN. Захист бездротових мереж. Архітектура засобів безпеки IPSec

Змістовий модуль 4. Технологія виявлення вторгнень та управління засобами захисту інформації.

Тема 7. Концепція адаптивного управління безпекою. Технологія аналізу захищеності. Засоби виявлення мережевих атак. Комп'ютерні віруси і проблеми антивірусного захисту. Антивірусні програми і комплекси.

Тема 8. Побудова систем антивірусного захисту мережі. Завдання управління системою мережевого захисту. Архітектура управління засобами мережевого захисту. Аудит і моніторинг безпеки.

3. Рекомендована література

1. ISO 15408-1-3: 1999. (ГОСТ Р-2002). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. Ч. 2. Защита функциональных требований. Ч. 3. Защита требований к качеству.
2. ISO 17799: 2002. Управление информационной безопасностью. Практические правила.
3. ISO 13335-1-5: 1996-1998. ИТ. ТО. Руководство по управлению безопасностью. Ч. 1. Концепция и модели обеспечения безопасности информационных технологий. Ч. 2. Планирование и управление безопасностью информационных технологий. Ч. 3. Техника управления безопасностью ИТ. Ч. 4. Селекция (выбор) средств обеспечения безопасности. Ч. 5. Безопасность внешних связей.
4. Закон України про інформацію, від 02.10.92.
5. Закон України про науково-технічну інформацію, від 25.06.93.
6. Закон України про захист інформації в автоматизованих системах, від 05.07.94.
7. Закон України про державну таємницю, від 21.01.94.
8. Закон України про Національну програму інформатизації, від 04.02.98.
9. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-001-98, ДСТСЗІ СБ України, Київ, 1998.
10. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-98, ДСТСЗІ СБ України, Київ, 1998.
11. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 2.2-001-98, ДСТСЗІ СБ України, Київ, 1998.
12. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – НД ТЗІ 2.2.-002 – 98, ДСТСЗІ СБ України, Київ, 1998.
13. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
14. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року № 2171-III.
15. Концепція технічного захисту інформації в Україні від 8 жовтня 1997 року № 1126.
16. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
17. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
18. Анин Б.Ю. Защита информации в компьютерной системе. – СПб.: БХВ – Санкт-Петербург, 2000. – 384с.

19. Антоненко В.М., Рогушина Ю.В. Сучасні інформаційні системи і технології. Навчальний посібник. – К.: КСУ МГІ, 2005. – 131 с.

20. Антонюк А.О. Основи захисту інформації в автоматизованих системах. Навч. посібн. - К.: Видавн. дім "КМ Академія", 2003. – 244 с.

21. Баричев С., Криптография без секретов. – М.: 1998.

22. Вертузаев М.С.,Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник /За редаг. С.Г. Лаптева.- К.:Вид-во Європ. Університету, 2001.- 321 с.

23. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994, в 2-х томах.

24. Герасименко В. А. Основы защиты информации: Учебник для вузов / Б. А. Герасименко, А. А. Малюк. — М.: Изд-во ООО «Ин-комбук», 1997. – 537 с.

25. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему – СПб: Мир и семья –95 ,1997. – 312с.

26. Мельников В.В. Защита информации в компьютерных системах. – М.: «Финансы и статистика», 1997.

27. Романец Ю.В., Тимофеев П. А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328с.

28. Росоловський В.М., Анкудович Г.Г., Катерноза К.О., Шевченко М.Ю. Основи інформаційної безпеки автоматизованої інформаційної системи державної податкової служби України: Навчальний посібник/За заг. ред. М.Я. Азарова. – Ірпінь: Академія ДПС України, 2003. – 466 с.

29. Петров А.А. Компьютерная безопасность. Криптографиче¬ские методы защиты. – М.: ДМК, 2000. – 448 с.

30. Праффенбергер Б. Эффективная работа с Microsoft Internet Explorer 5.5. – СПб.: Питер, 1998. – 416с.

31. Программно-аппаратные средства обеспечения информаци¬онной безопасности. Защита программ и данных: Учеб. пособие для вузов / П.Ю. Белкин, О. О.Михальский, А. С. Першаков. – М.: Радио и связь, 1999. – 168 с.

32. Столлингс В. Криптография и защита сетей: теория и практика. – М.: Вильямс. – 2001.

