МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное
бюджетное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

_____

«___»_____ 2024г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	Информационная безопасность WEB-приложений
направление подготовки:	09.03.01 Информатика и вычислительная техника
направленность (профиль):	Информационная безопасность компьютерных систем и сетей
форма обучения:	Очная

Рабочая программа рассмотрена на заседании кафедры математики и прикладных информационных технологий

Протокол №____от_____2024г.

1. Цели и задачи освоения дисциплины

Цель освоения дисциплины:

- Освоение теоретических знаний и практических навыков по обеспечению информационной безопасности WEB -приложений.

Задачи освоения дисциплины:

- Изучение нормативно-правовых и организационных основ обеспечения информационной безопасности WEB -приложений.
- Изучение методов и процедур:

- выявления угроз безопасности;
- оценки степени их опасности.

- Освоение принципов построения защищённых WEB-сайтов.
- Приобретение навыков настройки и эксплуатации средств защиты WEB - приложений.
- Практическая отработка методов и порядка проведения работ по обеспечению информационной безопасности WEB -приложений.
- Развитие исследовательских и аналитических навыков, а также интеллектуального потенциала.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части учебного плана, формируемой участниками образовательных отношений.

Необходимые условия для освоения дисциплины:

1. Знание теоретических основ:
   - информационных технологий;
   - основ информационной безопасности, включая уязвимости и угрозы WEB - приложений.
2. Умение разрабатывать алгоритмы и реализовывать их с использованием языков программирования, применяемых при создании WEB -приложений (например, Python, JavaScript, PHP).
3. Владение навыками работы с WEB -технологиями (HTML, CSS, базы данных, протоколы HTTP/HTTPS).

Применимость дисциплины:

Содержание курса может служить основой для:

- прохождения учебной и производственной практик, связанных с разработкой и защитой WEB -приложений;
- подготовки к выполнению выпускной квалификационной работы на тему информационной безопасности;
- дальнейшей профессиональной деятельности в области защиты WEB - приложений.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикаторов достижения компетенций (ИДК)	Код и наименование результата обучения по дисциплине
ПКС-1. Способен обеспечивать информационную	ПКС-1.1. Управляет информационной безопасностью;	Знать (З1) теоретические основы управления информационной безопасностью WEB-приложений, современные методы

безопасность компьютерных систем и сетей.	администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	предотвращения угроз, связанных с WEB - средой (SQL-инъекции, XSS, CSRF и др.).
		Уметь (У1) планировать восстановление работы WEB -приложений и их инфраструктуры после сбоев или атак, документировать уязвимости и ошибки в компонентах WEB -приложений.
		Владеть (В1) практическими навыками администрирования конфигурации и управления безопасностью серверов и WEB – приложений, навыками обеспечения безопасности баз данных и предотвращения утечек данных, методами предотвращения потерь и повреждений данных при инцидентах.
ПКС-2. Способен осуществлять техническое обслуживание и администрирование средств защиты информации и процесса управления безопасностью сетевых устройств и программного обеспечения в компьютерных системах и сетях.	ПКС-2. 1. Осуществляет администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения.	Знать (З2) теоретические основы администрирования и технического обслуживания средств защиты WEB – приложений, принципы работы программно-аппаратных средств обеспечения информационной безопасности в WEB –среде, стандарты и методы защиты WEB - приложений, серверов и баз данных.
		Уметь (У2) планировать и организовывать мероприятия по техническому обслуживанию средств защиты информации для WEB - приложений и серверов, настраивать программное и аппаратное обеспечение для защиты WEB -приложений от атак (например, WAF, IDS/IPS, брандмауэры).
		Владеть (В2) практическими навыками внедрения, настройки, администрирования и технического обслуживания средств защиты информации для WEB –приложений, навыками мониторинга и анализа работы систем защиты (например, через журналы событий, аналитические панели), методами оперативного реагирования на инциденты безопасности в WEB -приложениях.
ПКС-3. Способен проводить оценку уровня безопасности компьютерных систем и сетей, а также проводить тестирование программного обеспечения на защищенность.	ПКС-3.1. Оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Знать (З3) теоретические основы проведения аудита безопасности WEB -приложений и серверного программного обеспечения, типы уязвимостей WEB -приложений (например, SQL-инъекции, XSS, CSRF, уязвимости авторизации и аутентификации), методологии и стандарты тестирования на защищенность
		Уметь (У3) планировать и организовывать мероприятия по аудиту безопасности WEB – приложений, разрабатывать тестовые сценарии для проверки защищённости программного обеспечения WEB – приложений, проводить анализ результатов тестирования для выявления и устранения уязвимостей.
		Владеть (В3) практическими навыками оценки уровня безопасности WEB -приложений и серверной инфраструктуры, навыками проведения тестирования на уязвимости с использованием специализированных инструментов, методами документирования результатов аудита и предоставления рекомендаций по улучшению защищённости.

