Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«__» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «БЕЗПЕКА WEB РЕСУРСІВ»

для студентів
спеціальності 125 Кібербезпека
освітнього рівня першого (бакалаврського)
освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

Розробник:

ТаджДіні Махіяр, старший викладач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладачі:

ТаджДіні Махіяр, старший викладач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми _____ (підпис) Артем ПЛАТОНЕНКО

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:

на 2023/2024 н.р. _____ (підпис) (Складанний П.І.), «23» 08 2023 р., протокол № 8

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	3	
Семестр	5	
Кількість змістових модулів з розподілом:	5	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	42	
Модульний контроль	6	
Семестровий контроль	30	
Самостійна робота	42	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Безпека Web ресурсів» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої 125.00.01 Безпека інформаційних і комунікаційних систем.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Безпека Web ресурсів» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Безпека Web ресурсів» складається з п'яти змістових модулів: Вступ до курсу та вимоги; XSS та Cookie атаки з перехоплення інформації; Вразливі сторони серверну та профілі ризику; SQLi, XSRF атаки; Злам Автентифікації. Обсяг дисципліни – 120 год (4 кредити).

Метою викладання навчальної дисципліни «Безпека у кіберпросторі» є вивчення атак у веб-просторі та усунення їх наслідків.

Завдання:

- вивчення теоретичних основ і положень захисту інформації;
- вивчення способів криптографічного перетворення інформації;
- отримання необхідних теоретичних знань побудови систем захисту інформації;
- отримання практичних навиків адміністрування систем захисту інформації

У результаті вивчення навчальної дисципліни формуються загальні компетентності:

- ***компетентності у сфері навчання:***
  - здатність до організації самостійної навчальної, практичної та науково-дослідної діяльності;
- ***компетентності у сфері застосування знань в практичних ситуаціях***
  - вміння застосовувати здобуті теоретико-концептуальні професійні знання у процесі практичної, викладацької та науково-дослідної роботи;

фахові компетентності:

- ***компетентності у сфері інформаційної безпеки:***
  - здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки;
  - здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики кібербезпеки;.
  - здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності;
  - здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики кібербезпеки.
- **компетентності у сфері науково-дослідної діяльності:**
  - уміння вивчати і систематизувати досягнення вітчизняних і зарубіжних досліджень у галузі інформаційно-комунікаційних технологій, педагогіки і психології, суміжних галузей знань;
  - вивчати, узагальнювати й упроваджувати на практиці вітчизняний і зарубіжний досвід управління інформаційними технологіями і системами, інформаційною інфраструктурою тощо.
- **компетентності у сфері вмінь працювати в групі:**
  - здатність використовувати навички взаємодії в роботі, компетентності у сфері навичок міжособистісного спілкування
  - здатність до продуктивного використання комунікації як складової професійної діяльності.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- об'єкти програмного забезпечення, на які можливі атаки з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації;
- мови програмування JavaScript, PHP, принципи функціонування XSS та Cookies та методи обмеження доступу вказаних файлів до внутрішньої інформації;
- принципи функціонування «Відбитки пальців» HTTP серверів, моделі маніпулювання HTTP заголовками, поняття Fuzz-тестування, Local file inclusion (LFI), Remote File Inclusion (RFI);
- методи несанкціонованого зйому та навмисного пошкодження інформації та засоби протидії цим спробам;
- методи побудови захисту окремих програмних продуктів;
- основні прийоми і програмні засоби для аналізу та дизасемблювання програмних продуктів з метою їх подальшого несанкціонованого використання, методи захисту від дизасемблювання.

уміти:

- виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконувати адміністрування прав доступу до комп'ютерної системи з метою перешкоди призначення невиправданих привілей;
- виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації;

- використовувати основні прийоми та програмні засоби хакерів для перевірки надійності захисту інформації та стійкості його щодо хакерських атак. забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;

та досягти наступних **програмних результатів навчання:**

ПРз-4 — вирішувати задачі супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискриційних, рольових); вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в ІТС.

