



«УТВЕРЖДАЮ»

Директор Института СПО

М.А. Харламова

**РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ**

МДК.09.03 Обеспечение безопасности веб-приложений

09.02.07 Информационные системы и программирование

Квалификация: Разработчик веб и мультимедийных приложений

Базовый уровень подготовки

Форма обучения: **очная**

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.07 – «Информационные системы и программирование», утвержденного приказом Министерства образования и науки Российской Федерации от «9» декабря 2016 г. № 1547.

Место дисциплины в структуре ППССЗ СПО МДК.09.03 «Обеспечение безопасности веб-приложений»

Учебная дисциплина МДК.09.03 «Обеспечение безопасности веб-приложений» входит в состав профессионального модуля ПМ.09 «Проектирование, разработка и оптимизация веб-приложений».

Рабочая программа разработана на кафедре математического моделирования, компьютерных технологий и информационной безопасности

Зав. кафедрой: О.Н. Масина

Разработчик(и) рабочей программы:

Преподаватель Института СПО Попов С.Е.

Рецензент

доцент, к. п. н., Тарова И.Н.

СОДЕРЖАНИЕ

- 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ **МДК.09.03 Обеспечение безопасности веб-приложений**

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью образовательной программы в соответствии с ФГОС по специальности 09.02.07 – Информационные системы и программирование.

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке по смежным специальностям.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Шифр дисциплины по учебному плану: МДК.09.03.

Дисциплина является частью профессионального модуля ПМ.09 учебного плана по специальности СПО 09.02.07 – Информационные системы и программирование. Направлена на формирование следующих общих и профессиональных компетенций: ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 7, ОК 8, ОК 9, ОК 10, ПК 9.8

1.3. Цели и задачи дисциплины – требования к результатам освоения содержания дисциплины

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК.09.03 должен:

уметь:

- выполнять мониторинг и анализ работы сети с помощью программно-аппаратных средств; всех компонентов сети;
- выполнять действия по устранению неисправностей;
- проводить SQL- инъекции и XSS-инъекции;
- проводить тестирование защищенности механизма управления доступом и сессиями;
- проводить тестирование на устойчивость к атакам отказа в обслуживании.

знать:

- Регламенты и методы разработки безопасных веб-приложений
- правила безопасной аутентификации и авторизации;
- способы повышения привилегий и общей отказоустойчивости системы;
- архитектуру и функции систем управления сетями, стандарты систем управления;
- средства мониторинга и анализа локальных сетей;
- методы устранения неисправностей в технических средствах
- основные принципы построения безопасных сайтов. Понятие безопасности приложений и классификация опасностей

иметь практический опыт:

- проектирования архитектуры локальной сети в соответствии с поставленной задачей;
- проверка корректности данных, вводимых пользователем;
- способы публикации изображений и файлов;
- применения методов шифрования;
- установки и настройки сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей;
- выбора технологии, инструментальных средств при организации процесса исследования объектов сетевой инфраструктуры;
- обеспечения целостности резервирования информации, использования VPN;
- установки и обновления сетевого программного обеспечения;
- мониторинга производительности сервера и протоколирования системных и сетевых событий;
- использования специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей;
- оформления технической документации;
- поиска источников угроз информационной безопасности и принятия мер по их предотвращению

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС СПО и ОПОП СПО по данной специальности:

а) общих (ОК):

- ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
- ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
- ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.
- ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
- ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
- ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
- ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
- ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
- ОК 9. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

б) профессиональных (ПК):

- ПК 9.8. Осуществлять аудит безопасности веб-приложения в соответствии с регламентами по безопасности

1.4. Рекомендуемое количество часов на освоение программы дисциплины:
 максимальной учебной нагрузки обучающегося 158 часов, в том числе:
 обязательной аудиторной учебной нагрузки обучающегося 126 часов;
 самостоятельной работы обучающегося 24 часа.
 Консультация 2 часа

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	158
Обязательная аудиторная учебная нагрузка (всего)	126
в том числе:	
лекционные занятия	63
лабораторные занятия	63
практические занятия	-
контрольные работы	-
курсовая работа (проект) (если предусмотрено)	6
консультация	2
Самостоятельная работа обучающегося (всего)	24
в том числе:	
Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).	8
Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа при самом широком использовании Интернета и других IT-технологий	8
Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите.	8
Промежуточная аттестация в форме: экзамен в 7 семестре	6

2.2. Тематический план и содержание учебной дисциплины
МДК.09.03 Обеспечение безопасности веб-приложений

