Министерство образования и науки Республики Казахстан

Карагандинский государственный технический университет

УТВЕРЖДАЮ
Председатель Ученого совета,
Ректор КарГТУ
_____Газалиев А.М.
_____2015г.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

Дисциплина **SD(II) 4312** «Спец.дисциплина II»

Модуль **SD 29** Спец.дисциплины

Специальность 5В100200 «Системы информационной безопасности»

Факультет информационных технологий

Кафедра ИТБ

2015

Предисловие

Программа обучения по дисциплине для студента (syllabus) разработана:
_____Солодовниковой И.В._____
(ученая степень, ученое звание Ф. И. О.)

Обсуждена на заседании кафедры ИТБ
Протокол № _____ от «____»_____2015г.
Зав. кафедрой _____ Коккоз М.М. «____»_____2015 г.
(подпись)

Одобрена учебно-методическим советом факультета информационных технологий
Протокол № _____ от «_____»_____2015г.
Председатель _____Мустафина Л.М. «____»_____ 2015г.
(подпись)

Сведения о преподавателе и контактная информация

Солодовникова Ирина Валентиновна , старший преподаватель

(фамилия, имя, отчество преподавателя, ученая степень, ученое звание, должность)

Кафедра ИТБ находится в главном корпусе КарГТУ (Караганда, б.Мира, 56), аудитория 429 , контактный телефон 56-59-35 (1028) , факс _-_, электронный адрес irinasolo@mail.ru

Трудоемкость дисциплины

вид обучения	Семестр	Количество кредитов	Количество кредитов ECTS	Вид занятий					Количество часов СРС	Общее количество часов	Форма контроля
				количество контактных часов			количество часов СРСП	всего часов			
				Лекции	практические занятия	лабораторные занятия					
очная	7	3	5	15	-	30	45	90	45	135	Экзамен

Характеристика дисциплины

Дисциплина «Спец.дисциплина II» входит в цикл профилирующих элективных дисциплин рабочего учебного плана государственного общеобязательного стандарта образования по специальности.

Цель дисциплины

Дисциплина «Спец.дисциплина II» ставит целью изучение теоретических и практических принципов разработки и защиты WEB приложений с учетом современных тенденций, основных типов атак на web-приложения и методов их предотвращения.

Задачи дисциплины

Задачи дисциплины следующие: планирование системы безопасности для web-приложения; создание защищенных web-страниц; кодирование, хэширование и подписывание данных; тестирование системы безопасности web-приложения.

В результате изучения данной дисциплины студенты должны:

иметь представление:

– о принципах разработки и функционирования современных безопасных web приложений; программно-аппаратных средствах анализа и обеспечения безопасности web приложений;

знать:

– виды и способы защиты информации при разработке WEB приложений;
– классификацию основных типов атак на web-приложения;

– основные методы и средства реализации удаленных сетевых атак на WEB-приложения;

– организационно-правовые и нормативные основы защиты интернет-технологий и WEB-приложений;

– основы проектирования и разработки защищенных WEB-приложений;

уметь:

– правильно проектировать и реализовывать все основные компоненты комплексного WEB приложения;

– выявлять уязвимости в web-приложениях;

– проектировать и реализовывать комплексную систему обеспечения ИБ WEB-приложений;

– тестировать и на основе результатов тестирования делать обоснованный выбор средств защиты WEB-приложений;

приобрести практические навыки:

– программной реализации WEB приложения;

– определения и устранения уязвимостей с использованием программно-аппаратных средств анализа безопасности web приложений.

Пререквизиты

Для изучения данной дисциплины необходимо усвоение следующих дисциплин:

1 Методы и средства защиты компьютерной информации

2 Интернет-технологии

3 Web-программирование

Постреквизиты

Знания, полученные при изучении дисциплины «Спец.дисциплина II», используются при освоении следующих дисциплин: при выполнении выпускной работы (дипломного проекта).