33. Чижухин Г.Н. Основы защиты информации в вычислительных системах и сетях ЭВМ: Учеб. Пособие. – Пенза: Изд-во Пенз. гос. ун-та, 2001. – 164 с.; 19 ил., 5 табл., библиогр. 8 назв.

34. Эдвардс М.Д. Безопасность в Интернете на основе Windows NT – М.:Издательский отдел "Русская Редакция" ТОО "Chennel Trading Ltd " – 1999. – 656 с.

35. Э. Ратбон. Windows XP для «чайников». – М.: Вильямс, 2002. – 304 с.

36. Microsoft Windows XP: Home Edition и Professional /Под ред. А.Н.Чекмарева. – СПб: BHV-Петербург, 2002. – 624 с.

4. **Форма підсумкового контролю успішності навчання - іспит**
5. **Засоби діагностики успішності навчання – усне опитування, захист лабораторних робіт, контрольні роботи, тестування**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
Кафедра інформаційних систем і технологій

"**ЗАТВЕРДЖУЮ**"
Завідувач кафедри інформаційних
систем і технологій Гавриленко В.В.

_____
"___"_____2016 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ТРАНСПОРТНОЇ ГАЛУЗІ»
(шифр і назва навчальної дисципліни)

Спеціальність: 122 «Комп'ютерні науки та інформаційні технології»
(шифр і назва спеціальності)
інститут, факультет, відділення: факультет транспортних та інформаційних технологій
(назва інституту, факультету, відділення)

Київ
2016

Робоча програма «Методи та засоби захисту інформації на об'єктах транспортної галузі» для PhD-студентів за спеціальністю 122 «Комп’ютерні науки та інформаційні технології».

Розробники: професор кафедри інформаційних систем і технологій, д.т.н., професор Баранов Г.Л., доцент кафедри інформаційних систем і технологій, к.т.н., доцент Міронова В.Л., доцент кафедри інформаційних систем і технологій, к.т.н., Косенко В.Р.

Робочу програму схвалено на засіданні кафедри інформаційних систем і технологій

Протокол № __ від «__» _____ 2016 року

Завідувач кафедри інформаційних систем і технологій

_____ (Гавриленко В.В.)
(підпис)

2. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, рівень вищої освіти, ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 5</td><td>Галузь знань
12 “Інформаційні технології”
(шифр і назва)</td><td colspan="2">Дисципліна професійної та практичної підготовки (самостійного вибору навчального закладу)</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність:

122 «Комп’ютерні науки та інформаційні технології»</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів – 4</td><td>2-й</td><td>-</td></tr>
<tr><td>Індивідуальне навчально-дослідне завдання: немає</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150</td><td>3-й</td><td>-</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних – 30
самостійної роботи студента – 60</td><td rowspan="11">Третій рівень вищої освіти
(доктор філософії)</td><td>15 год.</td><td>-</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>0 год.</td><td>-</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>30 год.</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>105 год.</td><td>-</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">0 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>екзамен</td><td>-</td></tr>
</table>

Примітка.
Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить (%):

для денної форми навчання – 42,86%

для заочної форми навчання – н/д

2. Мета та завдання навчальної дисципліни

Навчальна дисципліна «Методи та засоби захисту інформації на об'єктах транспортної галузі» є невід’ємною частиною циклу комп’ютерних дисциплін, необхідних фахівцям-аналітикам які, використовуючи сучасні комп’ютерні і телекомунікаційні технології, проводять теоретичну та практичну підготовку по проектуванню й застосуванню на транспорті з різноманітними транспортними засобами навичок в області захисту інформації й інформаційної безпеки..

Мета *навчальної дисципліни* – ознайомити PhD-студентів із сучасними інформаційними технологіями побудови і дослідження систем та практичними навичками використання методів та засобів захисту інформації на об'єктах транспортної галузі.

Предмет навчальної дисципліни – методологія захисту інформації, методи і процеси дослідження систем транспортної галузі, а також сучасні засоби і технології захисту інформації на об'єктах транспортної галузі.

Вивчення дисципліни дозволяє PhD-студентам за спеціальністю 122 «Комп'ютерні науки та інформаційні технології» оволодіти знаннями та навичками використання сучасних інформаційних систем і технологій в області захисту інформації й інформаційної безпеки; забезпечення вивчення основних програмно-апаратних засобів захисту комп'ютерів і програм; практичного використання сучасних методів, засобів та технологій забезпечення інформаційної безпеки при роботі в мережі. Дисципліна викладається на другому році навчання, що дозволяє PhD-студентам застосувати отримані знання і навички при написанні дисертаційної роботи.