4. **Объем дисциплины**

Общий объем дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	8	12	-	22	47	27	Экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины.

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Контроль, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.					
1	1	Введение в безопасность веб-приложений и нормативно-правовая база	2	-	2	7	-	11	ПКС-1.1 ПКС-2.1 ПКС-3.1	Задания на лабораторную работу
2	2	Аутентификация, авторизация и защита данных	2	-	5	7	-	14		
3	3	Защита от атак и мониторинг безопасности	3	-	7	11	-	21		
4	4	Безопасность API и облачные технологии	2	-	5	9	-	16		
5	5	Практическое применение и защитные технологии	3	-	3	13	-	19		
6	Экзамен		-	-	-	-	27	27	ПКС-1.1 ПКС-2.1 ПКС-3.1	Вопросы к экзамену
Итого:			12	-	22	47	27	108	X	X

заочная форма обучения (ЗФО): не реализуется
очно-заочная форма обучения (ОЗФО): не реализуется

5.2. Содержание дисциплины.
5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. Введение в безопасность веб-приложений и нормативно-правовая база

Основы информационной безопасности веб-приложений
- Основные угрозы и уязвимости веб-приложений
- Типы атак на веб-приложения (SQL-инъекции, XSS, CSRF и другие)
- Модели безопасности веб-приложений (CIA, PAM, и другие)

Нормативно-правовые акты и стандарты безопасности веб-приложений
- Международные и национальные стандарты безопасности
- Лицензирование и сертификация в сфере информационной безопасности
- Аудит и аттестация веб-приложений по требованиям безопасности

Правовые и организационные основы информационной безопасности в веб-разработке
- Правовые аспекты безопасности веб-приложений
- Права и обязанности разработчиков и администраторов
- Влияние законодательных изменений на безопасность веб-приложений

Раздел 2. Аутентификация, авторизация и защита данных

Технологии аутентификации и авторизации в веб-приложениях
- Принципы аутентификации
- Методы авторизации (RBAC, ABAC)
- Проблемы безопасности в аутентификации и авторизации

Шифрование и защита данных в веб-приложениях
- Протоколы безопасности для защиты данных (SSL/TLS, HTTPS)
- Шифрование на уровне базы данных и при передаче данных
- Хеширование паролей и защита учетных данных

Обеспечение безопасности сессий и данных в веб-приложениях
- Устранение уязвимостей в сессиях
- Защита конфиденциальных данных
- Обеспечение устойчивости к атакам на сессии

Раздел 3. Защита от атак и мониторинг безопасности

Защита от атак на веб-приложения
- Применение WAF (Web Application Firewalls) и прокси-серверов
- Защита от SQL-инъекций, XSS, CSRF и других атак
- Инструменты для защиты от уязвимостей в веб-приложениях

Мониторинг, аудит и тестирование безопасности веб-приложений
- Роль мониторинга в обеспечении безопасности
- Аудит безопасности веб-приложений и анализ уязвимостей
- Инструменты для тестирования веб-приложений (OWASP ZAP, Burp Suite)

Защита от DDoS-атак и безопасность на уровне сети
- Влияние DDoS-атак на веб-приложения
- Защита от DDoS-атак с использованием различных технологий
- Сетевые механизмы защиты веб-приложений

Раздел 4. Безопасность API и облачные технологии

Безопасность API в веб-приложениях
- Принципы безопасности для RESTful и SOAP API
- Аутентификация и авторизация в API
- Защита от атак на API (например, избыточный доступ, атаки на аутентификацию)

Облачная безопасность для веб-приложений
- Основы безопасности облачных сервисов и инфраструктуры
- Защита данных в облаке и безопасность облачных веб-приложений

- Проблемы безопасности и решения при использовании облачных платформ (AWS, Google Cloud, Azure)

