ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Безопасность информационных технологий и систем

Код модуля
1152564

Модуль
Программно-технологическая безопасность информационных систем

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 Е.А. Смирнова

Авторы:

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

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Безопасность информационных технологий и систем

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Безопасность информационных технологий и систем

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-20 -Способность к организации ИТ-инфраструктуры, администрированию инфокоммуникационной системы и управлению информационной безопасностью	З-6 - Перечислить способы и средства обеспечения информационной безопасности инфокоммуникационной системы организации. П-6 - Осуществить выбор средств администрирования сетевых устройств и прикладного программного обеспечения инфокоммуникационной системы организации с учетом требований информационной безопасности У-6 - Обоснованно выбирать способы и средства обеспечения информационной безопасности инфокоммуникационной системы организации	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	8,16	*50*
Активность работы на лекциях	8,16	*50*
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**
Отчет по практическим работам	8,16	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 –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**

Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**		

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. Описание угроз ИТ объекта из списка банка данных рисков ФСТЭК (по угрозам списка ФСТЭК).
2. Требования по обеспечению информационной безопасности КИС предприятия (список предприятий).
3. Обработка персональных данных в организации.
4. Обеспечение безопасности персональных данных в организации.

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. Информационная безопасность государства.
2. Информационная система как объект защиты безопасность в internet.
3. Принципы построения систем защиты.
4. Законодательная, нормативно--методическая и научная база функционирования систем защиты информации.
5. Математические модели систем и процессов защиты информации.
6. Структура и задачи органов, осуществляющих защиту информации.
7. Политика информационной безопасности (организационно-технические и режимные меры).
8. Программно-технические методы и средства защиты информации.
9. Техническая защита информации на объектах ИС.
10. Защита информационных и физических объектов ИС.
11. Защита процессов и программ.
12. Технологии брандмауэров.
13. Защита каналов связи.
14. Управление системой защиты.
15. Построение системы защиты информации.
16. Выявление потенциальных угроз и каналов утечки информации.
17. Оценка уязвимости и рисков.
18. Требования к системам защиты информации.
19. Осуществление выбора средств защиты информации.
20. Внедрение и использование выбранных средств защиты информации.
21. Контроль целостности и управление ИС.
22. Сертификация ИС и ее компонентов по требованиям информационной безопасности.
23. Модель комплексной оценки СЗИ.
24. Решения по защите информации.

Примерные задания

Математические модели систем и процессов защиты информации

ФИО _____ группа _____

Цель: Общие знания по моделированию защиты информации

Исходные положения для создания модели защиты информации:

1. _____

2. _____

Основные блоки модели

1. _____

2. _____

3. _____

4. _____

Процесс создания математической модели

1. Разработка принципов, методов и средств сокращения размерности описания СЗИ:

- _____
- _____
- _____
- _____

2. Разработка методологии, методов и средств решения задач обеспечения БИТ:

- _____
- _____

Составляющие модель процессы защиты информации:

- _____
- _____
- _____
- _____

LMS-платформа − не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

1. Ключевые проблемы информационной безопасности государства.
2. Основные задачи обеспечения безопасности информации.
3. Безопасность информационных ресурсов.
4. Типовые компоненты ИС.
5. Проблемы защиты ИС.
6. Проблемы защиты открытых систем клиент/сервер.

7. Угрозы для протоколов и служб Internet.
8. Защищенная ИС и система защиты информации.
9. Стратегическая направленность защиты информации.
10. Создание службы информационной безопасности.
11. Типовой перечень задач службы информационной безопасности.
12. Организационно-правовой статус службы информационной безопасности.
13. Структура службы информационной безопасности информационной безопасности.
14. Определение политики информационной безопасности.
15. Принципы политики безопасности.
16. Виды политики безопасности.
17. Организационно-технические мероприятия.
18. Защита данных административными методами.
19. Организация секретного делопроизводства.
20. Организация мероприятий по ЗИ.
21. Политики безопасности для Internet.
22. Службы и механизмы защиты информации.
23. Методы идентификации и аутентификации пользователей.
24. Управление доступом.
25. Конфиденциальность данных и сообщений.
26. Регистрация действий пользователей.
27. Метод парольной защиты и его модификации.
28. Подсистема управления ключами.
29. Биометрические средства аутентификации и контроля доступа.
30. Метод автоматической генерации обратного вызова.
31. Метод перекрестного опознавания.
32. Проверка адреса корреспондента.
33. Проверка обратного кода.
34. Схема рукопожатия.
35. Контроль доступа пользователей к ресурсам ИС.
36. Методы предотвращения повторного использования объектов.
37. Средства защиты информации в ИС.
38. Средства защиты от НСД.
39. Анализаторы протоколов.
40. Инструментальные средства тестирования системы защиты.
41. Межсетевые экраны.
42. Хеш-функции.
43. Общие сведения и классификация хеш-функций.
44. Стандарты кодов аутентификации сообщений.
45. MAC-коды.
46. Бесключевые хеш-функции.
47. Модель итеративных хеш-функций.
48. Специализированные хеш-функции.
49. Цифровые подписи.
50. Общие определения и классификация схем цифровых подписей.
51. Механизмы неотказуемости.
52. Механизм доказательства неотказуемости происхождения сообщения.

