ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Технические способы защиты информации

Код модуля	Модуль
1144713	Информационное обеспечение профессиональной деятельности

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Крылов Виктор Гаврилович	без ученой степени, без ученого звания	Старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности
2	Шкурко Валентина Евгеньевна		старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности

Согласовано:

Управление образовательных программ И.Ю. Русакова

Авторы:

- **Шкурко Валентина Евгеньевна, старший преподаватель, региональной экономики, инновационного предпринимательства и безопасности**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Технические способы защиты информации

1.	**Объем дисциплины в зачетных единицах**	3	
2.	**Виды аудиторных занятий**	Лекции Практические/семинарские занятия	
3.	**Промежуточная аттестация**	Зачет	
4.	**Текущая аттестация**	Контрольная работа	1
		Домашняя работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Технические способы защиты информации

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ПК-4 -Способен обеспечивать условия защиты ресурсов организации от внешних и внутренних угроз экономической безопасности	З-1 - Знать понятия внешних и внутренних угроз экономической безопасности З-2 - Знать методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности П-1 - Владеть методиками защиты ресурсов организации от внешних и внутренних угроз экономической безопасности У-1 - Уметь применять методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	7,16	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	7,16	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -		

Промежуточная аттестация по онлайн-занятиям – **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям –**

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	Шкала оценивания		
		Традиционная характеристика уровня		Качественная характеристика уровня
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. Угрозы в информационных сетях
2. Безопасность операционных систем
3. Безопасность программного обеспечения
4. Способы и средства защиты информации
5. Основы кодирования информации
6. Математические основы криптографии
7. Криптографические методы защиты информации
8. Сетевые средства защиты информации
9. Управление рисками информационной безопасности

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Введение. Угрозы в информационных сетях
2. Безопасность операционных систем и программного обеспечения
3. Способы и средства защиты информации
4. Криптографические методы защиты информации
5. Сетевые средства защиты информации
6. Управление рисками информационной безопасности

Примерные задания

Ответить на вопросы контрольной работы:

1. Основные понятия. Информационная безопасность как отрасль. Роль и место информационной безопасности в профессиональной деятельности. Виды угроз. Внутренние и внешние источники угроз. Организационно-правовое обеспечение информационной безопасности. Современное состояние и перспективы информационной безопасности. Государственное регулирование в сфере ИБ. Международные нормы и стандарты по ИБ.

Нарушения конфиденциальности, достоверности, целостности, доступности. Классификация угроз информации и информационным технологиям. Субъекты ИБ. Угрозы доступности, целостности и конфиденциальности информации. Категории атак на информационные системы. Сценарий типовой атаки на информационную систему. Локальные атаки. Удаленные атаки. Атаки на поток данных. Атаки на пользователя (социальная инженерия).

2. Средства защиты информации и обеспечения безопасности информационных технологий. Определение понятия «уязвимость программного обеспечения». Обзор методик тестирования и выявления уязвимостей. Организационные меры по обеспечению безопасности использования программного обеспечения.

Средства идентификации и аутентификации пользователей. Группы безопасности. Политика регистрации событий. Шифрование. Корпоративная безопасность. Службы сертификации. Встроенный Firewall. Политика ограничения используемых приложений. Средства электронной цифровой подписи. Защита от макровирусов. Централизованные средства управления. Компьютерные вирусы и антивирусные средства. Антивирусное программное обеспечение (АВПО). Обзор технологий и производителей АВПО. Практика применения АВПО. Эшелонированные системы антивирусной защиты. Атаки на АВПО.

3. Основные способы и средства защиты информации. Системы защиты информации.

Основы криптографии. Терминология и основные понятия криптологии. Основные аспекты криптографии. Основные аспекты криптоанализа. Шеноновские модели криптографии. Теоретико-информационные оценки стойкости симметричных

криптосистем. Криптографические методы защиты информации. Компьютерные вирусы и антивирусные программы

4. Основные принципы кодирования. Основы экономного кодирования. Введение в теорию кодирования. Основы экономного кодирования. Сжатие без потерь информации. Сжатие с потерями информации. Кодеры, основанные на системе сжатия без потерь информации. Основные методы побуквенного кодирования. Код Хаффмана. Код Шеннона. Код Шеннона-Фано. Код Гильбера-Мура. Помехоустойчивое кодирование. Коды с обнаружением ошибок. Коды с исправлением ошибок. Линейные блоковые коды. Коды Хэмминга. Циклические коды.

