МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
М.В. Афанасьєв

СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЯ АТАКАМ

робоча програма навчальної дисципліни

Галузь знань	**12 “ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”**
Спеціальність	**125 “КІБЕРБЕЗПЕКА”**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**“КІБЕРБЕЗПЕКА”**

Вид дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця

2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 6 від 10.12.2019 р.
Розробник(-и):

Погасій, к.е.н., доцент кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Програма вивчення навчальної дисципліни "Системи виявлення та протидія атакам" складена відповідно до освітньої програми підготовки бакалаврів зі спеціальності 125 "Кібербезпека".

Анотація навчальної дисципліни: Дисципліна “Системи виявлення та протидія атакам” є базовою навчально дисципліною за спеціальністю “Кібербезпека”.

В даний час, при стрімкому розвитку мережевих технологій і глобальної інформатизації суспільства на перший план висуваються проблеми забезпечення високого рівня захищеності інформаційних систем. Зі збільшенням числа комп’ютерних інцидентів, пов’язаних з безпекою, почали стрімко розроблятися системи виявлення атак (СВА).

Студенти, спеціальності "Кібербезпека", які досліджують базові етапи розробки систем виявлення атак і організації, та використовують СВА повинні розуміти й вивчати їх класифікацію, щоб вибрати кращі рішення для систем захисту інформації.

Вивчення інформаційних систем, гарантовано стійких до шкідливих впливів і комп'ютерним атакам, пов'язане з істотними витратами як часу, так і матеріальних ресурсів. Крім того, існує відома зворотна залежність між зручністю користування системою і її захищеністю: чим досконаліше системи захисту, тим складніше користуватися основним функціоналом інформаційної системи.

Предметом навчальної дисципліни є вивчення методів виявлення атак на розподілені інформаційні системи (РІС) на основі аналізу поведінки об'єктів, системи що захищається. дослідження моделей комп'ютерної атаки і методів автоматичного виявлення атаки на основі моделі, що дозволяє виявляти комп'ютерні атаки при спостереженні за поведінкою об'єктів РІС і їх взаємодією.

Метою навчальної дисципліни формування в студентів знань та вмінь щодо захисту комп’ютерних мереж з використанням сучасних програмно-апаратних засобів. Ознайомити з типовими порушеннями безпеки, з методами та засобами захисту інформації в мережах, виявлення, попередження та протидії атакам.

Головне завдання курсу – дослідження ефективності доступних в даний час у сучасних системах виявлення атак і визначити основні недоліки використовуваних в них методів виявлення атак на основі відкритої інформації про програмну архітектуру і використовуваних формальних методів виявлення атак.

Курс	**4**	
Семестр	**8**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**36**
	лабораторні	**38**
Самостійна робота		**74**
Форма підсумкового контролю	**Залік**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Корпоративні мережі та системи доступу	Захист дипломної роботи
Безпека та аудит бездротових та рухомих мереж	
Основи планування та адміністрування служб доступу до інформаційних ресурсів	

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою	Виконувати налаштування захисних механізмів мережних програмно-апаратних засобів;
Здатність здійснювати управління інцидентами інформаційної та кібербезпеки	Використовувати механізми захисту, що реалізовані в програмно-апаратних комплексах, з метою побудови захищених мереж.
Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій	Реалізовувати можливості та особливості використання спеціалізованих програмно-апаратних засобів при проведенні аудиту інформаційної безпеки

3. Програма навчальної дисципліни

Змістовний модуль 1. Методи та засоби виявлення атак.

Тема 1 Вступ. Поняття та класифікація атак на мережі..

1.1. Предмет, ціль і задачі курсу. Поняття та класифікація атак на мережі. Загальна характеристика загроз безпеці корпоративних мереж та методи їх реалізації. Модель програмної атаки, етапи її виконання, класифікація, джерела та наслідки програмних атак.

1.2. Атаки на паролі. Засоби автоматичної генерації, перехвату та відкриття паролів.