Тематический план дисциплины

Наименование раздела, (темы)	Трудоемкость по видам занятий, ч.				
	лекции	практические	лабораторные	СРСП	СРС
1 Введение в безопасность Web-приложений: терминология, статистика атак на web- ресурсы, публичность web-приложений как один из факторов повышенного внимания злоумышленников к web- ресурсам.	1			5	1
2 Уязвимости веб-приложений. Анализ архитектуры Схемы аутентификации. Стандарты в области обеспечения защиты информации.	3			5	1

3 Уязвимости клиентской части. Типовые уязвимости веб-приложений. Рассмотрение кейсов: уязвимости на примере opensource-проектов.	3			5	2
4 Архитектура веб-приложений. Типовые уязвимости веб-приложений. Сценарии использования. Действия злоумышленника после получения доступа (закрепление, распространение)	3			10	2
5 Сетевой уровень. Цели, практика аудита. Статический анализ кода. Локальные уязвимости систем.	3			10	2
6 Проектирование защищенного Web-приложения. Обеспечение конфиденциальности и целостности данных при работе с Web-приложением. Тестирование системы безопасности Web-приложения	2			10	2
7. Сбор информации о веб-приложении.			2		3
8. Тестирование защищенности транспортного уровня.			3		3
9. Тестирование защищенности механизма управления доступом.			3		3
10. Тестирование защищенности механизма управления сессиями.			3		3
11. Тестирование на устойчивость к атакам отказа в обслуживании.			3		3
12. Поиск уязвимостей к атакам CSRF.			3		4
13. Поиск уязвимостей к атакам XSS.			3		4
14. Поиск уязвимостей к атакам SQL-injection.			3		4
15. Поиск уязвимостей к атакам RCE.			3		4
16. Сканирование уязвимостей веб-приложений.			4		4
ИТОГО:	**15**		**30**	**45**	**45**

Перечень лабораторных занятий

1. Сбор информации о веб-приложении.
2. Тестирование защищенности транспортного уровня.
3. Тестирование защищенности механизма управления доступом.
4. Тестирование защищенности механизма управления сессиями.
5. Тестирование на устойчивость к атакам отказа в обслуживании.
6. Поиск уязвимостей к атакам CSRF.
7. Поиск уязвимостей к атакам XSS.
8. Поиск уязвимостей к атакам SQL-injection.
9. Поиск уязвимостей к атакам RCE.
10. Сканирование уязвимостей веб-приложений.

Тематический план самостоятельной работы студента с преподавателем

Наименование темы СРСП	Цель занятия	Форма проведения занятия	Содержание задания	Рекомендуемая литература
1 Введение в безопасность Web-приложений	Получение практических навыков	Выполнение индивидуальных заданий	Изучить классификацию основных типов атак на web-приложения	[1,2]
2 Уязвимости веб-приложений.	Получение практических навыков	Выполнение индивидуальных заданий	Подготовка к аудиту безопасности WEB-приложений	[1, 2]
3 Уязвимости клиентской части.	Получение практических навыков	Выполнение индивидуальных заданий	Предложить сценарий атаки, на клиентской стороне веб-приложения.	[1, 2, 3]
4 Архитектура веб-приложений.	Получение практических навыков	Выполнение индивидуальных заданий	Описание векторов атаки и оценка рисков.	[3,4]
5 Сетевой уровень.	Получение практических навыков	Выполнение индивидуальных заданий	Подготовка тестов для проверки защищенности служб SSL/TLS	[1,2,5]
6 Проектирование защищенного Web-приложения.	Получение практических навыков	Выполнение индивидуальных заданий	Создание плана тестирования; реализация процедуры тестирования	[2,4,5,7]

Темы контрольных заданий для СРС

1. Атака «злоупотребление функциональностью». Привести примеры. Дать рекомендации по минимизации рисков возникновения данного типа атаки.
2. Атака «грубая сила». Привести примеры. Методы исключения атаки перебором на реальных web-приложениях.
3. Атака «межсайтовый скриптинг». Привести примеры. Способы защиты.
4. Атака «снятие отпечатков пальцев»: методы и утилиты. Меры, применяемые для минимизации успешности данного типа атаки.
5. Атака «переполнение буфера». Причина возникновения, примеры.
6. Атака «отказ в обслуживании». Классификация методов. Меры, применяемые для минимизации успешности данного типа атак.
7. Понятие LDAP-репозитория (Lightweight Directory Access Protocol), методы атак на LDAP. Примеры и способы исключения возможности данного типа атак.
8. Атака «навигация по запрещенным путям». Примеры и способы исключения возможности данного типа атаки.

