МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

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

ВЕБ-БЕЗПЕКА

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***другий (магістерський)***
Освітня програма	***Кібербезпека***

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

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків

2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Алексієв В. О., д.т.н., проф. кафедри КІТ.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

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

Анотація навчальної дисципліни

Зараз безпека веб-рішень набуває великого значення тому, що від надійної та продуктивної роботи веб-ресурсів та сервісів будь-якого підприємства залежить ефективність виконання бізнес процесів та безпосередньо рішення завдань просування продукції чи послуг на ринку країни та зарубіжжя. У дисципліні пропонується комплексний погляд з оцінки та побудови контуру безпеки, починаючи з окремого веб-серверу, до взаємодії розподілених сервісів у корпоративній мережі.

Мета курсу – формування теоретичних знань та практичних умінь у сфері забезпечення безпеки веб-ресурсів, їх інформаційної та кібернетичної безпеки. Забезпечення комплексного захисту бізнес-процесів компанії чи підприємства на рівні веб-рішення. Розглядаються основи програмування захищених веб-сайтів та засоби серверної безпеки рівня веб-серверу, бази даних, засобів авторизації та аутентифікації користувачів.

Результатами вивчення даної дисципліни є придбання навичок з проектування захисту рівня веб-серверу та отримання вмінь користуватися засобами щодо побудови контуру безпеки мережі як для малого підприємства, так й рівня корпоративної мережі.

Характеристика навчальної дисципліни

Курс	**1М**
Семестр	**1**
Кількість кредитів ECTS	**3**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Інформаційна безпека держави	Безпека вбудованих систем
Розробка та аналіз алгоритмів	Технології програмування
Основи побудови та функціонування мікропроцесорних систем	Теоретичні основи криптографії

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КФ 1. Здатність розробляти та впроваджувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства)
КФ 4. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки інформаційних технологій (в т.ч. хмарних технологій та додатків), а також безпеки	ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність ПРН-7 – виявляти, описувати та використовувати систему аналізу зв’язків між інформаційними потоками

бізнес/операційних процесів з метою забезпечення функціонування інформаційно-комунікаційних систем згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства) ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо) ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки
КФ 9. Здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам, а також здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів.	ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо) ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність

Програма навчальної дисципліни

Змістовий модуль 1. Основи безпеки рівня веб-серверу.
Тема 1. *Введення. Основні терміни та визначення.*
Тема 2. *Особливості побудови та розгортання сучасного веб-сайту на базі системи управління вмістом (CMS).*
Тема 3. *Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології віртуалізації рівня операційної системи.*
Тема 4. *Архітектура веб-систем. Об'єкти захисту/атаки.*
Аутентифікація та авторизація.
Тема 5. *Взаємодія між веб-сервісами. REST-інтерфейс та його безпека*.

Змістовий модуль 2. Практика забезпечення безпеки веб-ресурсів.
Тема 6. *Забезпечення безпеки даних. Особливості застосування баз даних для побудови захищених веб-рішень.*
Тема 7. *Відкритий проект по забезпеченню безпеки веб-додатків (OWASP).*
Тема 8. *Перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу.*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції, презентації, бесіди, індивідуальні та групові проєкти, майстер-класи.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

– знати особливості побудови та розгортання сучасного веб-сайту на базі системи управління вмістом (CMS);

– застосовувати засоби безпеки рівня серверної інфраструктури. Володіти на практиці технологіями віртуалізації рівня операційної системи;

– Розуміти різні аспекти побудови архітектура веб-систем. Знати об’єкти захисту/атаки та технології безпеки щодо виконання аутентифікації та авторизації користувачів веб-серверу чи системи;

– аналізувати та декомпозувати рівні взаємодії між веб-сервісами. Розуміти основи побудови REST-інтерфейсу та заходи забезпечення його безпеки;

– вирішувати задачі забезпечення безпеки даних. Знати особливості застосування баз даних для побудови захищених веб-рішень;

– орієнтуватися у проектах відкритої ініціативи з забезпечення безпеки веб-додатків (OWASP – Open Web Application Security Project).

– формулювати напрямки та перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу.

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.

Лекційні заняття: максимальна кількість балів 2,5 (робота на лекції).

Лабораторні заняття: максимальна кількість балів становить 42,5 (виконання лабораторних робіт – 2,5, захист лабораторних робіт – 40, контрольні роботи – 15), а мінімальна – 20.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням іспиту.

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

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне 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. Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню структурної схеми архітектури веб-серверу(ів), виконання його оцінюється 10 балами; третє завдання – евристичне щодо вибору оптимального рішення з організації веб-безпеки, виконання його оцінюється 10 балами.