ПРз-6 — вирішувати задачі управління процесами забезпечення неперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; вирішувати задачі корекції цілей, стратегій, планів забезпечення неперервності бізнесу після здійснення кібератак, збоїв та відмов різних класів; створювати і впроваджувати плани процесу забезпечення неперервності бізнесу; виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Вступ до курсу та вимоги							
Тема 1. Про курс: навіщо нам потрібна безпека в Інтернеті; огляд топ-10 списку OWASP. Приклад вразливого веб-сайту. Використання Chrome's/Firefox інструментів для розробників; моніторинг та складання запитів за допомогою Fiddler. Модифікація запитів та відповідей у Fiddler. Захист транспортного рівня.	5	2		2			3
Тема 2. Поняття атаки «людини посередині». Захист конфіденційної інформації підчас її пересилання. Ризик надсилання файлів cookies через незахищені з'єднання. Чому завантажувати форми для входу HTTP є ризикованим. Використання вмісту змішаного режиму.	5						3

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Тема 3. Заголовок HSTS; основні поняття JavaScript; основні поняття PHP; серверна сторона VS. Клієнтські мови.	6			2			4
Разом	16	2		4			10
Змістовий модуль 2. XSS та Cookie атаки з перехоплення інформації							
Тема 4. Виявлення ненадійної інформації та її ліквідація. Встановлення сигналів для використання практик ліквідації. Поняття XSS та вихідних даних; визначення обставин використання вихідних даних. Доставка інформації через відображений XSS. Тестування ризиків стійкості XSS. Заголовок X-XSS-Захист.	6	1		2			3
Тема 5. Cookies 101. Поняття Http лише cookies. Поняття безпечних cookies.	6	1		2			3
Тема 6. Обмеження доступу файлів cookie задаванням шляху. Зниження ризику у зв’язку із закінченням терміну дії файлів cookie. Використання тимчасових cookies для подальшого зменшення ризиків.	8	2		2			4
Модульний контроль	2						
Разом	22	4		6			10
Змістовий модуль 3. Вразливості серверної сторони та профіль ризику							
Тема 7. Як зловмисник створює профіль ризику на веб-сайті. Поняття заголовку відповіді сервера. Розміщення ризикованих веб-сайтів; «Відбитки пальців» HTTP серверів. Розкриття інформації через robots.txt. Ризики в джерелах HTML; внутрішнє повідомлення про помилку.	6	1		2			3
Тема 8. Відсутність засобів контролю діагностичних даних. Ідентифікація ненадійних даних у параметрах запитів HTTP. Захоплення запитів та маніпулювання параметрами. Маніпулювання логікою програми за допомогою параметрів. Тестування відсутності перевірки з боку сервера Розуміння побудови моделі.	6	1		2			3
Тема 9. Приведення в дію атаки масового призначення. Маніпуляція HTTP заголовками; Fuzz-тестування; вразливість	8	2		2			4

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
при завантаженні файлу. Local file inclusion (LFI); Remote File Inclusion (RFI)							
Разом	20	4		6			10
Змістовий модуль 4. SQLi, XSRF атаки							
Тема 10. Складові SQLi атак – небезпечні введення та помилки серверу. Складові SQLi атак – назви таблиць та колонок, отримання дійсних облікових даних для сайту. Типи SQL вводу: параметризовані запити та збережені процедури, уникнення введення команд користувача, обмеження привілеїв, перевірка білого списку.	7	1		2			4
Тема 11. Тестування ризикованих рішень. Дослідження структури бази даних за допомогою введення даних. Збирання даних за допомогою введення інформації. Автоматизація атак з “Havij” або “Sqlmap”. Сліпе SQL введення даних; безпечні моделі додатків.	5	1					4
Тема 12. Що таке XSRF? Вивчення за прикладом - XSRF з GET та POST параметрами. XSRF введення даних – референт, заголовок джерела та відповідь на виклик. XSRF введення даних – маркер синхронізатора. Поняття cross site атак. Тестування ризику підробки cross site; роль anti-forgery знаків; тестування підробки cross site запитів проти APIs.	4	2		2			
Модульний контроль	2						
Разом	18	4		4			8
Змістовий модуль 5. Злам Автентифікації							
Тема 13. Встановлення атаки кликджекингу. Поняття міцності паролю та векторів атаки. Обмеження введення символів у паролях. Надсилання облікових даних для створення облікових записів. Перерахування рахунку.	3	1		2			
Тема 14. Відмова від сервісу за допомогою оновлення паролю. Забезпечення правильного оновлення паролю; встановлення небезпечного зберігання	5	1		2			2