Раздел 5. Практическое применение и защитные технологии

Практическое применение технологий защиты веб-приложений

- Кейсы реальных атак и их анализ
- Рекомендации по безопасности для разработчиков веб-приложений
- Советы по внедрению безопасности на разных этапах разработки

Использование инструментов безопасности для тестирования веб-приложений

- Обзор и применение инструментов для тестирования безопасности (например, Metasploit, Nessus)
- Статический и динамический анализ безопасности кода
- Разработка и внедрение политики безопасности для веб-приложений

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1	1	2	-	-	Введение в безопасность веб-приложений и нормативно-правовая база
2	2	2	-	-	Аутентификация, авторизация и защита данных
3	3	3	-	-	Защита от атак и мониторинг безопасности
4	4	2	-	-	Безопасность API и облачные технологии
5	5	3	-	-	Практическое применение и защитные технологии
Итого:		12	-	-	-

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема практического занятия
		ОФО	ЗФО	ОЗФО	
1	1	2	-	-	Введение в безопасность веб-приложений и нормативно-правовая база
2	2	5	-	-	Аутентификация, авторизация и защита данных
3	3	7	-	-	Защита от атак и мониторинг безопасности
4	4	5	-	-	Безопасность API и облачные технологии
5	5	3	-	-	Практическое применение и защитные технологии
Итого:		22	-	-	-

Практические занятия

Практические занятия учебным планом не предусмотрены.

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	7	-	-	Введение в безопасность веб-приложений и нормативно-правовая база	Подготовка к лабораторным работам
2	2	7	-	-	Аутентификация, авторизация и защита данных	Подготовка к лабораторным работам

3	3	11	-	-	Защита от атак и мониторинг безопасности	Подготовка к лабораторным работам
4	4	9	-	-	Безопасность API и облачные технологии	Подготовка к лабораторным работам
5	5	13	-	-	Практическое применение и защитные технологии	Подготовка к лабораторным работам
6	1-5	27	-	-	Экзамен	Подготовка к экзамену
Итого:		74	-	-		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- информационно-телекоммуникационная (лекционные занятия, практические занятия)
- групповая (практические занятия)
- индивидуальная (практические занятия)
- рейтинговая (практические занятия)

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены.

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Лабораторная работа № 1	0-15
2	Лабораторная работа № 2	0-15
	ИТОГО за первую текущую аттестацию	0-30
2 текущая аттестация		
3	Лабораторная работа № 3	0-15
4	Лабораторная работа № 4	0-15
	ИТОГО за вторую текущую аттестацию	0-30
3 текущая аттестация		
5	Лабораторная работа № 5	0-40
	ИТОГО за третью текущую аттестацию	0-40
	ВСЕГО	0-100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

- Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/;

- Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/;
- Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru;
- Электронно-библиотечная система «ЛАНЬ» https://e.lanbook.com;
- Образовательная платформа ЮРАЙТ www.urait.ru;
- Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru;
- Библиотеки нефтяных вузов России:
    - Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/;
    - Электронная библиотека Уфимского государственного нефтяного технического университета http://bibl.rusoil.net/;
    - Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books.

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;
- Nmap;
- Snort;
- Wireshark;
- КриптоПро;
- OpenVPN.

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно – наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1.	Информационная безопасность WEB-приложений	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблок - 1 шт., проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70.
		Лабораторные занятия:	625039, г. Тюмень, ул. Мельникайте, д. 70

		Учебная аудитория для проведения (лабораторных занятий); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблоки, проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим, лабораторным занятиям.

Практические занятия способствуют углублённому изучению дисциплины и служат основной формой подведения итогов самостоятельной работы студентов. Цель практических занятий заключается в углублении и закреплении теоретических знаний, а также в формировании практических компетенций, необходимых будущим специалистам.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику будущих функциональных обязанностей обучающихся, в том числе предусматривать задания с проведением деловых игр (эпизодов).

Студенту рекомендуется следующая схема подготовки к занятию:

- проработать конспект лекций;
- изучить рекомендованную литературу;
- при затруднениях сформулировать вопросы к преподавателю;
- после выполнения практического задания оформить отчет и подготовиться к защите.

Важной формой самостоятельной работы студента является систематическая и планомерная подготовка к лабораторному занятию. После лекции студент должен познакомиться с планом лабораторных занятий и списком обязательной и дополнительной литературы, которую необходимо прочитать, изучить и законспектировать. Разъяснение по вопросам новой темы студенты получают у преподавателя в конце предыдущего лабораторного занятия.

