Учреждение образования «Полоцкий государственный университет»

УТВЕРЖДАЮ
Проректор по учебной работе
учреждения образования
«Полоцкий государственный
университет»

_____ Ю.П. Голубев
«__16__» _____ 2021 г.
Регистрационный №УД-213/21/уч

ТЕХНОЛОГИИ РАЗРАБОТКИ И ЗАЩИТЫ СЕРВЕРНЫХ ВЕБ-ПРИЛОЖЕНИЙ И ВЕБ-СЛУЖБ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
1-98 01 01 Компьютерная безопасность
(по направлениям)
направление специальности
1-98 01 01-01 Компьютерная безопасность
(математические методы и программные системы)

2021 г.

Учебная программа составлена в соответствии с требованиями образовательного стандарта высшего образования Министерства образования Республики Беларусь по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» ОСВО 1-98 01 01-2013 и учебного плана специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)». Регистрационный №13-13/уч. ФИТ от 29.08.2013 г. для дневной очной формы получения высшего образования.

СОСТАВИТЕЛЬ:
Ирина Брониславовна Бураченок, к.т.н., доцент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет»
(протокол № 9 от «20» 09 2021 г.).

Методической комиссией факультета компьютерных наук и электроники учреждения образования «Полоцкий государственный университет»
(протокол № 4 от «14» 12 2021 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Технологии разработки и защиты серверных веб-приложений и веб-служб» знакомит студентов с фундаментальными понятиями, с концепцией, принципами проектирования веб-приложений, удовлетворяющих требованиям безопасности и надежности, технологиям разработки и применения веб-сервисов. Изучение технологии разработки и защиты серверных веб-приложений и веб-служб позволит по-новому взглянуть на архитектуру приложений и применять передовой опыт обеспечения безопасности при их разработке. Знания, полученные студентами при изучении данной дисциплины, позволят не только защитить веб-приложение от хакеров, но и выбрать тактику поиска уязвимостей и взлома, а также искать уязвимости новых типов, разрабатывать способы взлома систем, которые никогда не использовались ранее, и защищать самые сложные системы от самых настойчивых злоумышленников.

Изучение данной дисциплины является необходимым этапом в профессиональном развитии «специалиста по защите информации, математика».

Целью изучения дисциплины «Технологии разработки и защиты серверных веб-приложений и веб-служб» является формирование у студентов базовых знаний и практических навыков в области разработки веб-приложений, удовлетворяющих требованиям безопасности и надежности.

Задачи изучения дисциплины «Технологии разработки и защиты серверных веб-приложений и веб-служб». При изучении данной дисциплины требуется разрешить основные задачи:

– изучение понятийного аппарата дисциплины, основных теоретических положений;

– изучение вопросов безопасности веб-приложений, методов и средств их защиты при разработке от наиболее распространенных и опасных типов атак, используемых в настоящее время;

– овладение инструментальными средствами разработки безопасных веб-приложений;

– изучение языков записи алгоритмов, позволяющих строить защиту веб-приложений на разных уровнях разработки;

– формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач;

– знакомство как минимум с одной популярной базой данных (MySQL, PostgreSQL, Microsoft SQL Server, Oracle, MongoDB и т. п.).

В результате изучения дисциплины «Технологии разработки и защиты серверных веб-приложений и веб-служб» обучаемый должен:

знать:

– отечественные и зарубежные стандарты информационной безопасности;

– источники уязвимости веб-приложений;

– инструментальные средства разработки безопасных веб-приложений;

– подходы к проведению тестирования информационной безопасности веб-приложения;

– способ описания сервисов с помощью языка описания веб-сервисов WSDL;

– основы коммуникационных протоколов SOAP и JSON;

уметь:

– формировать функциональные требования к средствам защиты веб-приложения от внутренних и внешних угроз;

– разрабатывать веб-приложения, удовлетворяющее требованиям безопасности и надежности;

– писать программы с базовыми функциями CRUD (создание, чтение, обновление, удаление) хотя бы на одном языке;

– писать серверный код (BackEnd разработка веб-приложений Node.js, Java, Django, Python, Ruby и др.);

– писать код, который запускается в браузере (rontEnd, обычно JavaScript или фреймворки на основе JS: AngularJS, ReactJS, VueJS);

– понимать HTTP и уметь выполнить на нем или хотя бы прочесть запросы GET/POST через HTTP на каком-либо языке или платформе;

– читать и понимать приложения, которые используют как серверный, так и клиентский код, и обмениваться данными между ними через HTTP;

– выбирать средства для проведения ручного и автоматизированного тестирования уязвимостей веб-приложения;

– разрабатывать и применять средства защиты веб-приложений и используемых ими баз данных;

– определять направление угрозы и находить дыры в безопасности, а также воздействия, предназначенные для создания угрозы данным, прерывания выполнения или вмешательства в ход работы приложений.

владеть:

– инструментальными средствами разработки безопасных веб-приложений;

– навыками разработки структуры системы информационной защиты веб-приложений;

– основными средствами разработки веб-приложений, удовлетворяющих требованиям безопасности и надежности;

– навыками практического использования различных специальных средств тестирования уязвимостей веб-приложения;

– навыками администрирования операционных систем с элементами обеспечения безопасности информации на примере Windows;

– технологией разработки .asmx веб-сервисов, их описанием и использованием;

– унифицированной моделью программирования распределенных приложений на платформе Microsoft Windows – Communication Foundation (WCF);

– технологией ASP.NET Web API сборки REST-приложений на базе .NET Framework;

– технологией разработки приложений сервис-ориентированной архитектуры с использованием возможностей, предоставляемых программной платформой.

Требования к уровню освоения содержания учебной дисциплины. При изучении дисциплины «Технологии разработки и защиты серверных веб-приложений и веб-служб» у студентов специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «Специалист по защите информации. Математик» обеспечивающих выпускникам по указанной специальности успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

Академические компетенции.

АК-1 уметь применять базовые научно-теоретические знания для решения теоретических и практических задач;

АК-6 владеть междисциплинарным подходом при решении проблем;

Профессиональные компетенции.

Научно-исследовательская деятельность

ПК-1 работать с научной, нормативно-справочной и специальной литературой с целью получения последних сведений о новых методах защиты информации, о стойкости существующих систем защиты информации;

Инновационная деятельность

ПК-27. Разрабатывать новые информационные технологии на основе математического моделирования и оптимизации.

Сформированные компетенции являются базовыми при изучении всех последующих дисциплин, связанных с программированием, а также фундаментальной основой для дальнейшей профессиональной деятельности специалиста в области защиты информации.