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.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

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

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція *"Введення. Основні терміни та визначення."*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №1 *"Розгортання веб-серверу у середовищі віртуальної машини. Знайомства з засобами безпеки рівня веб-сервера."*	Виконання лабораторної роботи	0,5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до		

		виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Лекція	Лекція *"Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології віртуалізації рівня операційної системи."*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №2 *" Установка та налагодження веб-сайту на базі CMS. Знайомства з засобами безпеки рівня веб-сайту."*	Виконання лабораторної роботи	0,5
			Захист лабораторної роботи № 1	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Архітектура веб-систем. Об'єкти захисту/атаки"*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №3. *"Тестування на проникнення веб-рішення, що було розгорнуте раніше."*	Виконання лабораторної роботи	0,5
			Захист лабораторної роботи № 2	10
			контрольна робота 1	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція "Взаємодія між веб-сервісами. REST-інтерфейс та його безпека. Забезпечення безпеки даних. Особливості застосування баз даних для побудови захищених веб-рішень"	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №4. *" Розгортання серверу LDAP. Застосування засобів авторизації користувачів веб-сайту засобами LDAP. Аналіз вразливості*	Виконання лабораторної роботи	0,5
			Захист лабораторної	10

		відповідного рішення."	роботи № 3	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція "Особливості застосування інструменту для безперервної інтеграції Jenkins"	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №4. *"Розгортання серверу LDAP. Застосування засобів авторизації користувачів веб-сайту засобами LDAP. Аналіз вразливості відповідного рішення"*	Виконання лабораторної роботи	0,5
			Захист лабораторної роботи № 4	10
			контрольна робота 2	10
Екзамен				40

Рекомендована література

Основна

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с.

2. Евсеев С. П. Концептуальная синергетическая модель оценки безопасности банковской безопасности в организациях банковского сектора / С. П. Евсеев, О. Г. Король // Матеріали Міжнародної науково-практичної конференції“ Проблеми і перспективи розвитку ІТ-індустрії ”: тези доповідей, 20–21 квітня 2017 р. – Х. : ХНЕУ ім. С. Кузнеця, 2017. – С. 51.

3. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ : навч.-метод. посіб. / В. О. Алексієв.– Х. : ХНАДУ, 2008. – 208 с.

4. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. – СПб.: Питер, 2020. – 448 с.

5. Топ-10 OWASP -2017Десять самых критичных угроз безопасности веб-приложений. [Электронный ресурс] – Режим доступа : https://owasp.org/www-pdf-archive/OWASP_Top_10-2017-ru.pdf

6. Уильямс Б., Дэмстра Д., Стэрн Х. WordPress для профессионалов. – СПб.: Питер, 2014. – 464 с.

7. Holistic Info-Sec for Web Developers. [Electronic resource]. –Access mode: https://holisticinfosecforwebdevelopers.com/

8. OWASP Web Security Testing Guide. [Electronic resource]. –Access mode : https://owasp.org/www-project-web-security-testing-guide/

Додаткова

9. Шило С.Г. Інформаційні системи та технології : навч. посіб. / С.Г. Шило, Г.В. Щербак, К.В. Огурцова. – Х. : ХНЕУ, 2013. – 219 с.

10. Ушакова, І. О. Проектування інформаційних систем : практикум / Ушакова І. О. – Х. : ХНЕУ ім. С. Кузнеця, 2015. – 234 с.

11. Глоба Л.С. Розробка інформаційних ресурсів та систем : у 2 т. / Л.С. Глоба // Київ – Т. 1 : Розподілені системи. Поняття розподіленого середовища, Зв'язок, Процеси, Іменування, Синхронизація. – 2013. – 378 с. [Електронний ресурс]. – Режим доступу: http://www.its.kpi.ua/ subjects/56/ Documents/ Глоба книга Том1.pdf.

12. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. – СПб.: Питер, 2020. – 448 с.

13. Уильямс Б., Дэмстра Д., Стэрн Х. WordPress для профессионалов. – СПб.: Питер, 2014. – 464 с.

14. Куалман Э. Безопасная сеть. Правила сохранения репутации в эпоху социальных медиа и тотальной публичности. – М. : Альпина Паблишер, 2018. – 214 с.

Інформаційні ресурси

15. Шпаргалки по безопасности: REST [Электронный ресурс] / Habr. – Режим доступа : https://habr.com/en/company/acribia/blog/453384/.

16. Как установить Linux, Apache, MySQL, PHP (LAMP) в Ubuntu 18.04 [Электронный ресурс] / Mark Drake. DigitalOcean, 2018. – Режим доступа : https://www.digitalocean.com/community/tutorials/linux-apache-mysql-php-lamp-ubuntu-18-04-ru.

17. WordPress Security Fundamentals [Электронный ресурс] / Wordfence. Defiant. – Режим доступа : https://www.wordfence.com/learn/.

18. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Розширена мережева та хмарна безпека" https://pns.hneu.edu.ua/course/view.php?id=7017.