Подготовка к лабораторному занятию требует, прежде всего, чтения рекомендуемых источников. Важным этапом в самостоятельной работе студента является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки – работа с теоретическими источниками. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на практическом занятии.

В начале лабораторного занятия должен присутствовать организационный момент и вступительная часть. Преподаватель произносит краткую вступительную речь, где формулируются основные вопросы и проблемы, способы их решения в процессе работы.

В конце каждой темы подводятся итоги, предлагаются темы докладов, выносятся вопросы для самоподготовки.

Лабораторные занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать теоретические знания, подготовиться к научно-исследовательской деятельности. В процессе работы на лабораторных занятиях обучающийся должен совершенствовать умения и навыки самостоятельного анализа источников и научной литературы, что необходимо для научно-исследовательской работы.

Усвоенный материал необходимо научиться применять при решении проставленных задач.

Успешному осуществлению внеаудиторной самостоятельной работы способствует проведение коллоквиумов. Они обеспечивают непосредственную связь между студентом и преподавателем (по ним преподаватель судит о трудностях, возникающих у студентов в ходе учебного процесса, о степени усвоения предмета, о помощи, какую надо указать, чтобы устранить пробелы в знаниях); они используются для осуществления контрольных функций.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Затраты времени на выполнение этой работы регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, подготовка мультимедиа-сообщений/докладов, подготовка реферата, тестирование, решение заданий по образцу, решение вариативных задач, выполнение чертежей, схем, расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Работа на лекции – это сложный процесс, который включает в себя такие элементы как слушание, осмысление и, собственно, конспектирование. Для того, чтобы лекция выполнила свое назначение, важно подготовиться к ней и ее записи еще до прихода преподавателя в аудиторию, поскольку в первые минуты лекции объявляется тема лекции, формулируется ее основная цель. Без этого дальнейшее восприятие лекции становится сложным. Важно научиться слушать преподавателя во время лекции. Здесь не следует путать такие понятия как слышать и слушать. Слушание лекции состоит из нескольких этапов, начиная от слышания (первый шаг в процессе осмысленного слушания) и заканчивая оценкой сказанного.

Чтобы процесс слушания стал более эффективным, нужно разделять качество общения с лектором, научиться поддерживать непрерывное внимание к выступающему. Для оптимизации процесса слушания следует:

1. научиться выделять основные положения. Нельзя понять и запомнить все, что говорит выступающий, однако можно выделить основные моменты. Для этого необходимо обращать внимание на вводные слова, словосочетания, фразы, которые используются, как правило, для перехода к новым положениям, выводам и обобщениям;

2. во время лекции осуществлять поэтапный анализ и обобщение, услышанного. Необходимо постоянно анализировать и обобщать положения, раскрываемые в речи говорящего. Стараясь представить материал обобщенно, мы готовим надежную базу для

экономной, свернутой его записи. Делать это лучше всего по этапам, ориентируясь на момент логического завершения одного вопроса (подвопроса, тезиса и т.д.) и перехода к другому;

3. готовность слушать выступление лектора до конца.

Слушание является лишь одним из элементов хорошего усвоения лекционного материала.

Поток информации, который сообщается во время лекции необходимо фиксировать, записывать – научиться вести конспект лекции, где формулировались бы наиболее важные моменты, основные положения, излагаемые лектором. Для ведения конспекта лекции следует использовать тетрадь. Ведение конспекта на листочках не рекомендуется, поскольку они не так удобны в использовании и часто теряются. При оформлении конспекта лекции необходимо оставлять поля, где студент может записать свои собственные мысли, возникающие параллельно с мыслями, высказанными лектором, а также вопросы, которые могут возникнуть в процессе слушания, чтобы получить на них ответы при самостоятельной проработке материала лекции, при изучении рекомендованной литературы или непосредственно у преподавателя в конце лекции.

Составляя конспект лекции, следует оставлять значительный интервал между строчками. Это связано с тем, что иногда возникает необходимость вписать в первоначальный текст лекции одну или несколько строчек, имеющих принципиальное значение и почерпнутых из других источников. Расстояние между строками необходимо также для подчеркивания слов или целых групп слов (такое подчеркивание вызывается необходимостью привлечь внимание к данному месту в тексте при повторном чтении). Обычно подчеркивают определения, выводы.