Перечень дисциплин, в продолжение и на базе которых изучается дисциплина. Для изучения учебной дисциплины «Технологии разработки и защиты серверных веб-приложений и веб-служб» по специальности 1-98 01 01 «Компьютерная безопасность (по

направлениям)» необходимы знания, полученные при изучении базовых дисциплин: «Операционные системы», «Алгоритмы и структуры данных» государственного компонента и «Программирование», «Надежность программного обеспечения», «Теория кодирования, сжатия и восстановления информации» компонента учреждения высшего образования.

Перечень дисциплин, которые изучаются на базе дисциплины.

Знания полученные при изучении дисциплины «Технологии разработки и защиты серверных веб-приложений и веб-служб» по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» являются основой для дисциплин: «Модели данных и системы управления базами данных» государственного компонента, а также при изучении дисциплин компонента учреждения высшего образования дисциплины «Технологии разработки программного обеспечения», «Базы данных» и «Защита информации в операционных системах и компьютерных сетях».

Изучение учебной дисциплины позволяет дать студентам базу, необходимую для успешного усвоения материала перечисленных выше учебных дисциплин, а также получить знания, необходимые им в дальнейшем для успешной работы.

В соответствии с учебным планом по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» на изучение учебной дисциплины отводится:

Форма получения высшего образования первой ступени	дневная
Курс (курсы)	3
Семестр	6
Всего часов по дисциплине	106
Всего аудиторных часов по дисциплине	68
В том числе:	
Лекции, часов	34
Лабораторные занятия, часов	34
Самостоятельная работа, часов	38
Форма текущей аттестации	зачет
Трудоёмкость дисциплины, зач. ед	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале. Основные задачи, решаемые инженерами-программистами и разработчиками веб-приложений. Основные задачи, решаемые инженерами по безопасности, пентестерами и охотниками за багами.

Раздел 1 ВВЕДЕНИЕ В РАЗВЕДКУ ВЕБ-ПРИЛОЖЕНИЙ

Тема 1.1 История безопасности программного обеспечения.

Истоки хакерства. «Энигма» и автоматизированный взлом ее шифра (1940-е годы). Фрикинг и первые методы борьбы с фрикингом (1960-е годы). Начало компьютерного взлома (1980-е годы). Расцвет Всемирной паутины (2000-е годы). Современные хакеры (2020-е годы).

Тема 1.2 Структура современных веб-приложений.

Введение в World Wide Web. URI и URL. Доменные имена. Хостинг. Индексация сайта поисковиками. Методы спама сайтов и защиты.

Карта веб-приложения. REST API. Формат JSON. JavaScript (Переменные и их область видимости. Функции. Контекст. Прототипное наследование. Асинхронное выполнение кода. Программный интерфейс DOM браузера). Фреймворки для SPA.

Тема 1.3 HTTP. Основные понятия и схема работы.

Версии протокола и их основные отличия. Запросы и ответы. Методы запросов. Заголовки запроса. Заголовки ответа. Коды статуса ответа. Кэширование и условный GET-запрос.

Тема 1.4 Системы аутентификации и авторизации.

Аутентификация. Авторизация. Веб-серверы. Базы данных на стороне сервера. Хранение данных на стороне клиента. Механизмы аутентификации.

Тема 1.5 Возможности браузера.

Введение в HTML. Формы в браузерах. Способы задания стилей, каскад, селекторы CSS . Объект XMLHttpRequest. Cookies и сессии.

Тема 1.6 Поиск субдоменов.

Приложения в рамках одного домена. Встроенные в браузер инструменты анализа. Кеши поисковых систем. Поиск в архиве. Социальные профили. Атаки на передачу зоны. Брутфорс субдоменов. Перебор по словарю.

Тема 1.7 Анализ API.

Обнаружение конечной точки. Разновидности конечных точек. Основные и специализированные разновидности

Тема 1.8 Обнаружение сторонних зависимостей.

Клиентские фреймворки. Фреймворки для одностраничных приложений. Библиотеки JavaScript. Библиотеки CSS. Фреймворки на стороне сервера. Заголовки. Стандартные сообщения об ошибке и страницы 404. Базы данных.

Тема 1.9 Веб-сервисы.

Что такое веб-сервис. Технологии веб-сервисов. XML/JSON over HTTP. XML-RPC. SOAP и WSDL. Архитектурные стили веб-сервисов. RPC. SOA. RESTful. Безопасность веб-сервисов.

Раздел 2 СОВРЕМЕННЫЕ УГРОЗЫ ВЕБ-ПРИЛОЖЕНИЯМ

Тема 2.1 Межсайтовый скриптинг (XSS, Cross Site Scripting).

Обнаружение XSS-уязвимости. Хранимый XSS. Отраженный XSS. XSS-атака на базе DOM. XSS с мутациями.

Тема 2.2 Подделка межсайтовых запросов (CSRF, Cross Site Request Forgery).

Подделка параметров запроса. Изменение содержимого запроса GET. CSRF-атака на конечные точки POST.

Тема 2.3 Атака на внешние сущности XML (XXE, XML eXternal Entity).

Атака напрямую. Непрямая XXE-атака.

Тема 2.4 Внедрение кода

Внедрение SQL-кода. Внедрение кода. Внедрение команд.

Тема 2.5 Отказ в обслуживании (DoS).

ReDoS-атака. Логические DoS-уязвимости. Распределенная DoS-атака.

Тема 2.6 Эксплуатация сторонних зависимостей.

Методы интеграции. Ветви и вилки. Приложения с собственным сервером. Интеграция на уровне кода. Диспетчеры пакетов. База данных общеизвестных уязвимостей.

РАЗДЕЛ 3. ЗАЩИТА СОВРЕМЕННЫХ ВЕБ-ПРИЛОЖЕНИЙ И ВЕБ-СЛУЖБ

Тема 3.1 Прикладные техники разведки и нападения в веб-технологиях.

Архитектура защищенного ПО. Глубокий анализ кода. Поиск уязвимости. Анализ уязвимости. Управление уязвимостями. Регрессивное тестирование. Меры по снижению риска.

Тема 3.2 Безопасная архитектура приложений.

Анализ требований к ПО. Протоколы SSL nTLS. Защита учетных данных. Хеширование учетных данных. Двухфакторная аутентификация. Личные данные и финансовая информация.

Тема 3.3 Проверка безопасности кода.

Основные типы уязвимостей и пользовательские логические ошибки. Антипаттерны безопасного программирования. Черные списки. Шаблонный код. Доверие по умолчанию. Разделение клиента и сервера.

Тема 3.4 Обнаружение уязвимостей.

Автоматизированная проверка. Статический анализ. Динамический анализ. Регрессионное тестирование. Программы ответственного раскрытия информации. Программы Bug Bounty. Сторонние пентестеры.