1.3. Механізми типових атак, що основані на вразливості мережних протоколів. Атаки на служби та протоколи інформаційного обміну. Засоби реалізації атак на протоколи. Атаки на мережні служби. Атаки з використанням проміжних вузлів та територій.

1.4 Віруси та троянські програми. Методи та засоби впровадження «ворожого» коду та шкідливих програм.

1.5. Методи та інструментальні засоби реалізації програмних атак.

Тема 2. Методи та засоби виявлення атак

2.1. Технології виявлення атак. Прямі та непрямі признаки атак. Методи виявлення атак. Сигнальний аналіз та виявлення аномалій. Обманні системи, функціональні можливості та особливості використання.

2.2. Класифікація та загальна характеристика систем виявлення атак. Вимоги щодо систем виявлення атак. Архітектура, функціональні можливості та особливості базових системи виявлення атак. Використання систем виявлення атак. Розміщення систем виявлення атак. Реагування на інциденти.

Змістовний модуль 2. Попередження, захист та протидія атакам.

Тема 3. Методології протидія атакам

3.1. Створення інфраструктури виявлення та протидії атакам. Вибір, планування та використання механізмів захисту. Класифікація та характеристика механізмів та технологій, що використовуються для протидії атакам.

3.2. Технології міжмережевого екранування. Стратегія та засоби міжмережевого екранування. Фільтрація пакетів: критерії та правила. Реалізація пакетних фільтрів. Шлюзи прикладного рівня.

3.3. Організація віртуальних приватних мереж. Задачі, що вирішують VPN. Захист даних на мережному та транспортному рівнях. Організація VPN прикладного рівня за допомогою протоколу S/MIME. Аналіз захищеності інформації, що передається.

3.4. Технології захищеної обробки інформації. Загальні відомості щодо технології термінального доступу. Забезпечення безпеки сервера ОС Windows Server 2003 та сервера MSTS. Загальні відомості щодо служби каталогів.

3.5. Служби каталогів. Структура каталогу LDAP. Система єдиного входу в мережу на основі протоколу Kerberos. Створення єдиного простору безпеки на базі Active Directory.

3.6. Виявлення і протидія атакам в безпровідних мережах. Інвентаризація мережних пристроїв. Діагностика проблем з пропускною здатністю безпровідних мереж. Контроль політики безпеки. Визначення вразливості конфігурації безпровідних мереж. Системи виявлення безпровідних атак. Позиціювання мережних пристроїв.

3.7. Аудит інформаційної безпеки в мережах. Цілі та задачі проведення аудиту безпеки. Етапи та методи проведення, результати робіт. Нормативно-правові та організаційні методи проведення аудиту безпеки систем.

Теми лабораторних робот

Лабораторна робота №1. Налаштування роботи IPsec в Linux

Лабораторна робота №2. Вивчення функціональних можливостей системи виявлення вторгнень Snort

Лабораторна робота №3. Отримання навиків для роботи з ресурсами Honeypot та Nmap

Лабораторна робота №4. Створення Java додатків в середовищі IDE Eclipse, на прикладі програми виведення інформації про мережеві інтерфейси

Лабораторна робота №5. Вивчення взаємодії по мережі по протоколу HTTP.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів максимальна сума – 100 балів;

модульний контроль, що проводиться у формі контрольних робіт, як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів.

Оцінювання знань студента під час лабораторних занять проводиться за наступними критеріями:

Вміння самостійно формувати комплекс заходів для управління інформаційною безпекою.

Продемонструвати отримані навички щодо налаштування захисних механізмів мережних програмно-апаратних засобів;

Представити дієві механізми управління інцидентами інформаційної та кібербезпеки.

Продемонструвати процес впровадження механізмів захисту, що реалізовані в програмно-апаратних комплексах, з метою побудови захищених мереж.

Виконати моніторинг даних, комп’ютерних зловживань та аномалій.

Реалізовувати можливості та особливості використання спеціалізованих програмно-апаратних засобів при проведенні аудиту інформаційної безпеки

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового заліку та за накопичуваними балами, що були отримані протягом навчального семестру,.