Завдання:

- оволодіння теоретичними знаннями в області інформаційних технологій і забезпечення їхньої безпеки, а також керування інформаційними ресурсами;
- придбання прикладних знань в області створення систем захисту інформації, а також оптимізації моделей складних процесів бізнесу;
- оволодіння навичками самостійного використання відповідних інструментальних програмних систем.

У результаті вивчення навчальної дисципліни PhD-студент повинен ***знати:***

- загальні характеристики системності та системного підходу;
- питання адміністративного й організаційно-правового забезпечення захисту інформації;
- основні системи захисту інформації в Україні й у провідних закордонних країнах;
- основні методологічні положення захисту інформації;
- основні програмно-апаратні засоби захисту комп'ютерів і програм;
- загальні питання забезпечення інформаційної безпеки при роботі в мережі;
- особливості захисту інформації в СУБД.

У результаті вивчення навчальної дисципліни PhD-студент повинен ***вміти:***

- обмежувати використання ресурсів комп'ютера на основі роздільного доступу користувачів в операційну систему;
- організовувати реєстрацію користувачів в мережній операційній системі;
- організовувати захист інформації в локальній мережі на рівнях входу в мережу й системи прав доступу;
- організовувати безпечну роботу в Інтернет і відправлення поштових повідомлень у глобальній мережі;
- використовувати засоби захисту даних від руйнуючих програмних впливів комп'ютерних вірусів.

3. Програма навчальної дисципліни

Модуль 1. Проблеми інформаційної безпеки та технології захисту даних.

Змістовий модуль 1. Проблеми інформаційної безпеки.

Тема 1. Основні поняття захисту інформації та інформаційної безпеки. Аналіз загроз інформаційної безпеки. Введення у мережевий інформаційний обмін. Аналіз загроз мережевої безпеки. Забезпечення інформаційної безпеки мереж.

Тема 2. Основні поняття політики безпеки. Структура політики безпеки організації. Розробка політики безпеки організації. Роль стандартів інформаційної безпеки. Міжнародні стандарти інформаційної безпеки. Вітчизняні стандарти безпеки інформаційних технологій.

Змістовий модуль 2. Технології захисту даних.

Тема 3. Основні поняття криптографічного захисту інформації. Симетричні криптосистеми шифрування. Асиметричні криптосистеми шифрування. Функція хешування. Електронний цифровий підпис. Управління криптоключами.

Тема 4. Автентифікація, авторизація, і адміністрування дій користувачів. Методи автентифікації, що використовують паролі та PIN-коди. Строга автентифікація. Біометрична автентифікація користувача. Апаратно-програмні системи ідентифікації та автентифікації.

Модуль 2. Багаторівневий захист корпоративних мереж, технологія виявлення вторгнень та управління засобами захисту інформації.

Змістовий модуль 3. Багаторівневий захист корпоративних мереж.

Тема 5. Проблеми забезпечення безпеки ОС. Архітектура підсистеми захисту ОС. Захист в ОС UNIX. Засоби безпеки ОС Windows XP.

Тема 6. Функції міжмережевих екранів. Концепція побудови віртуальних захищених мереж VPN. Захист бездротових мереж. Архітектура засобів безпеки IPSec

Змістовий модуль 4. Технологія виявлення вторгнень та управління засобами захисту інформації.

Тема 7. Концепція адаптивного управління безпекою. Технологія аналізу захищеності. Засоби виявлення мережевих атак. Комп'ютерні віруси і проблеми антивірусного захисту. Антивірусні програми і комплекси.

Тема 8. Побудова систем антивірусного захисту мережі. Завдання управління системою мережевого захисту. Архітектура управління засобами мережевого захисту. Аудит і моніторинг безпеки.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
Модуль 1. Проблеми інформаційної безпеки та технології захисту даних.												
Змістовий модуль 1. Проблеми інформаційної безпеки.												
Тема 1. Основні поняття захисту інформації та інформаційної безпеки. Аналіз загроз інформаційної безпеки. Введення у мережевий інформаційний обмін. Аналіз загроз мережевої безпеки. Забезпечення інформаційної безпеки мереж.	17	1	-	2	-	14	-	-	-	-	-	-
Тема 2. Основні поняття політики безпеки. Структура політики безпеки організації. Розробка політики безпеки організації. Роль стандартів інформаційної безпеки. Міжнародні стандарти інформаційної безпеки. Вітчизняні стандарти безпеки інформаційних технологій.	17	2	-	4	-	11	-	-	-	-	-	-
Разом за змістовим модулем 1	34	3	-	6	-	25	-	-	-	-	-	-