Тема 3.5 Управление уязвимостями.

Классификации уязвимостей. Общая система оценки уязвимостей. CVSS: Базовая метрика. CVSS: Временная метрика. CVSS: Контекстная метрика.

Тема 3.6 Противодействие XSS-атакам.

Приемы написания кода для противодействия XSS. Очистка пользовательского ввода. Приемник DOMParser. Приемник SVG. Приемник Blob. Санация гиперссылок. Символьные

сущности в HTML. CSS. Политика защиты контента для предотвращения XSS. Директива script-src. Ключевые слова unsafe-eval и unsafe-inline. Внедрение CSP.

Тема 3.7 Защита от CSRF.

Проверка заголовков. CSRF-токен. CSRF-токены без сохранения состояния. Противодействие CRSF на уровне кода. Запросы GET без сохранения состояния. Снижение риска CSRF на уровне приложения.

Тема 3.8 Защита от XXE-атак.

Оценка других форматов данных. Дополнительные риски, связанные с XXE.

Тема 3.9 Противодействие внедрению SQL-кода.

Распознавание внедрения SQL-кода. Подготовленные операторы. Защита от других видов внедрения. Принцип минимальных привилегий. Белый список команд.

Тема 3.10 Противодействие DoS-атакам.

Противодействие атакам ReDoS. Защита от логических DoS-атак. Защита от DdoS. Смягчение DDoS-атак.

Тема 3.11 Защита сторонних зависимостей

Моделирование дерева зависимости. Деревья зависимостей на практике. Автоматизированная оценка. Техники безопасной интеграции. Разделение интересов. Безопасное управление пакетами.

Учебно-методическая карта учебной дисциплины «Технологии разработки и защиты серверных веб-приложений и веб-служб»

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
	Раздел 1 Введение в разведку веб-приложений	**16**	**16**				
1	**Лекция № 1** Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале. Основные задачи, решаемые инженерами-программистами и разработчиками веб-приложений. Основные задачи, решаемые инженерами по безопасности, пентестерами и охотниками за багами. *Тема 1.1 История безопасности программного обеспечения.* Истоки хакерства. «Энигма» и автоматизированный взлом ее шифра (1940-е годы). Фрикинг и первые методы борьбы с фрикингом (1960-е годы). Начало компьютерного взлома (1980-е годы). Расцвет Всемирной паутины (2000-е годы). Современные хакеры (2020-е годы).	2				Осн. лит.: [1], [3]. Доп. лит.: [12], [13], [14], [18]. Эл. рес. [1], [13].	Блиц-опрос
2	**Лекция № 2** *Тема 1.2 Структура современных веб-приложений.* Введение в World Wide Web. URI и URL. Доменные имена. Хостинг. Индексация сайта поисковиками. Методы спама сайтов и защиты.	2				Осн. лит.: [1], [3]. Доп. лит.: [8], [13], [14], [18]. Эл. рес. [1], [12].	Блиц-опрос

1	2	3	4	5	6	7	8
	Карта веб-приложения. REST API. Формат JSON. JavaScript (Переменные и их область видимости. Функции. Контекст. Прототипное наследование. Асинхронное выполнение кода. Программный интерфейс DOM браузера). Фреймворки для SPA.						
3	**Лабораторная работа №1** *Анализ внутренних и внешних угроз информационной безопасности веб-приложения.* *(Знакомство с примерами внутренних угроз безопасности веб-приложения. Знакомство с примерами внешних угроз безопасности веб-приложения. Знакомство с основными методами анализа уязвимостей веб-приложения.)*		4			Методические указания	Защита отчета по лабораторной работе № 1
4	**Лекция № 3** *Тема 1.3 HTTP. Основные понятия и схема работы.* Версии протокола и их основные отличия. Запросы и ответы. Методы запросов. Заголовки запроса. Заголовки ответа. Коды статуса ответа. Кэширование и условный GET-запрос.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [3], [12], [19]. Эл. рес. [3], [11].	Блиц-опрос
5	**Лекция № 4** *Тема 1.4 Системы аутентификации и авторизации.* Аутентификация. Авторизация. Веб-серверы. Базы данных на стороне сервера. Хранение данных на стороне клиента. Механизмы аутентификации.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [2], [12], [18], [20]. Эл. рес. [4], [7], [9].	Блиц-опрос
6	**Лабораторная работа №2** *Разработка проекта по построению системы защиты веб-приложения.* *(Знакомство с примерами отечественных и иностранных стандартов информационной безопасности. Знакомство с языком программирования для разработки веб-приложения.)*		4			Методические указания	Защита отчета по лабораторной работе № 2
7	**Лекция № 5** *Тема 1.5 Возможности браузера.* Введение в HTML. Формы в браузерах. Способы задания стилей, каскад, селекторы CSS. Объект XMLHttpRequest. Cookies и сессии.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [5], [9]. Эл. рес. [5], [6], [12].	*Контрольное тестирование №1

1	2	3	4	5	6	7	8
8	**Лекция № 6** *Тема 1.6 Поиск субдоменов.* Приложения в рамках одного домена. Встроенные в браузер инструменты анализа. Кеши поисковых систем. Поиск в архиве. Социальные профили. Атаки на передачу зоны. Брутфорс субдоменов. Перебор по словарю. *Тема 1.7 Анализ API.* Обнаружение конечной точки. Разновидности конечных точек. Основные и специализированные разновидности.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [4]. Эл. рес. [6], [10], [11].	***Контрольная работа №1**
9	**Лабораторная работа №3** *Разработка клиентской части модуля безопасности веб-приложения.* *(Применение Content Security Policy. Знакомство с межсетевыми запросами. Знакомство с механизмом атаки CRLF-инъекции, направленной на пользователя веб-приложения.)*		4			Методические указания	Защита отчета по лабораторной работе № 3
10	**Лекция № 7** *Тема 1.8 Обнаружение сторонних зависимостей.* Клиентские фреймворки. Фреймворки для одностраничных приложений. Библиотеки JavaScript. Библиотеки CSS. Фреймворки на стороне сервера. Заголовки. Стандартные сообщения об ошибке и страницы 404. Базы данных.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [19]. Эл. рес. . [8], [12].	Блиц-опрос
11	**Лекция № 8** *Тема 1.9 Веб-сервисы.* Что такое веб-сервис. Технологии веб-сервисов. XML/JSON over HTTP. XML-RPC. SOAP и WSDL. Архитектурные стили веб-сервисов. RPC. SOA. RESTful. Безопасность веб-сервисов.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [4], [5], [6], [11], [13], [14], [16]. Эл. рес. [5], [8], [12].	Блиц-опрос
12	**Лабораторная работа №4** *Разработка серверной части модуля безопасности веб-приложения.* *(Изучение серверных операционных систем, которые чаще всего используют в сети Интернет. Изучение виртуальных хостов в веб-серверах Apache и Nginx. Знакомство с примерами архитектурных анти-паттернов, связанных с безопасностью.)*		4			Методические указания	Защита отчета по лабораторной работе № 4

