НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ

ЗАТВЕРДЖУЮ
Директор ІПРІ НАН України
академік НАН України
_____В.В.Петров
«16» 11 2021 р.

ОСНОВИ ІНФОРМАЦІЙНОЇ І КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

(назва навчальної дисципліни)

РОБОЧА ПРОГРАМА
кредитного модуля

ГАЛУЗЬ ЗНАНЬ **12 «Інформаційні технології»**

СПЕЦІАЛЬНІСТЬ **122 «Комп'ютерні науки»**

СПЕЦІАЛІЗАЦІЯ **«Інформаційні технології»**

Ухвалено Вченою радою ІПРІ НАН України
(протокол від « 16 » 11 2021 р. № 11)

Київ
ІПРІ НАН України
2021

2

РОЗРОБНИК ПРОГРАМИ:

завідувач лабораторії, д.т.н., с.н.с. Циганок Віталій Володимирович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

(підпис)

© ІПРІ НАН України, 2021 рік

Опис кредитного модуля

<table>
<tr><th>Галузь знань, спеціальність, спеціалізація</th><th>Загальні показники</th><th>Характеристика кредитного модуля</th></tr>
<tr><td>Галузь знань
12 «Інформаційні технології»
(шифр і назва)</td><td>Назва дисципліни, до якої належить кредитний модуль «Основи інформаційної і кібернетичної безпеки»</td><td>Форма навчання
денна
(денна / заочна)</td></tr>
<tr><td>Спеціальність
122 «Комп’ютерні науки»</td><td>Кількість кредитів ECTS
2</td><td>Статус кредитного модуля
нормативна</td></tr>
<tr><td>Спеціалізація
«Інформаційні технології»</td><td>Кількість тем 7</td><td>Цикл до якого належить кредитний модуль
1.1. Цикл загальної підготовки</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">Індивідуальне завдання
відсутнє
(вид)</td><td>Рік підготовки другий</td></tr>
<tr><td>Семестр третій</td></tr>
<tr><td rowspan="5">Рівень вищої освіти
третій (доктор філософії)</td><td rowspan="3">Загальна кількість годин
60</td><td>Лекції
16 год.</td></tr>
<tr><td>Практичні (семінарські)
14 год.</td></tr>
<tr><td>Лабораторні роботи
0 год.</td></tr>
<tr><td rowspan="2">Тижневих годин:
аудиторних – 2
СРС – 4</td><td>Самостійна робота
30 год.,
у тому числі на виконання індивідуального завдання
0 год.</td></tr>
<tr><td>Вид та форма семестрового контролю
залік</td></tr>
</table>

2. Мета та завдання кредитного модуля

2.1. Метою кредитного модуля є формування у аспірантів здатностей:

– використання майбутніми фахівцями знань щодо технологій захисту від шкідливого програмного забезпечення;

– ознайомлення з основними поняттями про комп’ютерні віруси, історією їх виникнення, основними принципами функціонування та поширення, класифікацією та набуття необхідних знань і навичок щодо захисту інформаційних ресурсів від вірусів;

– використовувати теоретичні знання й практичні навички для прийняття адекватних рішень на гарантоване досягнення очікуваного результату в сфері інформаційної та кібербезпеки.

2.2. Основні завдання кредитного модуля.

Згідно з вимогами програми навчальної дисципліни аспіранти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

знання: термінології пов’язаної з основними поняттями про комп’ютерні віруси, історії їх виникнення, основні принципи функціонування та поширення, класифікації; сучасних загроз безпеці інформаційним системам; сучасних методів протидії загрозам інформаційній та кібербезпеці; технічних методів і засобів захисту інформації; програмних методів і засобів захисту; актуальних проблем захисту від шкідливого програмного забезпечення;