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
<u>Змістовий модуль 2.</u> Технології захисту даних.												
Тема 3. Основні поняття криптографічного захисту інформації. Симетричні криптосистеми шифрування. Асиметричні криптосистеми шифрування. Функція хешування. Електронний цифровий підпис. Управління криптоключами.	18	2	-	4	-	6	-	-	-	-	-	-
Тема 4. Автентифікація, авторизація, і адміністрування дій користувачів. Методи автентифікації, що використовують паролі та PIN-коди. Строга автентифікація. Біометрична автентифікація користувача. Апаратно-програмні системи ідентифікації та автентифікації.	18	2	-	4	-	8	-	-	-	-	-	-
Разом за змістовим модулем 2	36	4	-	8	-	24	-	-	-	-	-	-
Разом за модулем 1	70	7	-	14	-	49	-	-	-	-	-	-
<u>Модуль 2.</u> Багаторівневий захист корпоративних мереж, технологія виявлення вторгнень та управління засобами захисту інформації.												
<u>Змістовий модуль 3.</u> Багаторівневий захист корпоративних мереж.												

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
Тема 5. Проблеми забезпечення безпеки ОС. Архітектура під-ми захисту ОС. Захист в ОС UNIX. Засоби безпеки ОС Windows XP.	20	2	-	4	-	14	-	-	-	-	-	-
Тема 6. Функції м/м екранів. Концепція побудови мереж VPN. Захист БМ. Архітектура засобів безпеки IPSec	20	2	-	4	-	14	-	-	-	-	-	-
Разом за змістовим модулем 3	40	4	-	8	-	28	-	-	-	-	-	-
<u>Змістовий модуль 4.</u> Технологія виявлення вторгнень та управління засобами захисту інформації.												
Тема 7. Концепція АУ безпекою. Технологія аналізу захищеності. Засоби виявлення МА. Комп'ютерні віруси і проблеми антивірусного захисту. Антивірусні програми і комплекси.	20	2	-	4	-	14	-	-	-	-	-	-
Тема 8. Побудова систем антивірусного ЗМ. Завдання управління системою МЗ. Архітектура управління засобами МЗ. Аудит і моніторинг безпеки.	20	2	-	4	-	14	-	-	-	-	-	-
Разом за змістовим модулем 4	40	4	-	8		28	-	-	-	-	-	-
Разом за модулем 2	80	8	-	16	-	30	-	-	-	-	-	-
Усього годин	150	15	-	30	-	105	-	-	-	-	-	-

5. Теми семінарських занять

Семінарські заняття навчальним планом дисципліни «Методи та засоби захисту інформації на об'єктах транспортної галузі» не передбачені.

6. Теми практичних занять

Практичні заняття навчальним планом дисципліни «Методи та засоби захисту інформації на об'єктах транспортної галузі» не передбачені.

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	*2*	*3*
1	Захист інформації за допомогою пароля.	4
2	Вивчення програмних засобів шифрування, комп'ютерної стеганографії и захисту від шкідливих програм.	4
3	Захист баз даних на прикладі MS ACCESS.	4
4	Одноалфавітна підстановка.	4
5	Багатоалфавітна одноконтурна звичайна підстановка.	4
6	Дослідження криптоалгоритма шифрування RSA.	4
7	Дослідження електронного цифрового підпису RSA.	6
Разом		30

8. Самостійна робота

Розподіл годин самостійної роботи

Всього годин - 105	
ПМК –підготовка до модульного контролю	**2 (***2 години на семестр***)**
ПП – підготовка до практичних занять	**45** *(до 4 годин на пару)*
ППК- підготовка до підсумкового контролю (іспиту)	**2**
ІКЗ – індивідуальне комплексне завдання або **ІНДЗ -** Індивідуальне навчально-дослідне завдання (наукова робота)	**56**