1	2	3	4	5	6	7	8
	Раздел 2 Современные угрозы веб-приложениям	**8**	**8**				
13	**Лекция №9** *Тема 2.1 Межсайтовый скриптинг (XSS, Cross Site Scripting).* Обнаружение XSS-уязвимости. Хранимый XSS. Отраженный XSS. XSS-атака на базе DOM. XSS с мутациями.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [12], [18], [19]. Эл. рес. [2], [4], [10].	Блиц-опрос
14	**Лекция №10** *Тема 2.2 Подделка межсайтовых запросов (CSRF, Cross Site Request Forgery).* Подделка параметров запроса. Изменение содержимого запроса GET. CSRF-атака на конечные точки POST.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [12], [18], [19]. Эл. рес. [2], [4], [10].	Блиц-опрос
15	**Лабораторная работа №5** *Исследование веб-приложения на уязвимости.* *(Знакомство с приемами межсайтового скриптинга. Знакомство с «XML-инъекциями». Знакомство с инъекциями в HTTP-заголовки.)*		4			Методические указания	Защита отчета по лабораторной работе №5
16	**Лекция №11** *Тема 2.3 Атака на внешние сущности XML (XXE, XML eXternal Entity).* Атака напрямую. Непрямая XXE-атака. *Тема 2.4 Внедрение кода* Внедрение SQL-кода. Внедрение кода. Внедрение команд.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [12], [18], [19]. Эл. рес. [2], [4], [10].	Блиц-опрос
17	**Лекция №12** *Тема 2.5 Отказ в обслуживании (DoS).* ReDoS-атака. Логические DoS-уязвимости. Распределенная DoS-атака. *Тема 2.6 Эксплуатация сторонних зависимостей.* Методы интеграции. Ветви и вилки. Приложения с собственным сервером. Интеграция на уровне кода. Диспетчеры пакетов. База данных общеизвестных уязвимостей.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [12], [18], [19]. Эл. рес. [2], [4], [10].	*Контрольное тестирование №2
18	**Лабораторная работа №6** *Разработка средств защиты базы данных веб-приложения.* *(Знакомство с циклом безопасной обработки данных. Знакомство с «SQL-инъекциями». Знакомство со способами борьбы с SQL-инъекциями.)*		4			Методические указания	Защита отчета по лабораторной работе № 6

1	2	3	4	5	6	7	8
	Раздел 3 Защита современных веб-приложений и веб-служб	**10**	**10**				
19	**Лекция №13** *Тема 3.1 Прикладные техники разведки и нападения в веб-технологиях.* Архитектура защищенного ПО. Глубокий анализ кода. Поиск уязвимости. Анализ уязвимости. Управление уязвимостями. Регрессивное тестирование. Меры по снижению риска. *Тема 3.2 Безопасная архитектура приложений.* Анализ требований к ПО. Протоколы SSL nTLS. Защита учетных данных. Хеширование учетных данных. Двухфакторная аутентификация. Личные данные и финансовая информация.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [12], [18], [19]. Эл. рес. [6], [8], [10].	Блиц-опрос
20	**Лекция №14** *Тема 3.3 Проверка безопасности кода.* Основные типы уязвимостей и пользовательские логические ошибки. Антипаттерны безопасного программирования. Черные списки. Шаблонный код. Доверие по умолчанию. Разделение клиента и сервера. *Тема 3.4 Обнаружение уязвимостей.* Автоматизированная проверка. Статический анализ. Динамический анализ. Регрессионное тестирование. Программы ответственного раскрытия информации. Программы Bug Bounty. Сторонние пентестеры. *Тема 3.5 Управление уязвимостями.* Классификации уязвимостей. Общая система оценки уязвимостей. CVSS: Базовая метрика. CVSS: Временная метрика. CVSS: Контекстная метрика.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [12], [18], [19]. Эл. рес. [6], [8], [10].	Блиц-опрос
21	**Лабораторная работа №7** *Создание сценариев атаки и защиты веб-приложения. (Знакомство с примерами атак «грубая сила» и «переполнение буфера». Знакомство с атаками «инъекция команд в протоколы электронной почты. Знакомство с атаками «злоупотребление функциональностью».)*		4			Методические указания	Защита отчета по лабораторной работе № 7

1	2	3	4	5	6	7	8
22	**Лекция №15** *Тема 3.6 Противодействие XSS-атакам.* Приемы написания кода для противодействия XSS. Очистка пользовательского ввода. Приемник DOMParser. Приемник SVG. Приемник Blob. Санация гиперссылок. Символьные сущности в HTML. CSS. Политика защиты контента для предотвращения XSS. Директива script-src. Ключевые слова unsafe-eval и unsafe-inline. Внедрение CSP. *Тема 3.7 Защита от CSRF.* Проверка заголовков. CSRF-токен. CSRF-токены без сохранения состояния. Противодействие CRSF на уровне кода. Запросы GET без сохранения состояния. Снижение риска CSRF на уровне приложения.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [12], [18], [19]. Эл. рес. [6], [8], [10].	Блиц-опрос
23	**Лекция № 16** *Тема 3.8 Защита от XXE-атак.* Оценка других форматов данных. Дополнительные риски, связанные с XXE. *Тема 3.9 Противодействие внедрению* SQL-кода. Распознавание внедрения SQL-кода. Подготовленные операторы. Защита от других видов внедрения. Принцип минимальных привилегий. Белый список команд.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [12], [18], [19]. Эл. рес. [6], [8], [10].	*Контрольное тестирование №3
24	**Лабораторная работа №8** *Нагрузочное тестирование веб-приложения.* *(Знакомство с процессом тестирования на проникновение. Изучение принципов работы балансировщика нагрузки. Изучение и использование скриптовых языков программирования. Изучение производительности веб-сервера.)*		4			Методические указания	Защита отчета по лабораторной работе №8
25	**Лекция № 17** *Тема 3.10 Противодействие DoS-атакам.* Противодействие атакам ReDoS. Защита от логических DoS-атак. Защита от DdoS. Смягчение DDoS-атак.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [12], [18], [19].	

