Министерство образования Иркутской области
Государственное бюджетное профессиональное
образовательное учреждение Иркутской области
«Иркутский авиационный техникум»

Методические указания по выполнению самостоятельной работы по междисциплинарному курсу

МДК.03.03 Обеспечение безопасности веб-приложений

специальности
09.02.11 Разработка и управление программным обеспечением

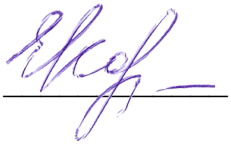
Иркутск, 2026

РАССМОТРЕНЫ

Председатель ЦК

_____ / /

УТВЕРЖДАЮ
Зам. директора


_____ Е.А. Коробкова

№	Разработчик ФИО
1	Бодоев Даниил Александрович

Пояснительная записка

МДК.03.03 Обеспечение безопасности веб-приложений относится к ПМ.03 проектирование и разработка веб-приложений. Самостоятельная работа является одним из видов учебно работы обучающегося без взаимодействия с преподавателем.

Основные цели самостоятельной работы:

- систематизация и закрепление теоретических знаний и практических умений обучающихся;
- углубление и расширение теоретических знаний, формирование умений использовать справочную документацию и дополнительную литературу;
- развитие познавательных способностей и активности обучающихся, творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельного мышления; развитие исследовательских умений.

Рекомендации для обучающихся по выработке навыков самостоятельной работы:

Внимательно читать план выполнения работы. Учиться кратко и емко излагать свои мысли. Обращать внимание на рекомендуемые источники.

Тематический план

Раздел Тема	Тема занятия	Название работы	Количество часов
Раздел 1. Основы безопасности веб-приложений Тема 3. Аутентификация и авторизация	Систематизация мер комплексной защиты веб-приложений.	Систематизация мер комплексной защиты веб-приложений.	2

Самостоятельная работа №1

Название работы: Систематизация мер комплексной защиты веб-приложений..
Цель работы: Систематизировать знания о мерах комплексной защиты веб-приложений, способах выявления и устранения уязвимостей, защите пользовательских данных, безопасной аутентификации и авторизации на стороне клиента.
Уровень СРС: реконструктивная.
Форма контроля: проверка письменного отчета.
Количество часов на выполнение: 2 часа.
Задание:
Подготовить письменный отчет по теме «Комплексная защита веб-приложений». В отчете раскрыть классификацию уязвимостей веб-приложений, модели анализа угроз, инструменты анализа безопасности, методы тестирования на проникновение и способы устранения уязвимостей на стороне клиента. Отдельно описать защиту пользовательских данных с использованием HttpOnly cookie, SameSite политики, Secure cookie и токена доступа. Сделать вывод о роли комплексного подхода в обеспечении безопасности веб-приложений.
Критерии оценки:

оценка «5» - Отчет выполнен полностью, раскрыты все основные меры комплексной защиты веб-приложений, верно описаны классификация уязвимостей, модели анализа угроз, инструменты анализа безопасности, методы тестирования на проникновение и способы устранения уязвимостей. Отдельно и корректно раскрыта защита пользовательских данных с использованием HttpOnly cookie, SameSite политики, Secure cookie и токена доступа. Вывод сформулирован логично.

оценка «4» - Отчет выполнен в основном правильно, раскрыты основные меры защиты веб-приложений, но отдельные вопросы описаны неполно или с незначительными неточностями. Защита пользовательских данных, инструменты анализа безопасности или методы устранения уязвимостей раскрыты частично. Вывод имеется, но требует уточнения.

оценка «3» - Отчет выполнен частично, раскрыты только отдельные меры защиты веб-приложений. Имеются ошибки или существенные пропуски в описании уязвимостей, анализа угроз, инструментов безопасности, тестирования на проникновение или способов устранения уязвимостей. Вывод краткий либо недостаточно обоснованный.