МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Защита информации в сети Интернет

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 66,35
самостоятельная работа 50,65
часов на контроль 27

Виды контроля в семестрах:
экзамены 9

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	66,35	66,35	66,35	66,35
Контактная работа	66,35	66,35	66,35	66,35
Сам. работа	50,65	50,65	50,65	50,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Подготовка специалистов в сфере защиты информации, передаваемой посредством сети "Интернет", ознакомление с основными понятиями безопасности, правовой защиты информации, подготовка к организации защиты компьютерных систем и сетей от несанкционированного доступа к хранимой информации. Задачи дисциплины: - изучение способов правовой защиты информации, распространяемой посредством сети "Интернет"; - изучение способов организационной защиты информации, распространяемой посредством сети "Интернет"; - изучение способов технической защиты информации, распространяемой посредством сети "Интернет"; - оценка эффективности существующих средств защиты; - изучение механизма организации централизованной антивирусной защиты.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Биометрические технологии контроля доступа
2.1.2	Практикум по решению эксплуатационных задач профессиональной деятельности
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-5: Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их работоспособность при возникновении нештатных ситуаций	
Знать:	
Уровень 1	методы и средства контроля и управления доступом при обеспечении безопасности автоматизированных систем; политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; современные методы предотвращения несанкционированного доступа (НСД) к объектам информатизации, основанные на биометрических технологиях распознавания личности
Уровень 2	принципы организации и структуру систем защиты программного обеспечения автоматизированных систем; средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; принципы формирования политики информационной безопасности автоматизированной системы; основные направления защиты информации в информационно- телекоммуникационных системах в соответствии с законодательством Российской Федерации
Уровень 3	современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; архитектуру автоматизированной системы управления технологическим процессом (АСУ ТП), модели промышленных систем автоматизации, сетевые технологии, используемые в современных АСУ ТП, понятия функциональной и информационной безопасности, их взаимосвязь и противоречия; основы организации своевременной и полноценной обработки инцидентов безопасности
Уметь:	
Уровень 1	использовать устройства контроля и управления доступом при обеспечении безопасности автоматизированных систем; применять политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; использовать устройства контроля доступа на основе биометрических характеристик человека
Уровень 2	регистрировать события, связанные с защитой информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять комплекс мер (правила, процедуры, практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; проводить оценку угроз безопасности информационно- телекоммуникационной системы, подключенной к сети Интернет;
Уровень 3	реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; работать со средствами обеспечения безопасности в системах промышленной автоматизации; настраивать межсетевой экран для обеспечения защиты периметра сети, для обеспечения сегментации внутренней сети
Владеть:	
Уровень 1	навыком использования систем контроля и управления доступом для управления процессами обеспечения

	безопасности автоматизированных систем; навыком применения инструментов администрирования подсистем информационной безопасности автоматизированной системы; навыком использования специальных средств биометрической идентификации личности для управления процессами обеспечения безопасности автоматизированных систем
Уровень 2	навыком обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы; навыком обеспечения работоспособности автоматизированных систем при возникновении нештатных ситуаций; навыком разработки частных политик информационной безопасности автоматизированных систем
Уровень 3	навыком использования антивирусного программного обеспечения для защиты информации в информационно- телекоммуникационных системах, подключенных к сети Интернет; анализом инцидентов кибербезопасности в современных промышленных системах автоматизации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основные направления защиты информации в информационно-телекоммуникационных системах в соответствии с законодательством Российской Федерации;
3.1.2	современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет
3.2	**Уметь:**
3.2.1	проводить оценку угроз безопасности информационно-телекоммуникационной системы, подключенной к сети Интернет;
3.2.2	реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет
3.3	**Владеть:**
3.3.1	использования антивирусного программного обеспечения для защиты информации в информационно-телекоммуникационных системах, подключенных к сети Интернет