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)		Объём в часах	Уровень освоения
1	2		3	4
Раздел ПМ.09. Проектирование, разработка и оптимизация веб-приложений				
МДК.09.03. Обеспечение безопасности веб-приложений				
Тема 3.1. Обеспечение безопасности веб-приложений	<i>Содержание</i>			
	1	История защиты программного обеспечения. Истоки хакерства. «Энигма». Автоматизированный взлом шифра «Энигмы». Появление «бомбы». Фрикинг. Метод борьбы с фрикингом. Начало компьютерного взлома. Расцвет Всемирной паутины. Современные хакеры.	2	2,3
	Разведка			
	2	Введение в разведку веб-приложений. Сбор информации. Карта веб-приложения	2	2,3
	3	Структура современных веб-приложений. Сравнение современных и более ранних версий приложений. REST API. Формат JSON. JavaScript. Переменные и их область видимости. Функции. Контекст. Прототипное наследование. Асинхронное выполнение кода. Программный интерфейс DOM браузера. Фреймворки для SPA. Системы аутентификации и авторизации. Аутентификация. Авторизация. Веб-серверы. Базы данных на стороне сервера. Хранение данных на стороне клиента.	2	2,3

4	Поиск субдоменов. Множество приложений в рамках одного домена. Встроенные в браузер инструменты анализа. Общедоступная информация. Кэши поисковых систем. Поиск в архиве. Социальные профили. Атаки на передачу зоны. Брутфорс субдоменов. Перебор по словарю.	2	2,3
5	Анализ API. Обнаружение конечной точки. Механизмы аутентификации. Разновидности конечных точек. Основные разновидности. Специализированные разновидности.	2	2,3
6	Обнаружение сторонних зависимостей. Обнаружение сторонних зависимостей. Фреймворки для одностраничных приложений. Библиотеки JavaScript. Библиотеки CSS. Фреймворки на стороне сервера. Заголовки. Стандартные сообщения об ошибке и страницы 404. Базы данных.	2	2,3
7	Поиск слабых мест в архитектуре приложения. Признаки безопасной и небезопасной архитектуры. Уровни безопасности. Заимствование и перекрой.	2	2,3
Нападение			
8	Введение во взлом веб-приложений. Мышление хакера. Применение данных, полученных в процессе разведки.	2	2,3
9	Межсайтовый скриптинг (XSS). Обнаружение XSS-уязвимости. Хранимый XSS. Отраженный XSS. XSS-атака на базе DOM. XSS с мутациями.	2	2,3
10	Подделка межсайтовых запросов (CSRF). Подделка параметров запроса. Изменение содержимого запроса GET.CSRF-атака на конечные точки POST.	2	2,3
11	Атака на внешние сущности XML (XXE). Атака напрямую.Непрямая XXE-атака.	2	
12	Внедрение кода. Внедрение SQL-кода.Внедрение кода. Внедрение команд.	2	
13	Отказ в обслуживании (DoS). ReDoS-атака.Логические DoS-уязвимости. Распределенная DoS-атака	2	
14	Эксплуатация сторонних зависимостей. Методы интеграции. Ветви и вилки. Приложения с собственным сервером. Интеграция на уровне кода. Диспетчеры пакетов. JavaScript. Java. Другие языки. База данных общеизвестных уязвимостей.	2	
Защита			
15	Защита современных веб-приложений. Архитектура защищенного ПО. Глубокий анализ кода. Поиск уязвимости. Анализ уязвимости. Управление уязвимостями. Регрессивное тестирование. Меры по снижению риска.	2	

	16	Безопасная архитектура приложений. Анализ требований к ПО. Аутентификация и авторизация. Протоколы SSL и TLS. Защита учетных данных. Хеширование учетных данных. Двухфакторная аутентификация. Личные данные и финансовая информация. Поиск.	2	
	17	Проверка безопасности кода. Начало проверки. Основные типы уязвимостей и пользовательские логические ошибки. С чего начать проверку безопасности. Антипаттерны безопасного программирования. Черные списки. Шаблонный код. Доверие по умолчанию. Разделение клиента и сервера.	2	
	18	Обнаружение уязвимостей. Автоматизированная проверка. Статический анализ. Динамический анализ. Регрессионное тестирование. Программы ответственного раскрытия информации. Программы Bug Bounty. Сторонние пентестеры.	4	
	19	Управление уязвимостями. Воспроизведение уязвимостей. Классификация уязвимостей. Общая система оценки уязвимостей. CVSS: Базовая метрика. CVSS: Временная метрика. CVSS: Контекстная метрика. Усовершенствованная классификация уязвимостей.	2	
	20	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.	4	
	21	Защита от CSRF. Проверка заголовков. CSRF-токен. CSRF-токены без сохранения состояния. Противодействие CSRF на уровне кода. Запросы GET без сохранения состояния. Снижение риска CSRF на уровне приложения.	4	
	22	Защита от XXE-атак. Оценка других форматов данных. Дополнительные риски, связанные с XXE.	4	
	23	Противодействие внедрению. Противодействие внедрению SQL-кода. Распознавание внедрения SQL-кода. Подготовленные операторы. Более специфические методы защиты. Защита от других видов внедрения. Потенциальные цели внедрения. Принцип минимальных привилегий. Белый список команд.	4	
	24	Противодействие DoS-атакам. Противодействие атакам ReDoS. Защита от логических DoS-атак. Защита от DDoS. Смягчение DDoS-атак.	4	