Главным отличием конспекта лекции от текста является свертывание текста. При ведении конспекта удаляются отдельные слова или части текста, которые не выражают значимую информацию, а развернутые обороты речи заменяют более лаконичными или же синонимичными словосочетаниями. При конспектировании основную информацию следует записывать подробно, а дополнительные и вспомогательные сведения, примеры – очень кратко. Особенно важные моменты лекции, на которые следует обратить особое внимание лектор, как правило, читает в замедленном темпе, что позволяет сделать их запись дословной. Также важно полностью без всяких изменений вносить в тетрадь схемы, таблицы, чертежи и т.п., если они предполагаются в лекции. Для того, чтобы совместить механическую запись с почти дословным фиксированием наиболее важных положений, можно использовать системы условных сокращений. В первую очередь сокращаются длинные слова и те, что повторяются в речи лектора чаще всего. При этом само сокращение должно быть по возможности кратким.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Информационная безопасность WEB-приложений
Код, направление подготовки: 09.03.01 Информатика и вычислительная техника
Направленность (профиль): Информационная безопасность компьютерных систем и сетей

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-1. Способен обеспечивать информационную безопасность компьютерных систем и сетей.	ПКС-1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Знать (З1) теоретические основы управления информационной безопасностью WEB-приложений, современные методы предотвращения угроз, связанных с WEB -средой (SQL-инъекции, XSS, CSRF и др.).	Не знает теоретические основы управления информационной безопасностью WEB-приложений, современные методы предотвращения угроз, связанных с WEB -средой (SQL-инъекции, XSS, CSRF и др.).	Знает на низком уровне теоретические основы управления информационной безопасностью WEB-приложений, современные методы предотвращения угроз, связанных с WEB -средой (SQL-инъекции, XSS, CSRF и др.).	Знает на среднем уровне теоретические основы управления информационной безопасностью WEB-приложений, современные методы предотвращения угроз, связанных с WEB -средой (SQL-инъекции, XSS, CSRF и др.).	Знает на высоком уровне теоретические основы управления информационной безопасностью WEB-приложений, современные методы предотвращения угроз, связанных с WEB -средой (SQL-инъекции, XSS, CSRF и др.).
		Уметь (У1) планировать восстановление работы WEB - приложений и их инфраструктуры после сбоев или атак, документировать уязвимости и ошибки в компонентах WEB - приложений.	Не умеет планировать восстановление работы WEB - приложений и их инфраструктуры после сбоев или атак, документировать уязвимости и ошибки в компонентах WEB - приложений.	Умеет на низком уровне планировать восстановление работы WEB - приложений и их инфраструктуры после сбоев или атак, документировать уязвимости и ошибки в компонентах WEB - приложений.	Умеет на среднем уровне планировать восстановление работы WEB - приложений и их инфраструктуры после сбоев или атак, документировать уязвимости и ошибки в компонентах WEB - приложений.	Умеет на высоком уровне планировать восстановление работы WEB - приложений и их инфраструктуры после сбоев или атак, документировать уязвимости и ошибки в компонентах WEB - приложений.