	Тема 3.11 Защита сторонних зависимостей Моделирование дерева зависимости. Деревья зависимостей на практике. Автоматизированная оценка. Техники безопасной интеграции. Разделение интересов. Безопасное управление пакетами.					Эл. рес. [6], [8], [10].	***Контрольная работа №2**
26	**Лабораторная работа №9** *Настройка специального программного обеспечения для мониторинга безопасной работы веб-приложений. (Знакомство и применение на практике защищенных и незащищенных протоколов передачи данных. Знакомство с примерами антивирусов, используемых для организации безопасности веб-серверов. Имитация и возможная митигация (смягчение) всех угроз, найденных приложением.)*		2			Методические указания	Защита отчета по лабораторной работе № 9
	Всего (68 часов)	**34**	**34**				

*** КОНТРОЛЬНЫЕ ТОЧКИ**

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Защита Web-приложений : учебное пособие : [16+] / А. В. Скрыпников, Д. В. Арапов, В. В. Денисенко, Т. Д. Герасимова ; науч. ред. И. А. Хаустов ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2020. – 77 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612405 (дата обращения: 10.08.2021). – Библиогр. в кн. – ISBN 978-5-00032-469-1. – Текст : электронный.

2. Заяц, А. М. Проектирование и разработка WEB-приложений. Введение в frontend и backend разработку на JavaScript и node.js : учебное пособие для вузов / А. М. Заяц, Н. П. Васильев. – 3-е изд., стер. – Санкт-Петербург : Лань, 2021. – 120 с. – ISBN 978-5-8114-7042-6. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/154380 (дата обращения: 10.08.2021). – Режим доступа: для авториз. пользователей.

3. Хофман, Эндрю. Безопасность веб-приложений. Разведка, защита, нападение /Пер. с англ. И. Рузмайкина. – СПб.: Питер, 2021. – 336 с.

Дополнительная:

1. Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз ; перевод с английского А. В. Добровольская. – Москва : ДМК Пресс, 2020. – 308 с. – ISBN 978-5-97060-649-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/131682 (дата обращения: 25.01.2022). – Режим доступа: для авториз. пользователей.

2. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. – Москва : ТУСУР, 2007. – 201 с. – ISBN 978-5-868889-467-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/10927 (дата обращения: 06.10.2021). – Режим доступа: для авториз. пользователей.

3. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. – Москва : ТУСУР, 2012. – 374 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/11381 (дата обращения: 06.10.2021). – Режим доступа: для авториз. пользователей.

4. WS-Security specification (OASIS) [Электронный ресурс]. – http://www.oasis-open.org/specs/index.php#wssv1.0

5. Rertino, F.lisa. Security for Web Services and Service-Oriented Architectures. / Elisa Bertino, Lorenzo D. Martino, Federica Paci, Anna C. Squicciarini. – Berlin, Heidelberg: Springer-Verlag, 2010. – 222 с.

6. Сибраро, Пабло. WCF 4: Windows Communication Foundation и .NET 4 для профессионалов / Пабло Сибраро , Курт Клайс, Фабио Коссолино, Йохан Грабнер. – М.: ООО «И.Д. Вильямс», 2011. – 464 с.

7. Радченко, Г.И. Распределенные вычислительные системы / Г.И. Радченко. – Челябинск: Фотохудожник, 2012. – 184 с.

8. REST: From Research to Practice / E. Wilde, C. Pautasso (ред.) // Springer Science+Business Media, LLC, 2011.

9. Allamaraju, Subbu. RESTful Web Services Cookbook / Subbu Allamaraju. – СПб.: O'Reilly, 2010. – 296 с.

10. Руководство по ASP.NET Web API 2 [Электронный ресурс]. – https://metanit.com/shaip/aspnet_webapi/

11. Лёве, Д. Создание служб WCF. / Д. Лёве. – СПб.: Питер, 2008. – 592 с.

12. Сергеев, Д. Н. Разработка программно-алгоритмического обеспечения контроля целостности веб-приложений / Д. Н. Сергеев ; Алтайский государственный технический университет им. И. И. Ползунова. – Барнаул : б.и., 2020. – 54 с. : ил.,табл.,схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=596486 (дата обращения: 25.01.2022). – Текст : электронный.

13. Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language [Электрон, ресурс]. – www.w3.org/TR/wsdl.

14. Web Services Description Language (WSDL) Version 2.0 Part 0: Primer [Электрон, ресурс]. – http://www.w3.org/TR/wsdl20-primer/.

15. Руководство по ASP.NET Core 2.0 [Электронный ресурс]. – https://metanit.com/sharp/aspnet5/.

16. SOAP 1.2 specification (W3C) [Электронный ресурс]. – http://www.w3.org/TR/soap12-part1/.

17. Troelsen, Andrew. C# 6.0 and the .NET 4.6 Framework. / Andrew Troelsen, Philip Japikse. – Apress, 2015. – 1625 c.

18. Малашкевич В.Б. Интернет-программирование : лабораторный практикум / В.Б. Малашкевич ; Поволжский государственный технологический университет. – Йошкар-Ола : ПГТУ, 2017. – 96 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=476400.

19. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс] : учебное пособие. – Москва : Издательский дом Высшей школы экономики, 2015. – 574 с. – Режим доступа :http://biblioclub.ru/index.php?page=book&id=440285.

20. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учебное пособие / А.А. Афанасьев [и др.] ; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – Москва : Горячая линия-Телеком, 2012. – 550 с. – Режим доступа: https://e.lanbook.com/book/5114.

21. Байер, Д. Microsoft ASP.NET: обеспечение безопасности. – М. ; СПб. : Русская Редакция : Питер, 2008. – XYIII, 428 с. : ил.

Электронные ресурсы:

1. Справочная правовая система Консультант плюс [электронный ресурс] – Режим доступа: http://www.consultant.ru/online/.

2. Бизнес без опасности [Электронный ресурс – Режим доступа : https://lukatsky.blogspot.com/2019/01/2018.html.

3. Что такое стандарты информационной безопасности? // официальный сайт компании «Эксперт СРО» [Электронный ресурс] – Режим доступа : https://sro-iso-expert.ru/stati/chto_takoe_standarty_informacionnoj_bezopasnosti/.

4. Международные стандарты информационной безопасности // сайт Лаборатория Сетевой Безопасности Your Private Network [Электронный ресурс] – Режим доступа : http://ypn.ru/177/international-standards-of-information-technologies-security/.

5. 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [Электронный ресурс] – Режим доступа : http://geoline-tech.com/top-20-sites-about-information-security/.

6. Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [Электронный ресурс] – Режим доступа : http://dorlov.blogspot.eom/p/blog-page_3151.html.

7. Информационная безопасность [Электронный ресурс] – Режим доступа : http://www.securrity.ru/.