вміння: аналізувати можливості несанкціонованого здобуття інформації потенційними порушниками; аналізувати вплив комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем; виявляти дії вірусів в різних операційних середовищах за допомогою аналізу наявних процесів, за допомогою аналізу кодів підозрілих програм, за допомогою антивірусних програм; організовувати та виконувати практичні дій посадових осіб відділу захисту інформації відповідно до інструкцій і обов'язків; планувати та виконувати конкретні заходи щодо протидії та нейтралізації загроз інформаційній та кібербезпеці; надавати пропозиції щодо вдосконалення нормативних та розпорядчих документів з питань планування, забезпечення, функціонування, коригування заходів безпеки інформації в інформаційно-телекомунікаційних системах спеціального призначення, комп’ютерних системах різних класів для різних організацій;

досвід: підбору та застосування програмного забезпечення для захисту інформаційних систем від різного типу загроз кібербезпеці; прийняття обґрунтованих рішень про необхідність обрання відповідних засобів та заходів.

3. Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні (семінарські) заняття	Лабораторні заняття (комп'ютерний практикум)	СР
Розділ (змістовий модуль) 1. *Основні поняття з теорії вірусів та хакерських атак*						
Тема 1	**Основні поняття з теорії вірусів та хакерських атак**	**60**	**16**	**14**	**0**	**30**
Заняття 1/1	Основні поняття з теорії вірусів 1. Історія комп'ютерних вірусів 2. Основні терміни й елементи безпеки 3. Концепції та етапи хакінгу 4. Основні види шкідливого програмного забезпечення та типи хакерських атак 5. Дослідження уразливостей 6. Комп'ютерні злочини й наслідки Основна література: [1-5] Допоміжна література: [1-12]	**3**	2			1
Заняття 2/1	Хакерські атаки. Збір інформації. 1. Концепції інформаційної розвідки (рекогносцировки). 2. Послідовність збору інформації 3. Методології збору інформації 4. Інструменти збору інформації 5. Заходи протидії збору інформації 6. Тестування на можливість збору інформації Основна література: [1-5] Допоміжна література: [1-6]	**3**	2			1
Заняття 2/2	Сканування, Перебори (Перерахування) та заходи протидії. 1. Сканування мережі. Типи сканування 2. Методологія, техніки та інструменти сканування відкритих портів 3. Заходи протидії скануванню портів 4. Збір банерів 5. Сканування уразливостей 6. Побудова мережевих діаграм уразливих хостів 7. Підготовка проксі. Техніки тунелювання. Анонімайзери 8. Спуфінг IP адреси й заходи протидії 9. Тестування на можливість сканування 10. Концепції перебору 11. Техніки перебору 12. Особливості переборів Netbios, SNMP, UNIX, LDAP, NTP, SMTP, DNS. 13. Заходи протидії перебору	**3**	2			1

	Основна література: [1-5] Допоміжна література: [5-8]					
Заняття 3/1	Безпека хмарних обчислень. 1. Концепція хмарних обчислень 2. Базові елементи безпеки в хмарах 3. Інструменти Cloud Security 4. Вразливості та атаки в хмарах. Основна література: [1-5] Допоміжна література: [7-10]	**З**	2			1
Заняття 3/2	Протидія зламуванню операційних систем. 1. Методології та послідовність злому системи 2. Злом паролів 3. Підвищення привілеїв 4. Виконання додатків 5. Приховування файлів 6 Приховування слідів Основна література: [1-5] Допоміжна література: [1-12]	**З**	2			1
Заняття 3/3	Застосування інструментів сканування. Заходи протидії. 1. Інструменти сканування відкритих портів 2. Тестування на можливість сканування Основна література: [1-4] Допоміжна література: [6]	**З**		1		2
Заняття 3/4	Застосування інструментів збору 1. Концепції перебору 2. Техніки перебору Основна література: [1-4] Допоміжна література: [6]	**З**		1		2
Заняття 4/1	Троянські програми й бекдори. 1. Що таке троян та як працюють трояни 2. Відкриті й приховані канали 3. Типи троянів 4. Методи виявлення троянів 5. Заходу протидії троянам 6. Анти-троянське ПО 7. Тестування на проникнення за допомогою трояна Основна література: [1-5] Допоміжна література: [1-14]	**З**	2			1
Заняття 4/2	Концепції та техніки переборів. Заходи протидії та тестування на можливість перебору. Основна література: [1, 2] Допоміжна література: [6]	**З**		1		2
Заняття 5/1	Віруси й хробаки. 1. Концепції вірусів і троянів 2. Робота вірусу 3. Типи вірусів 4. Хробаки 5. Відмінність хробаків від вірусів 6. Аналіз шкідливого ПО	**З**	2			1