Розподіл годин самостійної роботи за темами

№ з/п	Назва теми	Кількість Годин	
		ПП	**ІКЗ**
1.	Тема 1. Опис стандартів інформаційної безпеки.	5	-
2.	Тема 2. Опис технологій захисту даних	5	8
3.	Тема 3. Технології захисту корпоративних мереж.	5	8
4.	Тема 4. Сучасні системи управління мережевим захистом.	5	8
5.	Тема 5. Захист інформації при роботі з мережевими ресурсами.	5	8
6.	Тема 6. Технологія аналізу захищеності.	6	12
7.	Тема 7. Оцінка якості та ефективності інформаційних систем.	6	3
8.	Тема 8. Аудит і моніторинг безпеки.	8	9
	Всього за темами	**45**	**56**
	Підготовка до модульного контролю №1	**1**	**-**
	Підготовка до модульного контролю №2	**1**	**-**
	Підготовка до підсумкового контролю (заліку)	**2**	**-**
	Всього	**49**	**56**

Розподіл годин за етапами виконання індивідуального навчально-дослідного завдання (наукової роботи)

№ п/п	**Етапи виконання роботи**	**Термін виконання**	**Кількість годин**
1.	Опрацювання літератури та складання змісту наукової роботи	20.09.15	10
2.	Написання І розділу роботи	15.10.16	10
3.	Написання ІІ розділу роботи	01.11.16	15
4.	Написання ІІІ розділу роботи	15.11.16	15
5.	Написання вступу та висновку	20.11.16	2
6.	Загальне оформлення роботи та здача її на перевірку	25.11.16	2
7.	Захист роботи	01.12.16-10.12.16	2
Всього			**56**

9. Індивідуальні завдання

Індивідуальна робота PhD-студента з вивчення дисципліни «Методи та засоби захисту інформації на об'єктах транспортної галузі» проводиться у наступних формах:

1) як аудиторні заняття (за розкладом), передбачені навчальним планом підготовки доктора філософії з комп’ютерних наук і навчальною програмою даної дисципліни.

На аудиторних заняттях проводяться наступні види робіт:

- контроль виконання завдань з тем курсу, винесених для самостійного опрацювання PhD-студентами;
- індивідуальне консультування викладачем PhD-студентів з тематики курсу;
- проведення поточного опитування, модульних контрольних (два модулі);
- звітування у процесі виконання індивідуальних навчально-дослідних завдань (ІНДЗ).

2) виконання та захист ІНДЗ (індивідуального навчально-дослідного завдання в рамках дисертаційної роботи).

ІНДЗ для PhD-студентів денної форми навчання полягає у зборі та обробці статистичних даних екологічних процесів з наступним відображенням їх на електронних картах визначеної території. PhD-студенти в індивідуальному порядку погоджують з викладачем обраний тип даних, обсяги вимірювань та їх територіальне походження.

10. Методи навчання

При вивченні курсу «Методи та засоби захисту інформації на об'єктах транспортної галузі» застосовуються 3 групи методів навчання:

– методи організації і здійснення навчально-пізнавальної діяльності;

– методи стимулювання і мотивації навчально-пізнавальної діяльності;

– методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності.

Перша група охоплює вербальні методи передачі і сприймання навчальної інформації (розповідь, лекція); наочні (ілюстрація, презентація); практичні (вправи, групові та індивідуальні завдання). В межах самостійної роботи – робота з книгами, методичними матеріалами, Інтернет-джерелами, творчі завдання.

При вивченні курсу активно використовуються інтерактивні методи (при веденні лекцій та семінарських занять) та проблемно-пошукові методи навчання (як при веденні аудиторних занять, так і при організації самостійної роботи PhD-студентів).

11. Методи контролю

Методи поточного контролю: поточне тестування, індивідуальне опитування, фронтальне опитування, перевірка домашніх завдань, перевірка індивідуальних завдань.

Методи модульного контролю: письмова контрольна робота, підсумкове тестування.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ (екзамен)

1. Основні поняття захисту інформації та інформаційної безпеки.
2. Аналіз загроз інформаційної безпеки.
3. Введення у мережевий інформаційний обмін.
4. Аналіз загроз мережевої безпеки.