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Введение, Политика доступа						
1.1	Введение, история WEB, устройство браузера /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
1.2	HTTP-протокол, DNS /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
1.3	HTTP-сессия. Понятия о Cookies /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
1.4	Политика одинакового происхождения. Подделка межсайтовых запросов /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
1.5	Политика одинакового происхождения. Исключения /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
1.6	Установка git bash /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
1.7	Основы работы с bash /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
1.8	Регулярные выражения. Принципы защиты и нападения /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
1.9	Сбор информации с использованием bash /Пр/	9	2	ПК-5	Л1.1 Л1.2	1	
1.10	Обработка данных /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
	Раздел 2. Атаки в сети "Интернет"						
2.1	Анализ данных /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
2.2	Мониторинг журналов в режиме реального времени /Пр/	9	2	ПК-5	Л1.1 Л1.2	1	
2.3	Мониторинг сети /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
2.4	Контроль файловой системы /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
2.5	Межсайтовый скриптинг /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
2.6	Атаки типа XSS /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
2.7	Противодействие атакам XSS /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
2.8	Приватность в сети "Интернет" /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
2.9	Самостоятельная работа /Ср/	9	20,65	ПК-5	Л1.1 Л1.2	0	

	Раздел 3. Архитектура браузера						
3.1	Отпечаток браузера (fingerprints) /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
3.2	Атаки типа UI DoS, фишинг и др. /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
3.3	Безопасность пользовательского интерфейса /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
3.4	Протокол защиты транспортного уровня /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
3.5	HSTS HPKP /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
3.6	Веб - Аутентификация /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
3.7	Архитектура браузера /Лек/	9	2	ПК-5	Л1.1 Л1.2	0	
3.8	Добавление записей в журнал /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
3.9	Мониторинг доступности системы /Пр/	9	2	ПК-5	Л1.1 Л1.2	1	
3.10	Аудит учетных записей /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
3.11	Разведка, обфускация сценария /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
3.12	Fuzzer, backdor /Пр/	9	2	ПК-5	Л1.1 Л1.2	1	
3.13	Пользователи, группы и права доступа /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
3.14	Защита информации с использованием антивирусного программного обеспечения /Пр/	9	2	ПК-5	Л1.1 Л1.2	0	
3.15	Самостоятельная работа /Ср/	9	30	ПК-5	Л1.1 Л1.2	0	
3.16	Экзамен /ИВКР/	9	2,35	ПК-5	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

1. В чем заключаются основные этапы развития Всемирной паутины (Web)?
2. Как изменялась архитектура веб-приложений от Web 1.0 до Web 3.0?
3. Какие функции выполняет браузер при открытии веб-страницы?
4. Какова архитектура современного браузера?
5. Какие основные компоненты входят в состав браузера и за что они отвечают?
6. Что такое движок рендеринга и какие виды движков существуют?
7. Как работает процесс загрузки и отображения веб-страницы в браузере?
8. Что такое HTTP и какие версии протокола используются сегодня?
9. Какие основные методы HTTP-протокола вы знаете и в чем их отличие?
10. Что означает заголовок HTTP-запроса и какие типы заголовков бывают?
11. Как осуществляется установление HTTP-сессии между клиентом и сервером?
12. Что такое DNS и как происходит разрешение доменного имени в IP-адрес?
13. Какую роль играет кэширование в работе HTTP и DNS?
14. Что такое cookies и для чего они используются в HTTP-сессиях?
15. Чем отличаются session cookies от persistent cookies?
16. Что такое HTTP-only и Secure-флаги для cookies?
17. В чем состоит политика одинакового происхождения (Same-Origin Policy)?
18. Почему политика одинакового происхождения важна для безопасности?
19. Какие существуют исключения из политики одинакового происхождения?
20. Что такое подделка межсайтовых запросов (CSRF) и как она работает?
21. Какие механизмы защиты от CSRF вы знаете?
22. Что такое межсайтовый скриптинг (XSS)?
23. Чем отличается отражённый XSS от сохранённого и DOM-based XSS?
24. Какие последствия могут возникнуть в результате XSS-атаки?
25. Как можно предотвратить XSS-атаки на веб-приложение?
26. Что такое Content Security Policy (CSP) и как она защищает от XSS?
27. Какие ещё существуют методы борьбы с XSS кроме CSP?
28. Как обеспечивается приватность пользователей в интернете?
29. Что такое браузерный отпечаток (browser fingerprinting)?
30. Какие параметры могут использоваться для создания отпечатка браузера?
31. Почему browser fingerprinting может быть угрозой приватности?
32. Какие методы существуют для снижения точности отпечатка браузера?
33. Что такое атака UI DoS и как она влияет на работу интерфейса?
34. В чем заключается суть фишинговой атаки в интернете?
35. Какие признаки могут указывать на фишинговый сайт?
36. Какие способы используют злоумышленники для проведения фишинга?
37. Что такое clickjacking и как от него защититься?