8. 30 ресурсов по безопасности, которые точно пригодятся [Электронный ресурс] – Режим доступа: https://proglib.io/p/information-security-guide/.

9. Информационная безопасность. Защита данных // habr – веб-сайт в формате коллективного блога с элементами новостного сайта [Электронный ресурс] – Режим доступа : https://habr.com/ru/hub/infosecurity/.

10. База Знаний Клуба Информационной безопасности [Электронный ресурс] – Режим доступа: http://wiki.informationsecurity.club/doku.php/main.

11. Информационная безопасность. Защита данных [Электронный ресурс] – Режим доступа: http://all-ib.ru/.

12. Электронные справочники по HTML и CSS [Электронный ресурс]. – Режим доступа: www.htmlbook.ru.

13. Закон Республики Беларусь № 455-З от 10.11.2008 г. «Об информации, информатизации и защите информации (Национальный реестр правовых актов Республики Беларусь, 2008 г, № 279, 2/155. http://pravo.by/document/?guid=12551&p0=H11400102&p1=1. https://normativka.by/lib/document/500066195/sid/5b93f5cc6a874b3ba977f2fbaf8b6e57.

14. https://habr.com/ru/post/254165/.

15. История Интернет. [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/History_of_the_Internet, http://ru.wikipedia.org/wiki/Интернет. – Дата доступа: 29.01.2021.

16. История World Wide Web. [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/History_of_the_World_Wide_Web; http://ru.wikipedia.org/wiki/WWW. – Дата доступа: 29.01.2021.

17. История W3C. [Электронный ресурс]. – Режим доступа: http://www.w3.org/Consortium/history; http://ru.wikipedia.org/wiki/W3C. – Дата доступа: 29.01.2019.

18. Web Standards Project. [Электронный ресурс]. – Режим доступа: http://webstandards.org/ – Дата доступа: 29.01.2018 и его история Режим доступа: http://www.webstandards.org/about/history/.– Дата доступа: 29.01.2021.

19. Дунаев, В.В. Д83 (X)HTML, скрипты и стили. Самое необходимое. [Электронный ресурс]. / В.В. Дунаев. – СПб.: БХВ-Петербург, 2009. – 488 с. – Режим доступа: http://znanium.com/bookread.php/book=489162. – Дата доступа: 29.01.2021.

20. Прохоренок, Н.А. Разработка Web-сайтов с помощью Perl и MySQL. [Электронный ресурс]. / Н.А. Прохоренок . – СПб.: БХВ-Петербург, 2009. –560 с. – Режим доступа: http://znanium.com/bookread.php/book=489301. – Дата доступа: 29.01.2018.

21. Прохоренок, Н.А. HTML, JavaScript, PHP и MySQL. Джентльменский набор Web-мастера. – 3-е изд., перераб. и доп. [Электронный ресурс]. / Н.А. Прохоренок. – СПб.: БХВ-Петербург, 2010. – 912 с. – Режим доступа:

22. https://studfiles.net/preview/6197065/. – Дата доступа: 29.01.2021.

23. Учебник по HTML. [Электронный ресурс]. – Режим доступа: http://html.find-info.ru/html/005/index.htm/. – Дата доступа: 29.01.2021.

24. Современный учебник JavaScript. [Электронный ресурс]. – Режим доступа: https://learn.javascript.ru/. – Дата доступа: 29.01.2021.

Перечень компьютерных программ:

1. Операционные системы: Windows и Linux.
2. Web-браузеры: Opera, Internet Explorer, Microsoft Edge, Firefox, Google Chrome.
3. FrontEnd разработка веб-приложений: фреймворки на основе JS: AngularJS, ReactJS, VueJS.
4. BackEnd разработка веб-приложений: Node.js, Java, Django, Python, Ruby и др.
5. Системы управления базами данных: MySQL, PostgreSQL, Microsoft SQL Server, Oracle, MongoDB и др.
6. Блокнот, Notepad++.

ПЕРЕЧЕНЬ ТЕМ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа №1 Анализ внутренних и внешних угроз информационной безопасности веб-приложения
(Знакомство с примерами внутренних угроз безопасности веб-приложения. Знакомство с примерами внешних угроз безопасности веб-приложения. Знакомство с основными методами анализа уязвимостей веб-приложения.)

Лабораторная работа №2 Разработка проекта по построению системы защиты веб-приложения
(Знакомство с примерами отечественных и иностранных стандартов информационной безопасности. Знакомство с языком программирования для разработки веб-приложения.)

Лабораторная работа №3 Разработка клиентской части модуля безопасности веб-приложения.
(Применение Content Security Policy. Знакомство с межсетевыми запросами. Знакомство с механизмом атаки CRLF-инъекции, направленной на пользователя веб-приложения.)

Лабораторная работа №4 Разработка серверной части модуля безопасности веб-приложения.
(Изучение серверных операционных систем, которые чаще всего используют в сети Интернет. Изучение виртуальных хостов в веб-серверах Apache и Nginx. Знакомство с примерами архитектурных анти-паттернов, связанных с безопасностью.)

Лабораторная работа №5 Исследование веб-приложения на уязвимости.
(Знакомство с приемами межсайтового скриптинга. Знакомство с «XML-инъекциями». Знакомство с инъекциями в HTTP-заголовки.)

Лабораторная работа №6 Разработка средств защиты базы данных веб-приложения.
(Знакомство с циклом безопасной обработки данных. Знакомство с «SQL-инъекциями». Знакомство со способами борьбы с SQL-инъекциями.)

Лабораторная работа №7 Создание сценариев атаки и защиты веб-приложения.
(Знакомство с примерами атак «грубая сила» и «переполнение буфера». Знакомство с атаками «инъекция команд в протоколы электронной почты. Знакомство с атаками «злоупотребление функциональностью».)

Лабораторная работа №8
Нагрузочное тестирование веб-приложения.
(Знакомство с процессом тестирования на проникновение. Изучение принципов работы балансировщика нагрузки. Изучение и использование скриптовых языков программирования. Изучение производительности веб-сервера.)

Лабораторная работа №9 Настройка специального программного обеспечения для мониторинга безопасной работы веб-приложений.
(Знакомство и применение на практике защищенных и незащищенных протоколов передачи данных. Знакомство с примерами антивирусов, используемых для организации безопасности веб-серверов. Имитация и возможная митигация (смягчение) всех угроз, найденных приложением.)

