МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

М. В. Афанасьєв

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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):
Євсеєв С.П, д.т.н., с.н.с., завідувач кафедри КІТ
Ткачов А.М., к.т.н.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

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

1. Вступ

Анотація навчальної дисципліни:

Подано тематичний план навчальної дисципліни й її змістовність за модулями та темами, вміщено плани лекцій і лабораторних занять, матеріал щодо закріплення знань (завдання для самостійної роботи, контрольні запитання), методичні рекомендації та оцінювання знань студентів. Перехід від постіндустріального суспільства до суспільства високих технологій на ряду з позитивними змінами в інформаційному просторі і збільшенні нових форм використання комп'ютерних технологій трансформував і негативні наслідки застосування відкритих комунікаційних систем, забезпечивши не тільки поява нових функцій і послуг, але і еволюцію алгоритмів і сценаріїв їх злому. Особливо гостро це зазначається з розвитком і практичною реалізацією кіберзагроз на інфраструктури критичного застосування (ІКП) до яких відносяться енергетика, транспорт, зв'язок, екологічно небезпечні виробництва, об'єкти оборонного комплексу, фінансово-кредитна сфера і т.п. Особливе місце серед ІКП займають АБС банківського сектора, що забезпечує в останні роки не тільки економічну, а й політичну стабільність держави.

Сучасні комп'ютерні технології, надавши нові інструментарії в життєдіяльність і комунікації банківського сектора якісно змінили і загострили проблему безпеки банківської інформації. Можливості несанкціонованого доступу до інформації, можливості несанкціонованого отримання і, як правило, без істотних організаційних і матеріальних витрат величезних масивів даних, що складають в ряді випадків найцінніші корпоративні ресурси, можливості миттєвого руйнування інформаційних ресурсів, що зберігаються або використовуються в комп'ютерній формі, визначили переклад завдань забезпечення безпеки інформації з розряду допоміжних, в число основних пріоритетів і умов функціонування критичних систем.

Мета навчальної дисципліни:

є навчання студентів використанню сучасних процедур забезпечення інформаційної безпеки, її складових та принципів забезпечення. Розгляд питань забезпечення захисту веб-застосунків.

Курс	**3**	
Семестр	**2**	
Кількість кредитів ECTS	**6**	
Аудиторні навчальні заняття	**лекції**	**40**
	семінарські, практичні	**–**
	лабораторні	**40**
Самостійна робота		**100**
Форма підсумкового контролю	**екзамен**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Основи криптографічного захисту	Основи технічного захисту інформації
Комплексні системи захисту інформації	Організаційне забезпечення захисту інформації

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності	Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки
Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем	Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінувати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж
Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов	Виконувати налаштування інформацій-них систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ

3. Програма навчальної дисципліни

Змістовий модуль 1. Механізми забезпечення інформаційної безпеки

Тема 1. Основні положення Концепції інформаційна безпека

Основні концептуальні положення системи захисту інформації. Концептуальна модель інформаційної безпеки. Загрози конфіденційної інформації. Дії, що призводять до неправомірного оволодінні конфіденційною інформацією. Синергетична модель безпеки інформації.

Тема 2. Стандарти та специфікацій в області інформаційної безпеки

Правовий захист. Розгляд міжнародних стандартів забезпечення інформаційної безпеки ISO 27XXX.

Тема 3. Напрями забезпечення інформаційної безпеки

Правовий захист. Організаційна захист. Інженерно-технічний захист. Фізичні засоби захисту. Апаратні засоби захисту. Програмні засоби захисту. Криптографічні засоби захисту. Методи виявлення аномалій або відхилення від нормального стану СЗІ.

Тема 4. Способи захисту інформації

Способи припинення розголошення. Захист інформації від витоку по візуально-оптичним каналам. Протидія несанкціонованому доступу до джерел

конфіденційної інформації.

Тема 5. Основі моделі забезпечення ІБ

Особливості реалізації процесу нападу на інформацію за відомими моделями. Статичні моделі. Статистичні моделі. Динамічні моделі.

Змістовий модуль 2. Принципи риск менеджменту. Забезпечення інформаційної безпеки в веб-застосунках.