Псевдослучайные последовательности. Равномерно распределенная случайная последовательность. Алго-ритмы генерации псевдослучайных последовательно-стей. Конгруэнтные генераторы. Линейные и мульти-пликативные конгруэнтные генераторы. Нелинейные конгруэнтные генераторы. Квадратичные конгруэнтные генераторы. Генератор Эйхенауэра - Лена с обращени-ем. Конгруэнтный генератор, использующий умноже-ние с переносом. Рекуренты в конечном поле. После-довательности, порождаемые линейными регистрами сдвига с обратной связью. Генераторы Фибонначи. Криптостойкие генераторы на основе односторонних функций. Криптостойкие генераторы, основанные на проблемах теории чисел. Методы «улучшения» эле-ментарных псевдослучайных последовательностей. Комбинирование алгоритмов генерации методом Ма-кларена - Марсальи. Комбинирование LFSR-генераторов. Комбинирование с помощью псевдослу-чайного прореживания. Конгруэнтный генератор со случайными параметрами.

Тестирование чисел на простоту и построение боль-ших простых чисел. Метод пробных делений. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Тест Соловея - Штрассена. Тест Ле-манна. Тест Рабина - Миллера. Полиномиальный тест распознавания простоты. Тест Конягина - Померанса. Метод Михалеску.

Теория сравнения Арифметика вычетов. Функция Эй-лера. Сравнение первой степени. Решение сравнения первой степени с использованием алгоритма Евклида. Решение сравнения первой степени с использованием расширенного алгоритма Евклида. Решение сравнения способ Эйлера. Первообразные корни. Дискретные ло-гарифмы в конечном поле. Разложение на множители (факторизация) Метод Ферма. - факторизация Поллар-да. Метод -Полларда. Метод Шермана-Лемана. Метод Ленстры.

Примеры систем шифрования, основанные на проблемах теории чисел Система шифрования RSA. Система шифрования Диффи-Хеллмана.

Шифрование (алгоритмы шифрования). Электронно-цифровая подпись (практика применения). Хэширование. Средства инфраструктуры открытых ключей. Атаки на криптографическую защиту

5. Технологии защиты вычислительных сетей. Обзор сетевых средств защиты информации (межсетевые экраны, виртуальные частные сети, шифрование, обнаружение вторжений). Методы применения сетевых СЗИ. Основы безопасной работы в сети Интернет. Безопасность электронной коммерции. Безопасность беспроводных технологий. Стандарты безопасности беспроводных сетей. Меры защиты от различного вида атак. Технологии защиты Wi-Fi-сетей

6. Соотношение угроз, уязвимостей и ущерба. Этапы управления рисками. Методики оценки рисков. Методы снижения рисков. Организация системы информационной

безопасности предприятия. Построение системы управления информационной безопасности (СУИБ) предприятия. Общие правила безопасности предприятия. Архитектура СУИБ. Настройки основных компонентов СУИБ. Корпоративные политики информационной безопасности.

Стандарты общего назначения, стандарты по криптографической защите. Стандарты, руководящие методические материалы информационной безопасности