25	История безопасности программного обеспечения. Разведка. Нападение. Защита.	3	
<i>В том числе практических занятий и лабораторных работ</i>			
1	Социальная инженерия	2	2,3
2	Исследование сетевых атак и инструментов проверки защиты сети	2	2,3
3	Настройка безопасного доступа к маршрутизатору	2	2,3
4	Обеспечение административного доступа AAA и сервера Radius	2	2,3
5	Настройка политики безопасности брандмауэров	2	2,3
6	Настройка системы предотвращения вторжений (IPS)	2	2,3
7	Настройка безопасности на втором уровне на коммутаторах	2	2,3
8	Исследование методов шифрования	2	2,3
9	Основные принципы построения безопасных сайтов. Понятие безопасности приложений и классификация опасностей	2	2,3
10	Источники угроз информационной безопасности и меры по их предотвращению	2	2,3
11	Регламенты и методы разработки безопасных веб-приложений	2	2,3
12	Безопасная аутентификация и авторизация.	2	2,3
13	Повышение привилегий и общая отказоустойчивость системы	2	2,3
14	Проверка корректности данных, вводимых пользователем. Публикация изображений и файлов. Методы шифрования. SQL- инъекции. XSS-инъекции	2	2,3
15	Сбор информации о web-приложении.	2	2,3
16	Тестирование защищенности механизма управления доступом и сессиями	2	2,3
17	Тестирование на устойчивость к атакам отказа в обслуживании	2	2,3
18	Поиск уязвимостей к атакам XSS.	2	2,3
19	Поиск уязвимостей к атакам SQL-injection.	2	2,3
20	Противодействие XSS-атакам.	2	2,3
21	Защита от CSRF.	2	2,3
22	Защита от XXE-атак.	4	2,3
23	Противодействие внедрению.	4	2,3
24	Противодействие DoS-атакам.	4	2,3
25	Финальная комплексная лабораторная работа по безопасности	9	2,3

Примерная тематика самостоятельной учебной работы: 1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы. 2. Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа при самом широком использовании Интернета и других IT-технологий. 3. Проектные формы работы, подготовка сообщений к выступлению на семинарах и конференциях; подготовка рефератов, докладов. 4. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите.	24	
Промежуточная аттестация	6	
Всего	158	

*Внутри каждого раздела указываются соответствующие темы. По каждой теме описывается содержание учебного материала (в дидактических единицах), наименования необходимых лабораторных работ и практических занятий (отдельно по каждому виду), контрольных работ, а также примерная тематика самостоятельной работы. Если предусмотрены курсовые работы (проекты) по дисциплине, описывается примерная тематика. Объем часов определяется по каждой позиции столбца 3 (отмечено звездочкой *). Уровень освоения проставляется напротив дидактических единиц в столбце 4 (отмечено двумя звездочками **).*

Для характеристики уровня освоения учебного материала используются следующие обозначения:

- 1. – ознакомительный (узнавание ранее изученных объектов, свойств);*
- 2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)*
- 3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)*

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требуется наличия лаборатории организации и принципов построения компьютерных систем

Оборудование:

Комплект учебной мебели (16 посадочных мест)

Персональный компьютер обучающегося (13 шт.)

Персональный компьютер преподавателя (1 шт.)