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Владеть (В1) практическими навыками администрирования конфигурации и управления безопасностью серверов и WEB – приложений, навыками обеспечения безопасности баз данных и предотвращения утечек данных, методами предотвращения потерь и повреждений данных при инцидентах.	Не владеет практическими навыками администрирования конфигурации и управления безопасностью серверов и WEB – приложений, навыками обеспечения безопасности баз данных и предотвращения утечек данных, методами предотвращения потерь и повреждений данных при инцидентах.	Владеет на низком уровне практическими навыками администрирования конфигурации и управления безопасностью серверов и WEB – приложений, навыками обеспечения безопасности баз данных и предотвращения утечек данных, методами предотвращения потерь и повреждений данных при инцидентах.	Владеет на среднем уровне практическими навыками администрирования конфигурации и управления безопасностью серверов и WEB – приложений, навыками обеспечения безопасности баз данных и предотвращения утечек данных, методами предотвращения потерь и повреждений данных при инцидентах.	Владеет на высоком уровне практическими навыками администрирования конфигурации и управления безопасностью серверов и WEB – приложений, навыками обеспечения безопасности баз данных и предотвращения утечек данных, методами предотвращения потерь и повреждений данных при инцидентах.
ПКС-2. Способен осуществлять техническое обслуживание и администрирование средств защиты информации и процесса управления безопасностью сетевых устройств и программного обеспечения в компьютерных системах и сетях.	ПКС-2. 1. Осуществляет администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения.	Знать (З2) теоретические основы администрирования и технического обслуживания средств защиты WEB –приложений, принципы работы программно-аппаратных средств обеспечения информационной безопасности в WEB – среде, стандарты и методы защиты WEB -приложений, серверов и баз данных.	Не знает теоретические основы администрирования и технического обслуживания средств защиты WEB –приложений, принципы работы программно-аппаратных средств обеспечения информационной безопасности в WEB – среде, стандарты и методы защиты WEB -приложений, серверов и баз данных.	Знает на низком уровне теоретические основы администрирования и технического обслуживания средств защиты WEB –приложений, принципы работы программно-аппаратных средств обеспечения информационной безопасности в WEB – среде, стандарты и методы защиты WEB -приложений, серверов и баз данных.	Знает на среднем уровне теоретические основы администрирования и технического обслуживания средств защиты WEB –приложений, принципы работы программно-аппаратных средств обеспечения информационной безопасности в WEB – среде, стандарты и методы защиты WEB -приложений, серверов и баз данных.	Знает на высоком уровне теоретические основы администрирования и технического обслуживания средств защиты WEB –приложений, принципы работы программно-аппаратных средств обеспечения информационной безопасности в WEB – среде, стандарты и методы защиты WEB -приложений, серверов и баз данных.

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Уметь (У2) планировать и организовывать мероприятия по техническому обслуживанию средств защиты информации для WEB - приложений и серверов, настраивать программное и аппаратное обеспечение для защиты WEB - приложений от атак (например, WAF, IDS/IPS, брандмауэры).	Не умеет планировать и организовывать мероприятия по техническому обслуживанию средств защиты информации для WEB - приложений и серверов, настраивать программное и аппаратное обеспечение для защиты WEB - приложений от атак (например, WAF, IDS/IPS, брандмауэры).	Умеет на низком уровне планировать и организовывать мероприятия по техническому обслуживанию средств защиты информации для WEB - приложений и серверов, настраивать программное и аппаратное обеспечение для защиты WEB - приложений от атак (например, WAF, IDS/IPS, брандмауэры).	Умеет на среднем уровне планировать и организовывать мероприятия по техническому обслуживанию средств защиты информации для WEB - приложений и серверов, настраивать программное и аппаратное обеспечение для защиты WEB - приложений от атак (например, WAF, IDS/IPS, брандмауэры).	Умеет на высоком уровне планировать и организовывать мероприятия по техническому обслуживанию средств защиты информации для WEB - приложений и серверов, настраивать программное и аппаратное обеспечение для защиты WEB - приложений от атак (например, WAF, IDS/IPS, брандмауэры).

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Владеть (В2) практическими навыками внедрения, настройки, администрирования и технического обслуживания средств защиты информации для WEB – приложений, навыками мониторинга и анализа работы систем защиты (например, через журналы событий, аналитические панели), методами оперативного реагирования на инциденты безопасности в WEB - приложениях.	Не владеет практическими навыками внедрения, настройки, администрирования и технического обслуживания средств защиты информации для WEB – приложений, навыками мониторинга и анализа работы систем защиты (например, через журналы событий, аналитические панели), методами оперативного реагирования на инциденты безопасности в WEB - приложениях.	Владеет на низком уровне практическими навыками внедрения, настройки, администрирования и технического обслуживания средств защиты информации для WEB – приложений, навыками мониторинга и анализа работы систем защиты (например, через журналы событий, аналитические панели), методами оперативного реагирования на инциденты безопасности в WEB - приложениях.	Владеет на среднем уровне практическими навыками внедрения, настройки, администрирования и технического обслуживания средств защиты информации для WEB – приложений, навыками мониторинга и анализа работы систем защиты (например, через журналы событий, аналитические панели), методами оперативного реагирования на инциденты безопасности в WEB - приложениях.	Владеет на высоком уровне практическими навыками внедрения, настройки, администрирования и технического обслуживания средств защиты информации для WEB – приложений, навыками мониторинга и анализа работы систем защиты (например, через журналы событий, аналитические панели), методами оперативного реагирования на инциденты безопасности в WEB - приложениях.