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. 1. Криптографические средства защиты информации в стандарте GSM и их стойкость. 2. Исследование алгоритма поточного шифрования RC4. 3. Особенности применения цифровой подписи вслепую в протоколах электронного тайного голосования. 4. Новые американские стандарты режимов шифрования с аутентификацией. 5. Схемы криптосистем на основе парных отображений. 6. Методы эффективной реализации схем электронной цифровой подписи на основе группы точек эллиптических кривых. 7. Возможности преобразования отечественного стандарта цифровой подписи в схему цифровой подписи вслепую. 8. Сравнение криптографических средств различных протоколов мобильных платежей. 9. Исследование свойств подстановок на двоичных векторах при малых размерностях и их применение при построении узлов алгоритмов шифрования. 10. Решение проблемы повторной траты (https://ru.wikipedia.org/wiki/Двойное_расходование) криптографическими методами в схемах электронных платежей. 11. Анализ подходов к ролевому управлению доступом 12. Аудит безопасности информационной системы с использованием теста на проникновение 13. Аудит информационной безопасности 14. Выявление нарушений законодательства в сети Интернет 15. Выявление признаков, определяющих группы по интересам 16. Шифрование информации. Цель, место, применение 17. Защита информации предприятия от утечки по техническим каналам 18. Защита конфиденциальной информации на предприятиях по формам собственности 19. Защита персональных данных на предприятиях 20. Криптографические методы защиты информации 21. Криптоанализ алгоритмов: Hughes XPD/KPD, Nanoteq 22. Криптоанализ генераторов: «стоп-пошёл» Both-Piper, DNRSG, Геффа, Дженнингса,каскад Голлманна 23. Криптоанализ потоковых шифров: Gifford, A5, LFSR 24. Защита информационной и интеллектуальной собственности 25. Информационные угрозы предпринимательству 26. Исследование проблем информационной безопасности и защита информации территориально разнесенных центров обработки данных 27. Исследование проблем информационной безопасности мобильного доступа 28. Исследование тенденций развития межсетевых экранов прикладного уровня 29. Линейная сложность генераторов на базе LFSR 30. Место DLP-систем (предотвращение утечек, Data Leak Prevention) в современной структуре обеспечения информационной безопасности автоматизированной информационной системы 31. Оценка рисков информационной безопасности при обеспечении доступа в Интернет 32. Защита информации в облачных сервисах 33. Организационно-правовое обеспечение информационной безопасности бизнеса 34. Организационно-правовые меры обеспечения режима защиты информации 35. Организация информационной безопасности в коммерческом секторе 36. Организация

системы безопасности корпоративных информационных систем 37. Защита информации и информационная безопасность финансовых организаций 38. Оценка экономической эффективности системы защиты информации в организации 39. Применение (не)квалифицированной электронной подписи. 40. Анализ деятельности Роскомнадзора в контроле Интернета 41. Защита информации и обеспечение информационной безопасности инфраструктуры центр обработки данных 42. Разработка рекомендаций по повышению эффективности защиты информации в кор-поративной сети передачи данных 43. Разработка технического задания на подсистему обеспечения информационной без-опасности базовой инфраструктуры катострофо-устойчивости 44. Разработка эскизного проекта системы обеспечения информационной безопасности заданного объекта информатизации 45. Оценка уровня угроз при распространении информации в социальных сетях 46. Регулирование деятельности с применением криптографии в России 47. Информационная безопасность и защита информации в сфере электронной торговли 48. Современные DDoS-атаки (Distributed Denial of Service, распределённая атака типа отказ в обслуживании) как угроза для бизнеса в Интернете: методы и средства защиты 49. Проблемы авторизации субъекта доступа 50. Тенденции развития отечественных средств электронной подписи 51. Анализ инцидентов информационной безопасности в организации 52. Структурирование массива событий и инцидентов информационной безопасности с использованием специализированного программного обеспечения 53. Методы разграничения доступа в компьютерных системах и их правовая регламентация 54. Управление инцидентами информационной безопасности на предприятии 55. Техническое регулирование информационной безопасности в России и за рубежом 56. Обеспечение информационной безопасности и защита информации на предприятиях малого и среднего бизнеса 57. Организационно-технические мероприятия по обеспечению информационной безопасности

Примерные задания

Написать реферат и сделать доклад на 3-5 минут по одной из выбранных тем.

LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Зачет

Список примерных вопросов

1. 1. Концепция информационной безопасности. 2. Виды угроз. Внутренние и внешние источники угроз. 3. Организационно-правовое обеспечение информационной безопасности. 4. Угрозы в информационных системах. 5. Способы защиты информации. 6. Средства защиты информации. 7. Компьютерные вирусы и антивирусные программы. 8. Государственные стандарты по информационной безопасности. 9. Понятие информационной безопасности. Угрозы. Механизмы анализа угроз. Инстру-ментарий построения рубежей. 10. Основы криптографии. Шифрование и кодирование. Общие принципы и модели. 11. Защита от несанкционированного доступа. 12. Простые шифры. Шифр простой замены. Шифр Цезаря (шифр сдвига, код Цезаря, сдвиг Цезаря). 13. Шифр вертикальной перестановки (перестановочный шифр, шифрограмма по вертика-лям). 14. Гаммирование (метод симметричного шифрования). 15. Методы расшифровки зашифрованной информации. Основные способы криптоанализа простых шифров. 16.

