|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Autogenerated |  |  |  |
|  |  |  |  |  |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ | | | | |
|  |  |  |  |  |
| **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  **«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**  **(ДГТУ)** | | | | |
|  |  |  |  |  |
| **Методические рекомендации**  **для проведения текущей и промежуточной аттестации** | | | | |
| «НИР»  для студентов направления  10.03.01 Информационная безопасность  10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) | | | | |
| Составитель , ст.преп.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ганжур Марина Александровна | | | | |
| Составитель , ст.преп.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ганжур Алексей Петрович | | | | |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 2022 г. | | | | |

**Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

Оценивание результатов обучения по дисциплине осуществляется в соответствии с показателями оценивания компетенций приведёнными в табл. 1.

Таблица 1– Распределение баллов по дисциплине

|  |  |
| --- | --- |
| ***Вид учебных работ по практике*** | ***Количество баллов*** |
| Подготовка обучающимся письменного отчета по результатам прохождения практики | 10 |
| Отзыв с места прохождения практики, подписанный непосредственным руководителем практики от предприятия | 5 |
| Дневник прохождения практики с периодической фиксацией конкретных дел и действий, выполняемых обучающимся-практикантом во время прохождения практики | 5 |
| Устный отчет обучающегося по результатам прохождения практики | 40 |
| Защита отчета по практике, ответы на вопросы преподавателя и правильное решение практической задачи | 10 |
| Выполнение индивидуального  задания по практике | 20 |
| Сдача отчета по практике в установленные сроки | 10 |
| **Сумма баллов по практике** | 100 |

Обучающиеся, проходящие практику, сдают на кафедру дневник практики, план-график прохождения практики, отражающий работу, отзыв руководителя практики от организации и отчет о прохождении практики с анкетами работодателя и обучающегося.

При защите практики учитывается объем выполнения программы практики, своевременность сдачи материалов по практике, правильность оформления документов по практике, содержание отзыва-характеристики; правильность ответов на заданные руководителем практики вопросы на защите отчета.

Промежуточная аттестация по практике проводится в форме зачета с оценкой.

Критерии оценивания практики и оценки приведены в табл. 2

Таблица 2 ‒ Шкала оценивания контрольных мероприятий по практике

| **Оценка** | **Количество баллов** | **Критерии оценивания** |
| --- | --- | --- |
| Зачтено с оценкой  отлично | Более 91 балла | Изложение материалов полное, последовательное, грамотное. Индивидуальное задание по практике выполнено. Приложены первичные документы. Приложения логично связаны с текстовой частью отчета. Отчет сдан в установленный срок. Программа практики выполнена. Отзыв положительный.  Компетенция (и) или ее часть (и) сформированы на высоком уровне (уровень 3) (см. табл. 1.1). |
| Зачтено с оценкой  хорошо | 76-90 баллов | Изложение материалов полное, последовательное, в соответствии с требованиями программы практики. Допускаются несущественные стилистические ошибки. Приложения в основном связаны с текстовой частью отчета. Отчет сдан в установленный срок. Программа практики выполнена. Отзыв положительный.  Компетенция (и) или ее часть (и) сформированы на среднем уровне (уровень 2) (см. табл. 1.1). |
| Зачтено с оценкой  удовлетворительно | 61-75 баллов | Изложение материалов не полное. Оформление неаккуратное. Текстовая часть отчета не везде связана с приложениями. Отчет сдан в установленный срок. Программа практики выполнена не в полном объеме. Компетенция (и) или ее часть (и) сформированы на базовом уровне (уровень 1) (см. табл. 1.1). |
| Не зачтено | Менее 60 балла | Изложение материалов неполное, бессистемное. Существуют ошибки, оформление не соответствует установленным требованиям. Приложения отсутствуют. Отчет сдан не в установленный срок. Отзыв отрицательный. Программа практики не выполнена.  Компетенция(и) или ее часть (и) не сформированы. |

**2. Контрольные задания (демоверсии) для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

**2.1 Типовые контрольные задания на практику**

1. Источники угроз информационной безопасности.
2. Виртуальные частные сети.
3. Органы по технической защите информации в РФ.
4. Классификация криптоалгоритмов.
5. Угрозы и уязвимости беспроводных сетей и средства противодействия им.
6. Категорирование информационных ресурсов организации.
7. Государственная система защиты информации.
8. Методы оценки уровня информационной безопасности организации
9. Технические каналы утечки информации.
10. Требования, предъявляемые к комплексной системе защиты информации.
11. Угрозы и уязвимости проводных корпоративных сетей и средства противодействия им.
12. Надежность, стойкость и живучесть автоматизированной системы.
13. Методы защиты информации от утечки за счет электромагнитного излучения
14. Защита персональных данных.
15. Защита информации, отнесенной к государственной тайне.
16. Модель потенциального нарушителя информационной безопасности
17. Требования и рекомендации по защите акустической (речевой) информации.
18. Методы и способы обеспечения отказоустойчивости автоматизированных систем.
19. Защита информации от утечки по визуально-оптическим каналам.
20. Организация информационно-защищенного делопроизводства.
21. Правовая защита информации.
22. Стадии проектирования комплексной системы защиты информации
23. Оценка эффективности системы защиты информации
24. Классификация технических средств защиты информации.
25. Проведение экспертизы при расследовании инцидентов нарушения информационной безопасности.
26. Типовые криптографические протоколы и стандарты.
27. Структура и функции службы безопасности предприятия.
28. Криптографические методы защиты информации.
29. Подходы к обеспечению безопасности компьютерных систем и сетей.
30. Назначение и принципы построения комплексной системы защиты информации
31. Основные типы несанкционированного доступа и способы противодействия им.
32. Анализ операционных систем с точки зрения их защищенности.
33. Организационная защита информации.
34. Механизмы защиты операционных систем.
35. Инженерно-техническая защита информации.
36. Общие принципы асимметричного и симметричного шифрования информации.
37. Проблемы безопасности IP-сетей и способы их решения.
38. Средства и методы защиты информации
39. Система безопасности предприятия и принципы ее построения.
40. Протоколы аутентификации.
41. Обнаружение и нейтрализация средств технической разведки.
42. Понятие цифровой подписи, сравнительный анализ алгоритмов RSA и RSS.
43. Средства и методы обнаружения технических каналов утечки информации.
44. Стратегии защиты информации и разработка политики информационной безопасности
45. Требования к политике безопасности в рамках ISO.
46. Классификация программных средств защиты информации.
47. Защита информации от утечки по техническим каналам
48. Обеспечение безопасности веб-серверов.