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
паролів. Тестування ризиків у функції «запам’ятати мене».							
Тема 15. Повторне підтвердження перед ключовими діями. Тестування брутфорс автентифікації. Тестування незахищеної captcha.	4	2					2
Модульний контроль	2						
Разом	14	4		4			4
Підготовка та проходження контрольних заходів	30						
Усього	120	18		24			42

5. Програма навчальної дисципліни

Змістовий модуль 1. ***Вступ до курсу та вимоги***

Основні питання:

- Поняття безпеки в Інтернеті. Розгляд питань чому веб-сайт може бути вразливим. Важливість захисту інформації в Інтернет просторі
- Використання розробниками Chrome's/Firefox інструментів. Причини існування комп'ютерних злодіїв. Методи проникнення до інформації у комп'ютері (хакінґ, крекінг, фрікінг). Розгляд атаки "Людина посередині", знайомство з cookies
- Поняття заголовку HSTS, JavaScript, PHP, серверної сторони VS та клієнтських мов

Змістовий модуль *2.* *XSS та Cookie атаки з перехоплення інформації*

Основні питання:

- Виявлення ненадійної інформації, практика встановлення сигналів для усунення шкідливих даних
- Поняття XSS та вихідних даних, їх використання. Тестування ризиків стійкості XSS Заголовок X-XSS-Захист
- Поняття HTTP лише для cookies. Поняття безпечних cookies, обмеження доступу файлів cookie задаванням шляху та вивчення умов для використання тимчасових cookies

Змістовий модуль 3. ***Вразливості серверної сторони та профіль ризику***

Основні питання:

- Розгляд питань як зловмисник створює профіль ризику на веб-сайті. Поняття: заголовку відповіді сервера, «Відбитки пальців» HTTP серверів, отримання інформації через robots.txt, ризики інформації, що надходить з джерел HTML
- Вміння ідентифікувати ненадійні дані у параметрах запитів HTTP. Захоплення таких запитів та маніпулювання їх параметрами. Методика маніпулювання логікою програми за допомогою настроюваних параметрів, маніпуляція HTTP заголовками
- Поняття Local file inclusion (LFI), Remote File Inclusion (RFI). Fuzz-тестування

Змістовий модуль 4. ***SQLi, XSRF атаки***
Основні питання:

- Понятння SQLi атак, типи SQL вводу даних. Розвиток вміння тестувати ризикові рішення
- Технологія збору даних за допомогою введення інформації, автоматизація атак з “Havij” або “Sqlmap”
- Поняття XSRF введення даних, cross site атаки. Вивчення ролі anti-forgery знаків

Змістовий модуль 5. ***Злам Автентифікації***
Основні питання:

- Поняття атаки кликджекингу: міцність паролів та вектори атаки. Все про паролі; навіщо існують обмеження на введення символів у паролях
- Тестування ризиків у функції "запам'ятати мене". Повторне підтвердження дії перед ключовими діями. Тестування брутфорс автентифікації та незахищеної captcha

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов’язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп’ютерного контролю:* програми-емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4		Модуль 5	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	1	1	2	2	2	2	2	2	2	2
Відвідування семінарських занять	1										
Відвідування практичних занять	1	2	2	3	3	3	3	2	2	2	2
Відвідування лабораторних занять	1										
Робота на семінарському занятті	10										
Робота на практичному занятті	10	2	20	3	30	3	30	2	20	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10										
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25			1	25			1	25	1	25
Виконання ІНДЗ	30										
Разом		-	28	-	65	-	40	-	54	-	54
Максимальна кількість балів: 241											
Розрахунок коефіцієнта: 241/60=4,02											