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами навчальної дисципліни розраховується з урахуванням балів, отриманих під поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

Теми змістового модуля			Лекційні заняття	Лабораторні заняття	Письмова контрольна робота	Усього
Змістовний модуль	Тема	Тиждень				
Змістовий модуль 1.	Тема 1	1 Тиждень	1			1
		2 Тиждень	1			1
		3 Тиждень	1			1
		4 Тиждень	1			9
		5 Тиждень	1	4		1
	Тема 2	6 Тиждень	1			5
		7 Тиждень	1			1
		8 Тиждень	1	8	8	9
		9 Тиждень	1			1
		10 Тиждень	1	8		9
Змістовий модуль 2.	Тема 3	11 Тиждень	1			1
		12 Тиждень	1			1
		13 Тиждень	1	8		1
		14 Тиждень	1			1
		15 Тиждень	1			1
		16 Тиждень	1	8		9
	Залік					40
Усього			16	36	8	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	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	не зараховано
1 – 34	F		

5. Рекомендована література

5.1 Основна

1. Вилер, К. Без эффективной коммуникации нет эффективного управления.
2. Головлева, Е. Л. Основы рекламы:учебное пособие для вузов/Е.Л.
3. Головлева. -Ростов-на-Дону:Феникс [и др.],2006.-271 с.
4. Голубкова, Е. Н. Маркетинговые коммуникации/Е. Н. Голубкова.М.:Финпресс,2000.-256 с.
5. Гринберг, Т. Э. Политические технологии: ПР и реклама:учебное пособие для вузов/ Т. Э. Гринберг -М.:Аспект Пресс,2006.-316 с.
6. Доблаев, В. Л. Организационное поведение/ В. Л. Доблаев -
7. Зверинцев, А. Б. Коммуникационный менеджмент: Рабочая книга менеджера PR/ А. Б. Зверинцев -2-е изд., испр.-СПб.:Союз,1997.-287 с.
8. Инженерно-техническая защита информации: учебное пособие/ Торокин А.А. – М.: Гелиос АРВ, 2005. – 960 с.
9. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). Минск, 1999. – 181 с.
10. М.:Эксмос,2002.-318, с.
11. Отличительный облик и имидж местной администрации: Пер. с англ./К. Вилер.Обнинск: Издательство Института муниципального управления,2002.-56 с.
12. Певцов Г.В., Залкін С.В., Сідченко С.О., Хударковский К.І. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: монографія / Г.В. Певцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковский. Х.: Цифрова друкарня № 1, 2014. – 272.
13. Сайт дистанційного навчання ХНЕУ ім. С. Кузнеця навчальної дисципліни “Системи виявлення та протидія атакам” https://pns.hneu.edu.ua/course/view.php?id=5677

5.2 Додаткова

14. Anderson, James P., "Computer Security Threat Monitoring and Surveillance, " Washing, PA, James P. Anderson Co., 1980.

15. Denning, Dorothy E., "An Intrusion Detection Model, " Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119—131

16. Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders, " Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22-23, 1990, pages 110—121.

17. Перейти↑ Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study, " The 11th National Computer Security Conference, October, 1988

18. Smaha, Stephen E., "Haystack: An Intrusion Detection System, " The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988

19. Vaccaro, H.S., and Liepins, G.E., "Detection of Anomalous Computer Session Activity, " The 1989 IEEE Symposium on Security and Privacy, May, 1989

5.3 Інформаційні ресурси в Інтернеті

20. Penetration Testing Software | Metasploit. https://www.metasploit.com/

21. Unrestricted File Upload. https://www.owasp.org/index.php/Unrestricted_File_Upload

22. Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/

23. Secunia Research Community https://secuniaresearch.flexerasoftware.com/community/research/

24. OSVDB | Everything is Vulnerable. https://blog.osvdb.org/

25. National Vulnerability Database. https://nvd.nist.gov/