38. Как работает защита пользовательского интерфейса в браузере?
39. Что такое протокол TLS и какую роль он играет в безопасности данных?
40. В чем отличие между HTTP и HTTPS?
41. Как работает TLS handshake при установке безопасного соединения?
42. Что такое сертификат безопасности сайта и как он проверяется браузером?
43. В чем состоит роль центра сертификации (CA) в TLS?
44. Что такое HSTS и как он усиливает безопасность HTTPS-соединений?
45. Что означает механизм HPKP и почему он считается устаревшим?
46. Какие риски могут возникнуть при неправильной настройке HSTS?
47. Как работает двухфакторная аутентификация в вебе?
48. Какие существуют современные методы веб-аутентификации?
49. Что такое WebAuthn и как он используется в браузерах?
50. Как реализуется безопасное хранение и передача паролей в веб-приложениях?
51. Что такое OAuth и как он используется в авторизации?
52. Каковы риски использования токенов доступа и способы их защиты?
53. Какие принципы лежат в основе безопасности веб-приложений?
54. Как можно контролировать доступ к ресурсам на основе ролей и прав?
55. Что такое CORS и как он связан с политикой одинакового происхождения?
56. В чем отличие preflight-запросов от обычных CORS-запросов?
57. Как браузер защищает пользователя от подозрительных переходов по ссылкам?
58. Какие ограничения накладываются на выполнение JavaScript в браузере?
59. Что такое sandbox-режим в контексте безопасности браузера?
60. Как работают расширения браузера и какие риски они могут представлять?
61. Какие инструменты доступны разработчику для диагностики сетевой безопасности?
62. Какую роль играют заголовки безопасности, такие как X-Frame-Options?
63. Что такое Referrer Policy и зачем она используется?
64. Как влияет автозаполнение форм на безопасность веб-приложения?
65. Какие меры могут снизить риск утечки данных через адресную строку?
66. Как браузеры реализуют защиту от вредоносных загрузок?
67. Что такое сертификат с EV (Extended Validation) и чем он отличается от DV?
68. Как действуют атаки человек посередине (MITM) и как от них защищаться?
69. Как можно обнаружить атаку на транспортном уровне при работе с сайтом?
70. Какие браузеры применяют дополнительные механизмы защиты (например, Safe Browsing)?
71. Какие особенности имеют мобильные браузеры в контексте безопасности?
72. Что означает происхождение (origin) в URL и как оно влияет на доступ к данным?
73. Как различаются localStorage и sessionStorage с точки зрения безопасности?
74. Как обеспечить защиту от утечки данных через JavaScript-интерфейсы?
75. Какие уязвимости могут возникнуть при использовании внешних библиотек?
76. Как безопасно интегрировать сторонние скрипты в веб-приложение?
77. Как реализуются механизмы автоматического выхода из системы при простое?
78. Что такое secure context и какие преимущества он даёт?
79. В чем заключается важность обновлений браузеров с точки зрения безопасности?
80. Как влияет архитектура браузера на его устойчивость к атакам?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Защита информации в сети Интернет" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 9 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Ковалева Н. Н., Брянцев И. И., Брянцева О. В., Варламова Е. В., Ересько П. В., Жирнова Н. А., Изотова В. Ф., Ильгова Е. В., Сергеева Е. Ю., Солдаткина О. Л., Тугушева Ю. М., Холодная Е. В., Чайковский Д. С.	Информационное право: учебник для вузов	Москва: Юрайт, 2024
Л1.2	Чурилов А. Ю.	Право новых технологий: учебное пособие для вузов	Москва: Юрайт, 2024
6.3.1 Перечень программного обеспечения			
6.3.1.1	Office Professional Plus 2019		
6.3.1.2	Windows 10		
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.	
6.3.2 Перечень информационных справочных систем			
6.3.2.1	База данных научных электронных журналов "eLibrary"		
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"		
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")		

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие	

		требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления	

		доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Защита информации в сети Интернет" представлены в Приложении 2 и включают в себя:

1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.