5. Забезпечення інформаційної безпеки мереж.
6. Основні поняття політики безпеки.
7. Структура політики безпеки організації.
8. Розробка політики безпеки організації.
9. Роль стандартів інформаційної безпеки.
10. Міжнародні стандарти інформаційної безпеки.
11. Вітчизняні стандарти безпеки інформаційних технологій.
12. Основні поняття криптографічного захисту інформації.
13. Симетричні криптосистеми шифрування.
14. Асиметричні криптосистеми шифрування.
15. Функція хешування.
16. Електронний цифровий підпис.
17. Управління криптоключами.
18. Автентифікація, авторизація, і адміністрування дій користувачів.
19. Методи автентифікації, що використовують паролі та PIN-коди.
20. Строга автентифікація.
21. Біометрична автентифікація користувача.
22. Апаратно-програмні системи ідентифікації та автентифікації.
23. Проблеми забезпечення безпеки ОС.
24. Архітектура підсистеми захисту ОС.
25. Захист в ОС UNIX.
26. Засоби безпеки ОС Windows XP.
27. Функції міжмережевих екранів.
28. Особливості функціонування міжмережевих екранів.
29. Схеми мережевого захисту на базі міжмережевих екранів.
30. Концепція побудови віртуальних захищених мереж VPN.
31. VPN-рішення для побудови захищених мереж.
32. Технічні і економічні переваги технологій VPN.
33. Протоколи формування захищених каналів на канальному рівні.
34. Протоколи формування захищених каналів на сеансовому рівні.
35. Захист бездротових мереж.
36. Архітектура засобів безпеки IPSec.
37. Захист переданих даних за допомогою протоколів AH і ESP.
38. Протокол управління криптоключами IKE.
39. Особливості реалізації засобів IPSec.
40. Управління ідентифікацією та доступом.
41. Організація захищеного віддаленого доступу.
42. Управління доступом за схемою однократного входу з авторизацією Single Sign-On.
43. Протокол Kerberos.
44. Інфраструктура управління відкритими ключами PKI.
45. Концепція адаптивного управління безпекою.
46. Технологія аналізу захищеності.
47. Засоби виявлення мережевих атак.
48. Комп'ютерні віруси і проблеми антивірусного захисту.
49. Антивірусні програми і комплекси.
50. Побудова систем антивірусного захисту мережі.

51.Завдання управління системою мережевого захисту.
52.Архітектура управління засобами мережевого захисту.
53.Аудит і моніторинг безпеки.

12. Розподіл балів, які отримують PhD-студенти

Модулі	Модуль I					Модуль II					Сума за 2 модулі	Підсумковий контроль
Кількість балів за модуль	**30**					**30**						
Змістові модулі	ЗМ 1		ЗМ 2		10 Модульний контроль	ЗМ 3		ЗМ 4		10 Модульний контроль		
Кількість балів за ЗМ та модульний контроль	10		10			10		10				
Кількість балів за видами роботи	Л	Л	Л	Л		Л	Л	Л	Л		**60**	**40**
Відвіду-вання	1	1	1	1		1	1	1	1			
Активність на заняттях	1	1	1	1		1	1	1	1			
Виконання срс	-	6	-	6		-	6	-	6			
Наукова робота	Участь у наукових конференціях, семінарах, круглих столах, студентських олімпіадах і конкурсах – 0-15 балів											**10**

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

13. Методичне забезпечення

1. Конспект опорних лекцій курсу в електронній формі.
2. Методичні вказівки для виконання лабораторних робіт в електронній формі.
3. Варіанти модульних контрольних робіт.
4. Теоретичні питання до екзамену.

14. Рекомендована література

Базова

1. ISO 15408-1-3: 1999. (ГОСТ Р-2002). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. Ч. 2. Защита функциональных требований. Ч. 3. Защита требований к качеству.
2. ISO 17799: 2002. Управление информационной безопасностью. Практические правила.
3. ISO 13335-1-5: 1996-1998. ИТ. ТО. Руководство по управлению безопасностью. Ч. 1. Концепция и модели обеспечения безопасности информационных технологий. Ч. 2. Планирование и управление безопасностью информационных технологий. Ч. 3. Техника управления безопасностью ИТ. Ч. 4. Селекция (выбор) средств обеспечения безопасности. Ч. 5. Безопасность внешних связей.
4. Закон України про інформацію, від 02.10.92.
5. Закон України про науково-технічну інформацію, від 25.06.93.
6. Закон України про захист інформації в автоматизованих системах, від 05.07.94.
7. Закон України про державну таємницю, від 21.01.94.
8. Закон України про Національну програму інформатизації, від 04.02.98.
9. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-001-98, ДСТСЗІ СБ України, Київ, 1998.
10. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-98, ДСТСЗІ СБ України, Київ, 1998.
11. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 2.2-001-98, ДСТСЗІ СБ України, Київ, 1998.
12. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – НД ТЗІ 2.2.-002 – 98, ДСТСЗІ СБ України, Київ, 1998.
13. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
14. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року № 2171-III.
15. Концепція технічного захисту інформації в Україні від 8 жовтня 1997 року № 1126.
16. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
17. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.