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Вступ до курсу та вимоги		**10**	**5**
1	Знайдіть криптографічну проблему та порушений контроль доступу відповідно до стандартів OWASP A3:2017, A5:2017 у відкритому доступі в Інтернеті • виконання завдань відповідно до теми; • опрацювання фахових видань.	10	5
Змістовий модуль 2. XSS та Cookie атаки з перехоплення інформації		**10**	**5**
2	Знайдіть помилки в XSS та XXE відповідно до стандартів OWASP	10	5

№ з/п	Назва теми	Кількість годин	Бали
	A7:2017, A4:2017 у відкритому доступі в Інтернеті: • виконання завдань відповідно до теми; • опрацювання фахових видань.		
Змістовий модуль 3. Вразливі сторони серверу та профіль ризику		**10**	**5**
3	Знайдіть RFI та LFI разом з доступними в Інтернет просторі компонентами дно до стандартів OWASP A9:2017 у відкритому доступі в Інтернеті: • виконання завдань відповідно до теми; • опрацювання фахових видань.	10	5
Змістовий модуль 4. SQLi, XSRF атаки		**8**	**5**
4	Знайдіть модуль перевірки достовірності введених даних користувача та введення даних відповідно до стандартів OWASP A1:2017, ASVS у відкритому доступі в Інтернеті: • виконання завдань відповідно до теми; • опрацювання фахових видань.	8	5
Змістовий модуль 5. Злам Автентифікації		**4**	**5**
5	Знайдіть неправильні налаштування автентифікації та безпеки відповідно до стандартів OWASP A6:2017, A2:2017, у відкритому доступі в Інтернеті: • виконання завдань відповідно до теми; • опрацювання фахових видань.	4	5
	Разом	**42**	**25**

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного

контролю.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом: 10 балів – комплексний комп'ютерний тест з дисципліни; 30 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями здійснювати інтерактивного контенту за спеціальністю.

Оцінювання практичного завдання відбувається в межах від 0 до 30 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь.

Бали за виконання тесту та бали за виконання практичного завдання додаються.

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре — достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре — в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно — посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо — мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання — незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу — досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 18 год., практичні заняття – 24 год., модульний контроль – 6 год., семестровий контроль – 30 год., самостійна робота – 42 год.