	7. Заходи протидії вірусам 8. Тестування на проникнення за допомогою вірусу Основна література: [1-6] Допоміжна література: [6-8]					
Заняття 5/2	Методи протидії атакам на хмарні сервіси. Способи захисту хмарних інфраструктур. Інструменти Cloud Security. Основна література: [1, 2] Допоміжна література: [5, 13, 14]	**З**		2		1
Заняття 5/3	Методи протидії зламуванню операційних систем. Протидії до злому паролів, підвищення привілеїв, виконання додатків. Способи приховування файлів. Основна література: [1-5] Допоміжна література: [1-12]	**З**		2		1
Заняття 6/1	Аналізатори трафіку - Сніффери. 1. Концепції сніффінгу 2. Як працює сніффер? 3. Типи сніффінгу 4. Апаратні аналізатори протоколів 5. SPAN порт 6. MAC, DHCP, ARP та Спуфінг атаки 7. Отруєння кешу DNS 8. Інструменти сніффінгу 9. Заходи протидії сніффінгу Основна література: [1-5] Допоміжна література: [6-9]	**З**	1			2
Заняття 6/2	Методи виявлення та заходи протидії троянським програмам. Тестування на проникнення за допомогою трояна. Основна література: [1-5] Допоміжна література: [1-12]	**З**		2		1
Заняття 6/3	Аналіз шкідливого ПО. Заходи протидії вірусам та хробакам. Тестування на проникнення за допомогою вірусу Основна література: [1-5] Допоміжна література: [6-9]	**З**		2		1
Заняття 6/4	Сніффери - аналізатори трафіку. Інструменти сніффінгу. Заходи протидії. Основна література: [1-5] Допоміжна література: [6-9]	**З**		2		1
Заняття 7/1	Соціальна інженерія. 1. Концепції соціальної інженерії 2. Техніки соціальної інженерії 3. Імперсонація в соціальних мережах 4. Крадіжка особистості 5. Заходи протидії соціальній інженерії	**З**	1			2

	6. Тестування на проникнення за допомогою соціальної інженерії Основна література: [1-5] Допоміжна література: [6-9]					
Заняття 7/2	Модульна контрольна робота. Основна література: [1-5] Допоміжна література: [1-13]	**3**		1		2
Залік		**6**				6
Всього годин		**60**	**16**	**14**		**30**

4. Самостійна робота

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
1	2	3
1	Тема 1. Основні поняття з теорії вірусів та хакерських атак 1. Визначення поняття “комп’ютерний вірус”. 2. Перші випадки масового зараження комп’ютерними вірусами 3. Умови первісного зараження комп’ютера вірусом. 4. Ознаки присутності вірусних програм. 5. Етичні проблеми пов’язані з розповсюдження комп’ютерних вірусів. 6. Хто й для чого пише віруси? 7. Сучасна ситуація та перспективи. 8. Поведінка комп’ютерних вірусів. 9. “Невидимі” віруси. 10. Самомодифікуючі віруси. 11. Класифікація вірусів. 13. Цикл функціонування вірусів. 14. Деструктивні можливості вірусів. 15. Завантажувальні віруси й боротьба з ними. 16. Макровіруси. 17. Поштові віруси. 18. Файлові віруси. 19. Бутові віруси. 20. Мережеві віруси. 21. Класифікаційний код вірусу. 22. Дескриптор вірусу. 23. Сигнатура вірусу. 24. Алгоритми роботи вірусу. 25. Принципи та алгоритми роботи Word/Excel/Access-макровірусів. 26. Роль комп’ютерних мереж при заражені вірусами. 27. “Небезпечний” Інтернет — міфи та реалії. 28. Небезпечні програми — троянські коні, приховане адміністрування. 29. Поняття вірусних та хакерських атак. 30. Пошкоджені й заражені файли.	24
	Підготовка до заліку	6

5. Індивідуальні завдання

Індивідуальні завдання не плануються.