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

Вопросы по теоретической части дисциплины

1. Цели и задачи изучения дисциплины.
2. Основные понятия и определения.
3. Проблемы безопасности веб-приложений.
4. Виды уязвимостей веб-приложения.
5. Особенности исследования веб-приложения на уязвимости.
6. Принципы безопасного использования интернет-сайтов.
7. Классификация угроз информационной безопасности.
8. Внутренние и внешние угрозы информационной безопасности веб-приложения.
9. Способы аутентификации пользователей.
10. Технологии безопасной передачи информации в сети Интернет.
11. Жизненный цикл защиты веб-приложения.
12. Этапы разработки клиентской части модуля безопасности веб-приложения.
13. Этапы разработки серверной части модуля безопасности веб-приложения.
14. Основы тестирования безопасности веб-приложения.
15. Средства защиты базы данных веб-приложения.
16. Технологии и инструменты обеспечения информационной безопасности на этапе разработки веб-приложения.
17. Технологии и инструменты обеспечения информационной безопасности на этапе тестирования веб-приложения.
18. Технологии и инструменты обеспечения информационной безопасности на этапе внедрения веб-приложения.
19. Технологии и инструменты обеспечения информационной безопасности на этапе использования веб-приложения.
20. Подсистемы защиты веб-порталов от информационных атак.
21. Защищенные и незащищенные протоколы передачи данных и их использование.
22. Виды DDoS-атак. Обнаружение DDoS-атак.
23. Причины возникновения уязвимостей типа Injection.
24. Подсистемы защиты веб-порталов от информационных атак
25. Приведите примеры внутренних угроз безопасности веб-приложения.
26. Приведите примеры внешних угроз безопасности веб-приложения.
27. Опишите основные методы анализа уязвимостей веб-приложения.
28. Приведите примеры отечественных и иностранных стандартов информационной безопасности.
29. Опишите безопасный цикл разработки веб-приложения.
30. Какие языки программирования используются для разработки веб-приложений?
31. Для чего используется Content Security Policy?
32. Что такое межсетевые запросы?
33. Опишите механизм атаки CRLF-инъекции, направленной на пользователя веб-приложения.
34. Какие серверные операционные системы чаще всего используют в сети Интернет?
35. Что такое виртуальные хосты в веб-серверах Apache и Nginx?
36. Приведите примеры архитектурных анти-паттернов, связанных с безопасностью.
37. Опишите цикл безопасной обработки данных.
38. Что такое «SQL-инъекция»?
39. Перечислите способы борьбы с SQL-инъекциями.
40. Что такое тестирование на проникновение?
41. Для чего нужен балансировщик нагрузки?
42. Влияет ли использование скриптовых языков программирования (например, PHP) на производительность веб-сервера?
43. Что такое межсайтовый скриптинг?

44. Что такое «XML-инъекция»?
45. Что такое инъекции в HTTP-заголовки?
46. Поясните суть атак «грубая сила» и «переполнение буфера».
47. Поясните суть атаки «инъекция команд в протоколы электронной почты».
48. Поясните суть атаки «злоупотребление функциональностью».
49. Как используются защищенные и незащищенные протоколы передачи данных?
50. Приведите примеры антивирусов, используемых для организации безопасности веб-серверов.
51. Специальное программное обеспечение для мониторинга безопасной работы веб-приложений.
52. Опишите возможную митигацию для всех угроз, найденных приложением.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Технологии разработки и защиты серверных веб-приложений и веб-служб» предполагает реализацию следующих форм самостоятельной работы студентов:

– проработка конспекта лекций и учебной литературы;

– изучение печатных источников по теме дисциплины;

– изучение профессиональных электронных ресурсов по теме дисциплины;

– изучение вопросов для самоконтроля;

– подготовка к аудиторному выполнению лабораторных работ (предварительное знакомство с методическими указаниями, программным обеспечением, вариантом индивидуального задания по работе);

– решение индивидуальных задач при подготовке к лабораторным занятиям;

– выполнение практических упражнений (работа с тренажерами) для закрепления знаний и навыков;

– подготовка к защите лабораторных (оформление отчёта по индивидуальному варианту задания, защита результатов работы и демонстрации степени освоения навыков и умений по конкретной теме);

– решение во внеурочное время контрольных задач, получаемых на лекциях;

– углублённое изучение отдельных тем учебной дисциплины для подготовки к устным опросам;

– изучение основной и дополнительной и научной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;

– подготовка к промежуточной и текущей диагностике компетенции (письменным контрольным работам);

–систематизация полученных знаний при подготовке к зачету.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации образовательного процесса, обеспечиваются:

– наличием и использованием в образовательном процессе открытых систем автоматизированного тестирования при использовании бесплатного сервиса для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google – Google Класс, которые доступны пользователям через Интернет в любое удобное для них время;

– использованием бизнес-мессенджера для групповой работы и общения Microsoft Teams;

– использованием «облачных» технологий, в частности облачного хранилища файлового хостинга компании Dropbox для размещения материалов по читаемой дисциплине;

– наличием и полной доступностью электронных вариантов курса лекций и учебно-методических указаний по основным разделам дисциплины.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещённые на бесплатном сервисе для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google Класс Room университета: шифр курса **Q2Q2T7F.**
2. Материалы, размещённые в бизнес-мессенджере для групповой работы и общения Microsoft Teams: шифр курса **DTXTDJH.**
3. Методические указания к выполнению лабораторных работ по дисциплине «Технологии разработки и защиты серверных веб-приложений и веб-служб» для студентов специальности 1-98 01 01 Компьютерная безопасность (по направлениям) 1-98 01 01-01 «Компьютерная безопасность (математические методы и программные системы)».