Модулі (назви, бали)	**Змістовий модуль 1. Вступ до курсу та вимоги** (28 балів)		**Змістовий модуль 2. XSS та Cookie атаки з перехоплення інформації** (65 балів)			**Змістовий модуль 3. Вразливості серверної сторони та профіль ризику** (40 балів)			**Змістовий модуль 4. SQLi, XSRF атаки** (54 бали)		**Змістовий модуль 5. Злам Автентифікації** (54 бали)	
Лекції (теми, бали)	Поняття безпеки в Інтернеті. Розгляд питань чому веб-сайт може бути вразливим. Важливість захисту інформації в Інтернет просторі Інструменти Chrome's/ Firefox для розробників, Причини існування комп'ютерних злодіїв. Методи проникнення до інформації у комп'ютері (хакінг, крекінг, фрікінг). Розгляд атаки "Людина посередині", знайомство з cookies Поняття заголовку HSTS, JavaScript, PHP, серверної сторони VS та клієнтських мов (1 бали)		Виявлення ненадійної інформації, практика встановлення сигналів для усунення шкідливих даних. Поняття XSS та вихідних даних, їх використання. Тестування ризиків стійкості XSS Заголовок X-XSS-Захист (1 бал)		Поняття HTTP лише для cookies, безпечні cookies, обмеження доступу файлів cookie задаванням шляху та вивчення умов для використання тимчасових cookies (1 бал)	Розгляд питань як зловмисник створює профіль ризику на веб-сайті. Поняття: заголовку відповіді сервера, «Відбитки пальців» HTTP серверів, отримання інформації через robots.txt, ризики інформації, що надходить з джерел HTML Ідентифікування ненадійних даних у параметрах запитів HTTP. Захоплення таких запитів та маніпулювання їх параметрами. Методика маніпулювання логікою програми за допомогою настроюваних параметрів, маніпуляція HTTP заголовками (1 бал)		Поняття Local file inclusion (LFI), Remote File Inclusion (RFI). Fuzz-тестування (1 бал)	Понятння SQLi атак, типи SQL вводу даних. Розвиток вміння тестувати ризикові рішення Технологія збору даних за допомогою введення інформації, автоматизація атак з “Havij” або “Sqlmap” (1 бал)	Понятя XSRF введення даних, cross site атаки. Вивчення ролі anti-forgery знаків (1 бал)	Поняття атаки кликджекингу: міцність паролів та вектори атаки. Все про паролі; навіщо існують обмеження на введення символів у паролях. Тестування ризиків у функції "запам'ятати мене". Повторне підтвердження дії перед ключовими діями. Тестування брутфорс автентифікації та незахищеної captcha (1 бал)	Поняття міцності паролю та векторів атаки. Обмеження введення символів у паролях (1 бал)
Практичні заняття (теми, бали)	Важливість захисту інформації в Інтернет просторі Дослідження методів проникнення до інформації у комп'ютері (11 балів)	Огляд понять заголовку HSTS, JavaScript, PHP, серверної сторони VS та клієнтських мов (11 балів)	Практика встановлення сигналів для усунення шкідливих даних (11 балів)	Дослідження поняття XSS та вихідних даних. Тестування ризиків стійкості XSS Заголовок X-XSS-Захист (11 балів)	Тестування HTTP лише для cookies, безпечні cookies, обмеження доступу файлів cookie задаванням шляху (11 балів)	Розгляд питань створення профілю ризику на веб-сайті. «Відбитки пальців» HTTP серверів, отримання інформації через robots.txt (11 балів	Ідентифікування ненадійних даних у параметрах запитів HTTP. Захоплення таких запитів та маніпулювання їх параметрами (11 балів)	Дослідження поняття Local file inclusion (LFI), Remote File Inclusion (RFI). Fuzz-тестування (11 балів)	Дослідж ення понятння SQLi атак, типи SQL вводу даних. (11 балів)	Автоматизація атак з “Havij” або “Sqlmap” (11 балів)	Тестування ризиків у функції "запам'ятати мене". (11 балів)	Дослідження понятя міцності паролю та векторів атаки (11 балів)
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (5 балів)			Самостійна робота (5 балів)			Самостійна робота (5 балів)		Самостійна робота (5 балів)	
Поточний контроль (вид, бали)			Модульна контрольна робота 1 (25 балів)						Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)											

8. Рекомендовані джерела

Основна (базова):

1. Єсін В.І., Кузнєцов А.А., Сорока Л.С. Безпека інформаційних систем та технологій – Х.: «ЕДЕНА», 2010. – 656с.
2. Горбенко І.Д., Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004 – 368 с.
3. Домарев В.В. Безпека інформаційних технологій: Системний підхід. – К.: "ТІД ДС", 2004. – 992с.

Додаткова

1. Білов Є.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основи інформаційної безпеки: Навч. посібник для ВНЗ. – Львів: Видавництво «Ранок», 2006. – 544 с.
2. Завгородній В.І. Комплексний захист інформації в комп’ютерних системах: Навч. посібник. - К.: Логос, 2011. – 264 с.
3. Хорошков В.К., Чекатков А.А. Методи и засоби захисту інформації / За ред. Ю.С. Ковтанюка – К.: Видавництво «Юніор», 2013. – 504с.
4. Zachman John A., «Enterprise Architecture: The Past and the Future» Article published in DM Review Magazine. December 1999 Issue.

9. Додаткові ресурси (інформаційні ресурси)

1. The Zachman Framework™: A Concise Definition, http://zachmaninternational.com.
2. Introducing The Open Group Architecture Framework (TOGAF), http://www.ibm.com.
3. Service-Oriented Architecture and Enterprise Architecture, http://www.ibm.com.
4. Microsoft Operations Framework; Cross Reference ITIL v3 and MOF 4.0. Microsoft Corporation. May 2009. http://go.microsoft.com/fwlink/?LinkId=151991.