Основные методы криптоанализа. Атака на основе шифротекста, открытых текстов и соответствующих шифротекстов, подобранного открытого текста, адаптивно подобранного открытого текста. 17. Дополнительные методы криптоанализа. Атака на основе подобранного шифротекста, подобранного ключа. Бандитский криптоанализ 18. Симметричные криптосистемы. Схема, сеть Фейстеля (Horst Feistel, Feistel network, Feistel cipher). Стандарты блочного шифрования. Федеральный стандарт DES. 19. Симметричные криптосистемы. Алгоритм шифрования ГОСТ 28147-89 (Магма), ГОСТ Р 34.12-2015 (Кузнечик). режимы шифрования и гаммирования. 20. Симметричные криптосистемы. Алгоритм блочного шифрования Rijndael - Advanced Encryption Standard (AES). 21. Атаки на блочные шифры. Дифференциальный криптоанализ. Дифференциальный криптоанализ на основе отказов устройства. 22. Атаки на блочные шифры. Линейный криптоанализ. Силовая атака на основе распре-деленных вычислений. 23. Поточные шифры. Регистры сдвига с обратной связью. Алгоритм поточного шифрова-ния RC4 (Rivest cipher 4, Ron's code; ARC4, ARCFOUR). 24. Основные теоремы теории чисел. Проверка числа на простоту. Эффективные алгорит-мы возведения в степень. 25. Криптосистема RSA (Rivest-Shamir-Adleman — криптографический алгоритм с откры-тым ключом). Устройство RSA. Эффективность реализации. Криптостойкость RSA. 26. Атаки на криптосистему RSA. Атака на основе выбранного шифр текста. Атака на ос-нове общего RSA модуля. Раскрытие малого показателя шифрования. 27. Криптосистема Эль-Гамаля (Elgamal). Вычисление и проверка подписи. Шифрование и дешифрование. Эффективность реализации. 28. Метод экспоненциального ключевого обмена Диффи-Хелмана. Протокол ключевого обмена для нескольких участников. 29. Хеш-функции. Понятие хеш-функции. Основные свойства односторонних функций. MD4 (Message Digest 4), RFC 1186 (The MD4 Message Digest Algorithm). 30. Цифровая подпись. Понятие цифровой подписи. Основные принципы и отличия от ре-альной подписи. Алгоритмы цифровой подписи - ГОСТ Р 34.10-2012. DSS (Digital Signature Standard). 31. Закон об электронной цифровой подписи в России. Удостоверяющие центры. 32. Протоколы генерации ключей. Случайные ключи. Протоколы распределения ключей. 33. Разделение секрета. Схема разделения секрета Шамира. 34. Применение помехоустойчивых кодов в криптографии. Недвоичные циклические коды Рида-Соломона(Reed–Solomon codes). 35. Верифицируемое разделение секрета. 36. «Шарады» с временным замком (Time-lock puzzles and timed-release Crypto). Построе-ние «шарад» с временным замком. Решение «Шарады» 37. Квантовая криптография - основанная на принципах квантовой физики. Квантовый протокол распределения ключей. Распределение ключей в оптических сетях. 38. Криптографические протоколы: обеспечение различных режимов аутентификации; генерация, распределение и согласование криптографических ключей; защита взаимодействий участников; разделение ответственности между участниками. 39. Доказательство принадлежности (Zero-knowledge proof). Доказательство при отказе отправителя. Доказательство при отказе получателя. 40. Нормативно-правовое обеспечение информационной безопасности. 41. Классификация секретной информации в России. Служебная, коммерческая и государ-ственная тайны. 42. Законы РФ: «Информации, информатизации и защите информации»; Закон о персо-нальных данных; ... 43. Стандарты ИБ: ISO/IEC 15408; руководящие документы ФСТЭК; Оранжевая книга (Критерии определения безопасности компьютерных систем - Trusted Computer System Evaluation Criteria; Радужная серия). 44. Политика безопасности. Уровень гарантированности. Классы безопасности. Безопас-ность распределенных систем.

Рекомендации X.800. 45. Роли и ответственности субъектов информационного пространства. Принцип распре-деления ответственности. Матрица распределения доступа для сотрудников организа-ции. 46. Понятие управления рисками. Качественные и количественные методики оценки рис-ков. Количественная модель рисков QRM (Quantitative Risk Model). Оценки по конфи-денциальности информации. 47. Политика информационной безопасности. Цели и задачи организации. Взаимодей-ствие между субъектами. Правила безопасности. 48. Политика информационной безопасности для локальной вычислительной сети.

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Профессиональное воспитание	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-4	З-1 З-2 У-1 П-1	Зачет Практические/семинарские занятия