ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ
Технологии и средства обеспечения информационной безопасности

Код модуля	**Модуль**
1158780	Информационное обеспечение автоматизированных систем управления технологическими процессами в металлургии

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Куделин Сергей Петрович	кандидат технических наук, без ученого звания	Доцент	теплофизики и информатики в металлургии

Согласовано:

Управление образовательных программ Ю.В. Коновалова

Авторы:

- **Куделин Сергей Петрович, Доцент, теплофизики и информатики в металлургии**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Технологии и средства обеспечения информационной безопасности

1.	**Объем дисциплины в зачетных единицах**	6	
2.	**Виды аудиторных занятий**	Лекции Практические/семинарские занятия	
3.	**Промежуточная аттестация**	Зачет	
4.	**Текущая аттестация**	Контрольная работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Технологии и средства обеспечения информационной безопасности

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-2 -Способность разрабатывать, вводить в эксплуатацию, обслуживать, модифицировать базы данных и другие хранилища информации.	З-3 - Сформулировать основные технологии и средства обеспечения целостности и доступности данных в хранилищах информации. З-4 - Перечислить основные технологии и средства защиты машинных носителей информации, технических средств и информационной системы. П-2 - Предлагать варианты концепций системы защиты информации в базах данных при их эксплуатации. У-3 - Определять меры обеспечения информационной безопасности при эксплуатации баз данных.	Зачет Контрольная работа Лекции

	У-4 - Оценивать эффективность средств защиты баз данных и хранилищ информации при их эксплуатации.	
УК-7 -Способен обрабатывать, анализировать, передавать данные и информацию с использованием цифровых средств для эффективного решения поставленных задач с учетом требований информационной безопасности	З-1 - Сделать обзор угроз информационной безопасности, основных принципов организации безопасной работы в информационных системах и в сети интернет З-2 - Описать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством З-3 - Сделать обзор современных цифровых средств и технологий, используемых для обработки, анализа и передачи данных при решении поставленных задач П-1 - Обосновать выбор технических и программных средств защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации П-2 - Решать поставленные задачи, используя эффективные цифровые средства и средства информационной безопасности У-1 - Определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты персональных данных и данных организации от мошенников и вредоносного ПО У-2 - Выбирать современные цифровые средства и технологии для обработки, анализа и передачи данных с учетом поставленных задач	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 – 0.60		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Активная работа на лекциях	3,16	*50*
Контрольная работа	3,8	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.60		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.40**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.40		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практические работы	3,16	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1.00		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0.00**		
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. Методические документы ФСТЭК и ФСБ России по защите информации.
2. Проблематика защиты информации обрабатываемой в АСУ ТП.
3. Нормативное обеспечение системе защиты информации в АСУ ТП.
4. Определение целей и задач защиты информации в автоматизированной системе управления.
5. Классы защищенности автоматизированной системы управления.
6. Определение угроз безопасности информации в АСУ ТП.
7. Требования к мерам защиты информации.

8. Определение видов и типов средств защиты информации, обеспечивающих реализацию технических мер защиты информации.

9. Контроль (мониторинг) за обеспечением уровня защищенности автоматизированной системы управления.

LMS-платформа

1. https://elearn.urfu.ru/course/view.php?id=4637

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. Основные понятия информационной безопасности.
2. Информационные технологии и необходимость ИБ.
3. Система защиты информации и ее структуры.
4. Экономическая информация как товар и объект безопасности.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компании.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.
17. Субъекты и причины совершения компьютерных преступлений.
18. Вредоносные программы, их виды.
19. История компьютерных вирусов и современность.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Государственное регулирование информационной безопасности в РФ.
22. Оценка эффективности инвестиций в информационную безопасность.
23. Доктрина информационной безопасности России.
24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
25. Уголовно-правовой контроль над компьютерной преступностью в РФ.
26. Политика безопасности и ее принципы.
27. Фрагментарный и системный подход к защите информации.
28. Методы и средства защиты информации.

29. Организационное обеспечение ИБ.

30. Организация конфиденциального делопроизводства.

31. Криптографические методы защиты информации.

32. Инженерно-техническое обеспечение компьютерной безопасности.

33. Организационно-правовой статус службы безопасности.

34. Защита информации в Интернете.

35. Электронная почта и ее защита.

36. Защита от компьютерных вирусов.

37. "Больные" мобильники и их «лечение».

38. Популярные антивирусные программы и их классификация.

39. Этапы и освоение защиты информации экономических объектов.

Примерные задания

Студенту предлагается ответить на вопросы письменно по выбранной теме. Необходимо изучить, проанализировать и систематизировать лекционный материал и рекомендованные учебные пособия, оформить работу в соответствии с требованиями и в установленные сроки. Контрольная работа пишется строгим научным языком, не допускается использование бытовых речевых оборотов, разговорной речи, а также дословное переписывание материала из литературных источников. По мере необходимости текстовый материал дополняется графиками, формулами и таблицами.

LMS-платформа

1. https://elearn.urfu.ru/course/view.php?id=4637

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

5.3.1. Зачет

Список примерных вопросов

1. Информационное оружие и информационные войны.

2. Международное сотрудничество в борьбе с киберпреступностью.

3. Стратегии, доктрины и основные направления информационной безопасности РФ.

4. Федеральные законы и постановления правительства и президента по защите информации.

5. Методические документы ФСТЭК и ФСБ России.

6. Автоматизированные системы управления технологическими процессами.

7. Промышленные протоколы.

8. Описание «типового» предприятия.

9. Проблематика защиты информации, обрабатываемой в АСУ ТП.

10. Методология оценки ущерба и рисков нарушения целостности, доступности и конфиденциальности информации.

11. Нормативные акты.

12. Международные стандарты и лучшие практики защиты информации.

13. Концепции информационной безопасности в АСУ ТП.

14. Формирование требований к защите информации в АСУ ТП.

15. Нормативное обеспечение системе защиты информации в АСУ ТП.

16. Определение целей и задач защиты информации в автоматизированной системе управления.

17. Классы защищенности автоматизированной системы управления.

18. Требование к классам защищенности.

19. Уровень значимости (критичности) обрабатываемой в ней информации.

20. Степень возможного ущерба от нарушения целостности, доступности и конфиденциальности информации.

21. Определяющие уровни защищенности автоматизированной системы управления.

22. Оценка возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей.

23. Анализ возможных уязвимостей автоматизированной системы управления.

24. Анализ возможных способов (сценариев) реализации угроз безопасности информации и последствий от них.

25. Модель угроз безопасности информации.

26. Идентификация и аутентификация субъектов доступа и объектов доступа.

27. Управление доступом субъектов доступа к объектам доступа.

28. Ограничение программной среды.

29. Защита машинных носителей информации.

30. Регистрация событий безопасности.

31. Антивирусная защита.

32. Обнаружение вторжений.

33. Контроль (анализ) защищенности информации.

34. Целостность автоматизированной системы управления и информации.

35. Доступность технических средств и информации.

36. Защита среды виртуализации.

37. Защита технических средств и оборудования.

38. Защита автоматизированной системы и ее компонентов.

LMS-платформа

1. https://elearn.urfu.ru/course/view.php?id=4637

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.