Содержание самостоятельной работы студентов

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины при подготовке к контрольным работам	*Тема 1.2 Структура современных веб-приложений.* Карта веб-приложения. REST API. Формат JSON. JavaScript (Переменные и их область видимости. Функции. Контекст. Прототипное наследование. Асинхронное выполнение кода. Программный интерфейс DOM браузера). Фреймворки для SPA. Осн. лит.: [1], [3]. Доп. лит.: [8], [13], [14], [18]. Эл. рес. [1], [12].	4
	Тема 1.6 Поиск субдоменов. Приложения в рамках одного домена. Встроенные в браузер инструменты анализа. Кеши поисковых систем. Поиск в архиве. Социальные профили. Атаки на передачу зоны. Брутфорс субдоменов. Перебор по словарю. Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [4]. Эл. рес. [6], [10], [11].	4
	Тема 1.9 Веб-сервисы. XML/JSON over HTTP. XML-RPC. SOAP и WSDL. Архитектурные стили веб-сервисов. RPC. SOA. RESTful. Безопасность веб-сервисов. Осн. лит.: [1], [2], [3]. Доп. лит.: [4], [5], [6], [11], [13], [14], [16]. Эл. рес. [5], [8], [12].	4
	Тема 3.2 Безопасная архитектура приложений. Анализ требований к ПО. Протоколы SSL nTLS. Защита учетных данных. Хеширование учетных данных. Двухфакторная аутентификация. Личные данные и финансовая информация. Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [12], [18], [19]. Эл. рес. [6], [8], [10].	4
	Тема 3.6 Противодействие XSS-атакам. Приемы написания кода для противодействия XSS. Очистка пользовательского ввода. Приемник DOMParser. Приемник SVG. Приемник Blob. Санация гиперссылок. Символьные сущности в HTML. CSS. Политика защиты контента для предотвращения XSS. Директива script-src. Ключевые слова unsafe-eval и unsafe-inline. Внедрение CSP. Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2], [3], [12], [18], [19]. Эл. рес. [6], [8], [10].	4
Подготовка к защите отчетов по лабораторным работам	**Лабораторная работа №1** *Анализ внутренних и внешних угроз информационной безопасности веб-приложения.*	2
	Лабораторная работа №2 *Разработка проекта по построению системы защиты веб-приложения.*	2
	Лабораторная работа №3 *Разработка клиентской части модуля безопасности веб-приложения.*	2
	Лабораторная работа №4 *Разработка серверной части модуля безопасности веб-приложения.*	2

1	2	3
Подготовка к защите отчетов по лабораторным работам	***Лабораторная работа №5*** *Исследование веб-приложения на уязвимости.*	2
	Лабораторная работа №6 *Разработка средств защиты базы данных веб-приложения.*	2
	Лабораторная работа №7 *Создание сценариев атаки и защиты веб-приложения.*	2
	Лабораторная работа №8 *Нагрузочное тестирование веб-приложения.*	2
	Лабораторная работа №9 *Настройка специального программного обеспечения для мониторинга безопасной работы веб-приложений.*	2
	ВСЕГО	**38**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Контроль качества усвоения знаний проводится в соответствии с Положением о рейтинговой системе оценки знаний и компетенций студентов (приказ ректора УО ПГУ № 294 от 06.06.2014 (в редакции, утверждённой приказом № 605 от 17.11.2014) в форме промежуточного контроля и текущей аттестации.

Для оценивания самостоятельной и аудиторной работы студентов в рамках дисциплины используется накопительная система контроля успеваемости, которая предполагает суммирование бальных оценок, выставляемых в электронный журнал за все виды работ в течение прохождения курса для определения среднеарифметических показателей успеваемости.

Мероприятия промежуточного контроля проводятся в течение семестра и включают в себя следующие формы контроля:

–устная форма (блиц-опрос на лекциях);

–письменная форма (тесты, контрольные работы, письменные отчёты по лабораторным работам);

–устно-письменная форма (отчёты по лабораторным с их устной защитой);

–техническая форма (электронные тесты, визуальные лабораторные работы).

Лабораторные работы предполагают выполнение и защиту. Последнее лабораторное занятие в семестре предусматривает выполнение и защиту зачётной работы, а также контрольное тестирование. При выполнении лабораторных работ выдаётся индивидуальное задание. Отчёт по лабораторной работе представляется в электронном виде. Содержание отчёта: название работы, вариант задания, анализ задания, ход выполнения работы, основные и промежуточные результаты, выводы по работе. Защита работ проводится индивидуально и оценивается в соответствии установленными правилами.

Промежуточная (аттестационная) диагностика компетенции студентов осуществляется на основании индивидуального рейтинга студента на момент аттестации. Для положительной аттестации (промежуточного контроля успеваемости) необходимо согласно календарному плану выполнить все лабораторные работы и индивидуальные задания, а также иметь положительную оценку по промежуточному контролю освоения теоретической части курса.

Результат *промежуточного контроля за семестр* оценивается отметкой в баллах по десятибалльной шкале и выводится, исходя из отметок, выставленных в ходе проведения мероприятий промежуточного контроля в течение семестра по следующей формуле:

$$П = \frac{(КТ_1 + ... + КТ_n) + (ЛР_1 + ЛР_9) + (КР_1 + КР_2)}{(11 + n)},$$

где $КТ_1 + ... + КТ_n$ – отметки, выставленные по результатам контрольного тестирования;

n – количество тестов;

$ЛР_1 + ЛР_9$ – отметки, выставленные по результатам защит лабораторных работ.

$КР_1, КР_2$ – отметки, выставленные по результатам контрольных работ.

Результат промежуточного контроля рассчитывается как округлённое среднее значение. Результат может быть увеличен в соответствии с п.п. 6.8 и 6.9 Положения.

Текущая аттестация проводится в форме зачёта.

Зачёт проводится согласно Положению.

Заключение о *зачёте* формируется на основе накопительного принципа по формуле:

$$З = k \cdot П,$$

где k– весовой коэффициент промежуточного контроля;

П – результат промежуточного контроля за семестр.

Весовой коэффициент k принимается равным 1.

Если полученная отметка $З < 4$ баллов, то проводится устный зачёт отдельно по представленным в программе вопросам.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основные методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

– проблемное обучение (проблемное изложение, вариативное изложение), реализуемое на лекционных занятиях;

– учебно-исследовательская деятельность, реализация творческого подхода, реализуемые на лабораторных занятиях.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Технологии разработки и защиты серверных веб-приложений и веб-служб» реализуют подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента, проявляющейся в чётком понимании им значимости всех видов выполняемых работ, как с точки зрения важности для профессиональной подготовки, так и с точки зрения оценивания. Подход предполагает использование элементов проблемного обучения и элементов исследовательской деятельности студентов в процессе аудиторной работы, а также при выполнении самостоятельных работ при постоянном рейтинговом контроле.

На лекционных занятиях по дисциплине «Технологии разработки и защиты серверных веб-приложений и веб-служб» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных и лабораторных занятиях.

На лекционных занятиях студенты овладевают системой теоретических знаний в области построения веб-приложений, удовлетворяющих требованиям безопасности и надежности. В ходе лекционного изложения теоретических сведений используются традиционные словесные приёмы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий с опорой на имеющуюся начальную подготовку студентов и их политехнический кругозор, использованием интерактивных методов обучения.

На лабораторных занятиях развиваются и формируются необходимые практические умения и навыки построения веб-приложений, удовлетворяющих требованиям безопасности и надежности, а также навыки ручного и автоматизированного тестирования уязвимостей веб-приложений с использованием различных специальных средств.

Применяется индивидуальный, творческий подход. Студенты получают от преподавателя индивидуальные задания, в рамках самостоятельной работы разрабатывают свои веб-приложений, удовлетворяющих требованиям безопасности и надежности. Также во время проведения лабораторных работ особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её выполнения.