Тема 6. Менеджмент інцидентів інформаційної безпеки

Модель PDCA опису життєвого циклу процесів управління інцидентами інформаційної безпеки. Етапи ефективного менеджменту інцидентів інформаційної безпеки за вимогами міжнародних стандартів ISO 27035 та ISO 18044. Особливості менеджменту за вимогами інцидентів міжнародного стандарту ITIL. Концепція побудови, структура та функціональні особливості ефективної системи менеджменту інцидентів ІБ.

Тема 7. Управління ризиками.

Модель безпеки з повним перекриттям. Методики побудови систем захисту інформації, що включають етап аналізу ризиків. Методика управління ризиками, яка запропонована Microsoft. Методики і програмні продукти для оцінки ризиків.

Тема 8. Основні принципи компрометації веб-застосунків

Основи тестування захищеності. Що тестуємо? Чому це проблема? Захищеність веб-додатків, протокол HTTP

Тема 9. Уразливості серверної частини веб-застосунків

Основні загрози серверної частини: ін'єкція, введення SQL, введення файлу, кодова ін’єкція. Зламане управління сесіями. Небезпечні прямі посилання на об’єкт.

Тема 10. Уразливості клієнтської частини веб-застосунків

Міжсайтовий сценарій (XSS). Підробка міжміських запитів (CSRF). Недійсні перенаправлення.

Тема 11. SOAP API і JSON API. Загальний чек-лист

Тестування API: загальний план. SOAP API и JSON API.

Теми лабораторних робіт

Лабораторна робота 1. Дослідження безпеки в ОС Linux;

Лабораторна робота 2. Дослідження адміністрування в ОС Linux;

Лабораторна робота 3. Дослідження брандмауера netfilter для Linux;

Лабораторна робота 4. Дослідження віддаленого доступу до сервера за допомогою SSH;

Лабораторна робота 5. Дослідження розгортання DHCP-сервера dhcpd;

Лабораторна робота 6. Дослідження розгортання web-сервера apache2;

Лабораторна робота 7. Дослідження розгортання DHCP-сервера dhcpd розгортання DNS-сервера.

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, практичних, семінарських, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі колоквіуму 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 семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час семінарських, практичних і лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності, прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем, відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов. Результатами навчання є: забезпечення знань основ законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних. Забезпечення оцінки можливості проникнення в ІТ-системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ-систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінувати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж. Виконувати налаштування ІС та комунікаційного обладнання; виконувати захист ІС від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина і міцність знань, рівень мислення, вміння систематизувати знання за окремими темами, вміння робити обґрунтовані висновки, володіння категорійним апаратом, навички і прийоми виконання практичних завдань, вміння знаходити необхідну інформацію, здійснювати її систематизацію та обробку, самореалізація на лабораторних заняттях.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних завдань та одне теоретичне завдання, які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або

перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час 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

(вказати засоби оцінювання згідно з технологічною картою)

Теми змістового модуля			Лекційні заняття	Захист лабораторних робіт	Поточні КР	Усього
Змістовий модуль 1	**Тема 1**	1 тиждень	1	–	–	1
	Тема 2	2 тиждень	1	–	–	1
	Тема 2	3 тиждень	1	4	–	5
	Тема 3	4 тиждень	1	–	–	1
	Тема 3	5 тиждень	1	4	–	5
	Тема 4,	6 тиждень	1	–	–	1
	Тема 4	7 тиждень	1	4	–	5
	Тема 5	8 тиждень	1	–	–	1
	Тема 5	9 тиждень	1	4	7	12
Змістовий модуль 2	**Тема 6**	10 тиждень	1	–	–	1
	Тема 7	11 тиждень	1	4	–	5
	Тема 8	12 тиждень	1	–	–	1
	Тема 8	13 тиждень	1	4	–	5
	Тема 9	14 тиждень	1	–	–	1
	Тема 9	15 тиждень	1	4	–	5
	Тема 10	16 тиждень	1	–	7	8
	Тема 11	17 тиждень	1	–	–	1
	Тема 11	18 тиждень	1	–	–	1
Екзамен			–	–	–	40
Усього			18	28	14	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. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6

2. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.

3. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2019 . – 678 с.

5.2 Додаткова

4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

5 Хорошко В. А. Методы и средства зашиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

5.3 Інформаційні ресурси в мережі Інтернет

6. Сайт дистанційного навчання ХНЕУ ім. С. Кузнеця https://pns.hneu.edu.ua/course/view.php?id=4928