6. Рейтингова система оцінювання результатів навчання

1. Оцінка з дисципліни виставляється за багатобальною системою, з подальшим перерахуванням у 100-бальну.
2. Максимальна кількість балів з дисципліни дорівнює 100.
3. Нарахування балів по окремих видах робіт:

Рейтинг аспіранта з кредитного модуля складається з балів, що він отримав за:
1. роботу на лекціях та лабораторних заняттях;
2. складання заліку.

Розрахунок шкали (R) рейтингу:

Сума вагових балів контрольних заходів протягом семестру складає:

R=28+52+20=100 балів

Таким чином, рейтингова шкала з кредитного модуля складає 100 балів.

Необхідною умовою заліку є стартовий рейтинг, що дорівнює 60 балів.

Для отримання аспірантом відповідних оцінок (ECTS та традиційних) його рейтингова оцінка **RD** переводиться згідно таблиці:

Шкала оцінювання

Оцінка за 100-бальною шкалою	**Оцінка ЄКТС**	**Оцінка за національною шкалою**
		Диференційована
90 – 100	A	Відмінно
82-89	B	Добре
74-81	C	
64-73	D	Задовільно
60-63	E	
35-59	FX	Незадовільно з можливістю повторногоскладання
0-34	F	Незадовільно зобов’язковим повторним вивченнямдисципліни

7. Контрольні заходи

Основною ціллю проведення контрольних заходів є узагальнення знань аспірантами та закріплення ними вивченого матеріалу. Контрольні заходи

провадять у формі експрес-контролю та усного опитування на лекційних, практичних заняттях, а також виконання завдань під час самостійної роботи. Семестровий контроль – залік.

Перелік питань на залік

Назва теми та перелік основних питань
Тема 1. Основні поняття з теорії вірусів та хакерських атак
1. Основні поняття з теорії вірусів 2. Історія комп'ютерних вірусів 3. Основні терміни й елементи безпеки 4. Концепції та етапи хакінгу 5. Основні види шкідливого програмного забезпечення та типи хакерських атак 6. Дослідження уразливостей 7. Комп'ютерні злочини й наслідки 8. Концепції інформаційної розвідки (рекогносцировки) 9. Послідовність збору інформації 10. Методології збору інформації 11. Інструменти збору інформації 12. Заходи протидії збору інформації 13. Тестування на можливість збору інформації 14. Сканування мережі. Типи сканування 15. Інструменти сніффінгу 16. Заходи протидії сніффінгу 17. Концепції соціальної інженерії 18. Техніки соціальної інженерії 19. Імперсонація в соціальних мережах 20. Заходи протидії соціальній інженерії 21. Тестування на проникнення за допомогою соціальної інженерії

8. Методичні рекомендації

Для кращого засвоєння матеріалу та раціонального розподілення об’єму учбової роботи для аспірантів денної форми навчання наступний розподіл часу вивчення дисципліни:

– лекції – один раз на два тижні;

– лабораторні роботи – один раз на два тижні.

Реалізація цільової настанови кредитного модуля здійснюється чіткою, взаємозв’язаною системою лекційних, практичних та семінарських занять, проведенням індивідуальних та групових консультацій, самостійною роботою аспірантів з вивчення навчального матеріалу, а також поточним та семестровим контролем.

На лекціях розглядаються найбільш складні теоретичні питання, які мають проблемний характер. Лекції складають основу теоретичної підготовки. На лекціях викладається матеріал щодо фундаментальних понять про загрози від шкідливого програмного забезпечення, види загроз та способи боротьби з такими загрозами. Розглядаються види вразливостей сучасних операційних середовищ та способи захисту інформації від згаданих загроз.