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-3. Способен проводить оценку уровня безопасности компьютерных систем и сетей, а также проводить тестирование программного обеспечения на защищенность.	ПКС-3.1. Оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Знать (З3) теоретические основы проведения аудита безопасности WEB - приложений и серверного программного обеспечения, типы уязвимостей WEB - приложений (например, SQL-инъекции, XSS, CSRF, уязвимости авторизации и аутентификации), методологии и стандарты тестирования на защищенность	Не знает теоретические основы проведения аудита безопасности WEB - приложений и серверного программного обеспечения, типы уязвимостей WEB - приложений (например, SQL-инъекции, XSS, CSRF, уязвимости авторизации и аутентификации), методологии и стандарты тестирования на защищенность	Знает на низком уровне теоретические основы проведения аудита безопасности WEB - приложений и серверного программного обеспечения, типы уязвимостей WEB - приложений (например, SQL-инъекции, XSS, CSRF, уязвимости авторизации и аутентификации), методологии и стандарты тестирования на защищенность	Знает на среднем уровне теоретические основы проведения аудита безопасности WEB - приложений и серверного программного обеспечения, типы уязвимостей WEB - приложений (например, SQL-инъекции, XSS, CSRF, уязвимости авторизации и аутентификации), методологии и стандарты тестирования на защищенность	Знает на высоком уровне теоретические основы проведения аудита безопасности WEB - приложений и серверного программного обеспечения, типы уязвимостей WEB - приложений (например, SQL-инъекции, XSS, CSRF, уязвимости авторизации и аутентификации), методологии и стандарты тестирования на защищенность

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Уметь (У3) планировать и организовывать мероприятия по аудиту безопасности WEB – приложений, разрабатывать тестовые сценарии для проверки защищённости программного обеспечения WEB – приложений, проводить анализ результатов тестирования для выявления и устранения уязвимостей.	Не умеет планировать и организовывать мероприятия по аудиту безопасности WEB – приложений, разрабатывать тестовые сценарии для проверки защищённости программного обеспечения WEB – приложений, проводить анализ результатов тестирования для выявления и устранения уязвимостей.	Умеет на низком уровне планировать и организовывать мероприятия по аудиту безопасности WEB – приложений, разрабатывать тестовые сценарии для проверки защищённости программного обеспечения WEB – приложений, проводить анализ результатов тестирования для выявления и устранения уязвимостей.	Умеет на среднем уровне планировать и организовывать мероприятия по аудиту безопасности WEB – приложений, разрабатывать тестовые сценарии для проверки защищённости программного обеспечения WEB – приложений, проводить анализ результатов тестирования для выявления и устранения уязвимостей.	Умеет на высоком уровне планировать и организовывать мероприятия по аудиту безопасности WEB – приложений, разрабатывать тестовые сценарии для проверки защищённости программного обеспечения WEB – приложений, проводить анализ результатов тестирования для выявления и устранения уязвимостей.

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Владеть (ВЗ) практическими навыками оценки уровня безопасности WEB - приложений и серверной инфраструктуры, навыками проведения тестирования на уязвимости с использованием специализированных инструментов, методами документирования результатов аудита и предоставления рекомендаций по улучшению защищённости.	Не владеет практическими навыками оценки уровня безопасности WEB - приложений и серверной инфраструктуры, навыками проведения тестирования на уязвимости с использованием специализированных инструментов, методами документирования результатов аудита и предоставления рекомендаций по улучшению защищённости.	Владеет на низком уровне практическими навыками оценки уровня безопасности WEB - приложений и серверной инфраструктуры, навыками проведения тестирования на уязвимости с использованием специализированных инструментов, методами документирования результатов аудита и предоставления рекомендаций по улучшению защищённости.	Владеет на среднем уровне практическими навыками оценки уровня безопасности WEB - приложений и серверной инфраструктуры, навыками проведения тестирования на уязвимости с использованием специализированных инструментов, методами документирования результатов аудита и предоставления рекомендаций по улучшению защищённости.	Владеет на высоком уровне практическими навыками оценки уровня безопасности WEB - приложений и серверной инфраструктуры, навыками проведения тестирования на уязвимости с использованием специализированных инструментов, методами документирования результатов аудита и предоставления рекомендаций по улучшению защищённости.

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: Информационная безопасность WEB-приложений
Код, направление подготовки: 09.03.01 Информатика и вычислительная техника
Направленность (профиль): Информационная безопасность компьютерных систем и сетей

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/449285	ЭР*	30	100	+
2	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739	ЭР*	30	100	+

ЭР* – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/