53. Режимы работы блочных алгоритмов шифрования.
54. Техническая защита информации на объектах ИС.
55. Файлы и базы данных как информационные объекты защиты.
56. Идентификация и проверка подлинности пользователей.
57. Угрозы для СУБД.
58. Управление доступом.
59. Поддержание целостности данных в СУБД.
60. Защита коммуникаций между сервером и клиентами.
61. Защита ресурсных объектов.
62. Защита физических объектов ИС.
63. Виртуальные сети.
64. Администрирование.
65. Системы сбора статистики и предупреждения об атаке.
66. Аутентификация.
67. Брандмауэры - основа СЗИ.
68. Шлюзы уровня приложений и посредники.
69. Защита от уязвимых мест в службах.
70. Управляемый доступ к системам сети.
71. Криптографические методы и средства защиты информации.
72. Подсистема криптографической защиты.
73. Аутентичность сообщений.
74. Анализ существующих методов криптографических преобразований.
75. Защита данных при передаче по каналам связи ИС.
76. Защита целостности сообщений.
77. Защищенный обмен сообщениями.
78. Цифровая подпись и цифровой конверт.
79. Алгоритм шифрования данных PGP.
80. Защищенные каналы.
81. Защита потоков маршрутизатором.
82. Выбор средств защиты сообщений.
83. Совместимость средств защиты сообщений.
84. Защита электронной почты.
85. Средства физической защиты информации.
86. Средства криптографической защиты.
87. Управление механизмами СЗИ.
88. Определение информации, подлежащей защите.
89. Угрозы безопасности информации.
90. Анализ характеристик угроз и уязвимых мест для информации в ИС.
91. Угрозы безопасности информации, ИС и субъектов информационных отношений.
92. Основные виды угроз безопасности субъектов информационных отношений.
93. Наиболее распространенные угрозы информации в ИС.
94. Угрозы несанкционированного доступа к информации в ИС.
95. Особенности НСД.
96. Специальные методы и технические средства съема информации.
97. Угрозы для процессов, процедур и программ обработки информации.
98. Угрозы для информации в каналах связи.

99. Вирусные угрозы для коммуникационных узлов ИС.
100. Угрозы, связанные с электронной почтой.
101. Угрозы для механизмов управления системой защиты.
102. Неформальная модель нарушителя.
103. Анализ и разработка методологии оценки рисков информационной безопасности.
104. Методики оценки потенциально возможных угроз ИС.
105. Оценка ущерба от угроз безопасности информации.
106. Общие требования к информационной безопасности.
107. Организационные требования.
108. Перечень основных функциональных задач, которые должна решать СЗИ.
109. Технические требования по защите информации от утечки по каналам ПЭМИН.
110. Модель ИС как объекта защиты.
111. Архитектурные вопросы построения безопасных компьютерных сетей.
112. Услуги и механизмы обеспечения безопасности сетей на основе модели ВОС.
113. Базовые сервисы для обеспечения безопасности компьютерных систем.
114. Средства защиты от НСД.
115. Инструментальные средства тестирования системы защиты.
116. Межсетевые экраны.
117. Выбор основных решений по обеспечению ЗИ.
118. Обеспечение ЗИ на стадиях проектирования ИС.
119. Рабочая документация, относящаяся к СЗИ.
120. ЗИ в процессе подготовки ИС к эксплуатации.
121. ЗИ при эксплуатации ИС.
122. Этапы выполнения работ по созданию СЗИ.
123. Процесс создания механизмов защиты ИС.
124. Построение системы защиты информации.
125. Реализация организационных мер защиты информации.
126. Контроль за работой пользователей.
127. Системы электронного документооборота.

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	учебно-исследовательская, научно-исследовательская целенаправленная работа с информацией для использования в	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности Технология самостоятельной	ПК-20	П-6	Зачет Контрольная работа Лекции Практические/семинарские занятия

	практических целях	работы			