Активізація роботи аспірантів досягається правильною організацією

проведення практичних занять. Практичні заняття проводяться з метою вивчення і закріплення окремих теоретичних питань та отримання навичок з практичного використання сучасних методів дослідження ризиків інформаційної безпеки; проектування загроз інформаційній безпеці; прогнозування, виявлення, оцінювання загроз інформаційному простору держави та зменшення наслідків дії від реалізованих загроз; формування дослідницьких навичок щодо аналізування ефективності нормативно-правових документів, практик регулювання суспільних відносин у сфері забезпечення інформаційної безпеки.

Методика проведення практичних занять полягає в оголошенні викладачем теми та порядку проведення заняття, перевірці готовності аспірантів шляхом проведення опитування. Викладач може видає кожному аспіранту або групі з декількох аспірантів практичне завдання. При цьому викладач повинен намагатися максимально активізувати роботу на занятті кожного аспіранта. Наприкінці заняття викладач підводить підсумки, відзначає кращих, а також тих, котрі незадовільно підготувались до заняття або не виконали поставлене завдання, оголошує завдання на самопідготовку.

Крім того, аспіранти отримують методичні та практичні навички з самостійного вивчення навчального матеріалу за навчальними посібниками та з послідовним обговоренням і контролем освоєння матеріалу на практичних заняттях.

Знання навчального матеріалу дисципліни, методичні та практичні навички, здобуті аспірантами, оцінюються на всіх видах занять шляхом проведення контрольних заходів.

Рейтинг аспіранта з навчальної дисципліни формується як сума усіх рейтингових оцінок, які складаються з балів, що він отримує за роботу на лекційних та практичних заняттях, за результатами самостійної роботи.

9. Рекомендована література

9.1. Базова

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. — СПб.: Питер, 2015. — 1120 с. (Глава 9. Безопасность).
2. CEH™ Certified Ethical Hacker Bundle, Third Edition (ebundle) © 2017 by McGraw-Hill Education, – 1221 p.
3. Безруков Н. Н. Компьютерная вирусология. — К., 1991. — 414 с.
4. Гульев И. Компьютерные вирусы, взгляд изнутри. — ДМК, 1998.
5. Коваленко М. М. Комп’ютерні віруси і захист інформації. — К.: Наук. думка, 1999. — 268 с.
6. Касперский Е. В. Компьютерные вирусы: что это такое и как с ними бороться. — СК Пресс, 1998.

9.2. Допоміжна

1. Навчальний курс Інформаційна безпека http://prometheus.org.ua/.
2. Косарёв В. П. Компьютерные сети и системы. — М., 2000.

3. Журнал “Хакер”. — № 32; № 35. — 2001.

4. Домарев В. В. Безопасность информационных технологий. — СПб.: DiaSoft, 2002. — 688 с.

5. История вирусологии — http://comp/comp-anv.php.

6. Антивирусные программы — http/www.allware.info/doc/viruses/avp 6.

7. Галатенко В. А., Гагин А. В. Информационная безопасность — обзор основных положений (Ч. 1, 2, 3), Jet INFO, # 1,2,3, 1996.

8. Галатенко В. А., Гагин А. В., Информационная безопасность — обзор основных положений (Ч. 1, 2, 3), Jet INFO, # 1,2,3, 1996.

9. Защита компьютерных систем от разрушающих программных воздействий / Под ред. проф. П. Д. Зегжды Руководство к практическим занятиям. — СПб., 1998. — 128 с.

10. 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.

11. Компьютеры: Справочное руководство: В 3 т. / Под ред. Г. Хелмса. — М.: Мир, 1986.

12. Конев И., Беляев А. Информационная безопасность предприятия. — СПб.: БХВ Петербург, 2003. — 752 с.

13. Методы и средства защиты информации / За ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.

14. Олецький О. В. Принципи роботи комп’ютерних систем: Навч. посіб. — К.: Вид. дім “КМ Академія”, 2003. — 144 с.