18. Анин Б.Ю. Защита информации в компьютерной системе. – СПб.: БХВ – Санкт-Петербург, 2000. – 384с.
19. Антоненко В.М., Рогушина Ю.В. Сучасні інформаційні системи і технології. Навчальний посібник. – К.: КСУ МГІ, 2005. – 131 с.
20. Антонюк А.О. Основи захисту інформації в автоматизованих системах. Навч. посібн. - К.: Видавн. дім "КМ Академія", 2003. – 244 с.
21. Баричев С., Криптография без секретов. – М.: 1998.
22. Вертузаев М.С.,Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник /За редаг. С.Г. Лаптева.-К.:Вид-во Європ. Університету, 2001.- 321 с.
23. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994, в 2-х томах.
24. Герасименко В. А. Основы защиты информации: Учебник для вузов / Б. А. Герасименко, А. А. Малюк. — М.: Изд-во ООО «Ин-комбук», 1997. – 537 с.
25. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему – СПб: Мир и семья –95 ,1997. – 312с.
26. Мельников В.В. Защита информации в компьютерных системах. – М.: «Финансы и статистика», 1997.
27. Романец Ю.В., Тимофеев П. А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328с.
28. Росоловський В.М., Анкудович Г.Г., Катерноза К.О., Шевченко М.Ю. Основи інформаційної безпеки автоматизованої інформаційної системи державної податкової служби України: Навчальний посібник/За заг. ред. М.Я. Азарова. – Ірпінь: Академія ДПС України, 2003. – 466 с.
29. Петров А.А. Компьютерная безопасность. Криптографиче¬ские методы защиты. – М.: ДМК, 2000. – 448 с.
30. Праффенбергер Б. Эффективная работа с Microsoft Internet Explorer 5.5. – СПб.: Питер, 1998. – 416с.
31. Программно-аппаратные средства обеспечения информаци¬онной безопасности. Защита программ и данных: Учеб. пособие для вузов / П.Ю. Белкин, О. О.Михальский, А. С. Першаков. – М.: Радио и связь, 1999. – 168 с.
32. Столлингс В. Криптография и защита сетей: теория и практика. – М.: Вильямс. – 2001.
33. Чижухин Г.Н. Основы защиты информации в вычислительных системах и сетях ЭВМ: Учеб. Пособие. – Пенза: Изд-во Пенз. гос. ун-та, 2001. – 164 с.; 19 ил., 5 табл., библиогр. 8 назв.
34. Эдвардс М.Д. Безопасность в Интернете на основе Windows NT – М.:Издательский отдел "Русская Редакция" ТОО "Chennel Trading Ltd " – 1999. – 656 с.
35. Э. Ратбон. Windows XP для «чайников». – М.: Вильямс, 2002. – 304 с.
36. Microsoft Windows XP: Home Edition и Professional /Под ред. А.Н.Чекмарева. – СПб: BHV-Петербург, 2002. – 624 с.

Додаткова

37. Антонюк А.А., Волощук А.Г., Суслов В.Ю., Ткач А.В. Что такое Оранжевая книга? (Из истории компьютерной безопасности) // Безопасность информации, № 2, 1996.

38. «Безопасность информации». Научно-технический журнал, Киев.

39. Галатенко В.А. Информационная безопасность: практический подход. - М.: Наука, 1998. – 301 с.

40. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: Изд. «ДиаСофт», 1999. – 480 с.

41. «Конфидент. Защита информации». Информационно-методический журнал, СПб.

42. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. Учебное пособие. Изд. 2-е, испр. и доп. М.: 1995. – 84 с.

43. Рублинецкий В.И. Введение в компьютерную криптологию. – Харьков: «ОКО», 1997.

44. Стенг Д., Мун С. Секреты безопасности сетей. – Киев, Диалектика, 1995.

45. Ярочкин В.И. Безопасность информационных систем. – М.: 1996. – 320с.