9. Атака «SQL-инъекция». Примеры и способы исключения возможности данного типа атаки.

10. Атака «XML-инъекция». Примеры и способы исключения возможности данного типа атаки

Критерии оценки знаний студентов

Экзаменационная оценка по дисциплине определяется как сумма максимальных показателей успеваемости по рубежным контролям (60%) и итоговой аттестации (экзамен) (40%) и составляет значение 100% .

График выполнения и сдачи заданий по дисциплине

Вид контроля	**Цель и содержание задания**	**Рекомендуемая литература**	**Продолжительность выполнения**	**Форма контроля**	**Срок сдачи**	**Баллы**
Посещаемость лекций и СРСП	Усвоение материала по темам лекций	Конспект лекций и основная литература	15 контактных часов	Текущий	На каждой лекции	15
Сдача лабораторных работ №№ 1-10	Усвоение материала по дисциплине	МУ к выполнению лабораторных работ	30 контактных часов	Текущий	2, 4, 6,7, 9,10,11, 12,13,15 недели	30
Задания к темам СРСП	Получение практических навыков	Согласно тематики СРСП	45 контактных часов	Текущий	Еженедельно	5
Теоретический модуль	Проверка усвоения материала дисциплины	Конспект лекций	4 контактных часа	Рубежный	7,14 неделя	10
Экзамен	Проверка усвоения материала дисциплины	Весь перечень основной и дополнительной литературы	2 контактных часа	Итоговый	В период сессии	40
Итого						100

Политика и процедуры

При изучении дисциплины «Спец.дисциплина II» прошу соблюдать следующие правила:

1 Не опаздывать на занятия.

2 Не пропускать занятия без уважительной причины, в случае болезни прошу представить справку, в других случаях – объяснительную записку.

3 В обязанности студента входит посещение всех видов занятий.

4 Согласно календарному графику учебного процесса сдавать все виды контроля.

5 Пропущенные практические и лабораторные занятия отрабатывать в указанное преподавателем время.

Список основной литературы

1. ИБ открытых систем: Учебник для ВУЗов. В 2-х томах. Том 1 – Угрозы уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская. А.И. Толстой, Д.В. Ушаков. – М.:Горячия линия – Телеком, 2006.

2. Прохода А. Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. -М.: Горячая линия-Телеком, 2007. - 180 с.

3 Лукацкий А. В. Обнаружение атак. СПб.: БХВ-Петербург, 2001. 624 с.

4 Мамаев М., Петренко С. Технология защиты в Интернете. Специальный справочник. СПб.:Питер, 2002. 848 с.

5. Касперски К. Техника сетевых атак. М.: Солон-Р, 2001. 396 с.

Список дополнительной литературы

6 Форристал Д. и др. Защита от хакеров Web-приложений / Джефф Форристал, Крис Брумс, Дрю Симонис, Брайн Бегнолл, Майкл Дайновиц, Джей Д. Дайсон, Джо Дьюлэй, Майкл Кросс, Эдгар Даниелян, Дэвид Г. Скабру ; Пер. с англ. В. Зорина –М. : Компания АйТи ; ДМК Пресс.,2008 – 496 с

7 Мак-Клар С, Скембрей Д., Курц Д. Секреты хакеров. Безопасность сетей - готовые решения.2-е изд.: Пер. с англ. М.: Изд. дом «Вильямс», 2001. 656 с.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

по дисциплине **SD(II) 4312** «Спец.дисциплина II»

модуль **SD 29** Спец.дисциплины

Гос.изд.лиц. № 50 от 31.03.2004.
Подписано к печати _____2015г. Формат 60×90 /16 Тираж ____ экз.
Объем _____ уч. изд. л. Заказ № _____ Цена договорная

100027. Издательство КарГТУ, Караганда, Бульвар Мира, 56