Экран для проектора напольный Projecta (ширина 160 см)

Мультимедийный проектор Epson EB-X8

Сетевое оборудование:

коммутатор D-Link DES-1228 24 порта, коммутатор COMPEX DS2216 16 портов,

шлюз IP-телефонии Cisco SPA8000 8 портов,

6 медиаконвертеров D-Link DMC-920R

Лицензионное программное обеспечение:

Microsoft Windows 7

(14 лицензий WinPro 7 RUS Upgrd OLP NL Acdmс

Торговый посредник: Softline Дата заказа: 2010-10-27

Код лицензии: 47592665 Родительская программа: OPEN 67582704ZZE1210)

Microsoft Office 2007 Professional

(9 лицензий OfficeProPlus 2007 RUS OLP NL Acdmс

Торговый посредник: ООО Рэдком Дата заказа: 2007-12-04

Лицензия: 43136305 Родительская программа: OPEN 63126856ZZE0912;

5 лицензий OfficeProPlus 2007 RUS OLP NL Acdmс

Торговый посредник: ООО Рэдком Дата заказа: 2008-09-19

Код Лицензии: 44544996 Родительская программа: OPEN 63786020ZZE1004)

Kaspersky Endpoint Security 11 для Windows

(Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 250-499 Node 2 year Educational Renewal License

№ лицензии: 1096-181214-111355-563-621

Срок использования ПО: с 2018-12-14 до 2021-03-02

Поставщик (реселлер): BENEФ.ИТ Бенефит, ООО)

АСКОН КОМПАС-3D V12 Университетская лицензия с библиотеками и приложениями (Лицензионное соглашение Кк-10-01408 от 03.12.2010 г. Кол-во копий: 50

Ключ аппаратной защиты HASP HL Net 50 v2 ID 1579998279)

Свободное программное обеспечение:

Libre Office 5.4

Oracle VM VirtualBox

Microsoft Visual C++ 2008 Express Edition

Microsoft Visual C# 2008 Express Edition

Microsoft Visual Basic 2008 Express Edition

Python 3.4

Maxima 5.3.7

Pascal ABC.NET

3.2. Информационное обеспечение обучения.

Основные источники:

1. Ковган, Н.М. Компьютерные сети : учебное пособие : [16+] / Н.М. Ковган. – Минск : РИПО, 2019. – 180 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book_view_red&book_id=599948 (дата обращения: 16.03.2022). – Библиогр. в кн. – ISBN 978-985-503-947-2. – Текст : электронный.

Дополнительные источники:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/viewer/kompyuternye-seti-i-telekommunikacii-marshrutizaciya-v-ip-setyah-v-2-ch-chast-1-452574#page/1> (дата обращения: 16.03.2022).
2. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/viewer/seti-i-telekommunikacii-450234#page/1> (дата обращения: 16.03.2022).

Программное обеспечение и Интернет-ресурсы:

1. ЭБС «Университетская библиотека онлайн». – Режим доступа: <http://biblioclub.ru>.
2. Образовательный портал. Режим доступа: Intuit.ru.
3. ЭБС IPRBooks/ - Режим доступа: <http://www.iprbookshop.ru/>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
<i>ПК 9.8. Осуществлять аудит безопасности веб-приложения в соответствии с регламентами по безопасности</i>	<p><i>Оценка «отлично» - проанализированы источники угроз безопасности; проанализированы методы защиты доступа к данным и защиты кода; предложены и реализованы меры защиты; код сайта и папки проанализированы на предмет наличия вредоносных программ; сделаны выводы о безопасности.</i></p> <p><i>Оценка «хорошо» - проанализированы источники угроз безопасности; предложены и реализованы меры защиты; код сайта и папки проанализированы на предмет наличия вредоносных программ; сделаны выводы о безопасности.</i></p> <p><i>Оценка «удовлетворительно» - проанализированы источники угроз безопасности; предложены и реализованы меры защиты; код сайта и папки проанализированы на предмет наличия</i></p>	<p><i>Экзамен/зачет в форме собеседования: практическое задание по обеспечению безопасности функционирования веб-приложения. Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ во время учебной/производственной</i></p>

	<i>вредоносных программ.</i>	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<p>— обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;</p> <p>- адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач</p>	Экспертное наблюдение за выполнением работ
ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	<p>- демонстрация ответственности за принятые решения</p> <p>- обоснованность самоанализа и коррекция результатов собственной работы;</p>	

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	<ul style="list-style-type: none"> - взаимодействовать с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных) 	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Демонстрировать грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	<ul style="list-style-type: none"> - соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, 	

<p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.</p>	<p>- эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности</p>	
<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.</p>	<p>- эффективность использовать средств физической культуры для сохранения и укрепления здоровья при выполнении профессиональной деятельности.</p>	
<p>ОК 09. Использовать информационные технологии в профессиональной деятельности.</p>	<p>- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;</p>	

<p>ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.</p>	<p>- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.</p>	
--	---	--