Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра вычислительной техники
Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАНАВТФ
к.т.н., доцент И.Л. Рева
“___ ”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Безопасность и защита информации в информационных системах

Образовательная программа: 09.04.01 Информатика и вычислительная техника, магистерская программа: Прикладные информационные системы и технологии

Новосибирск 2020

1. Обобщенная структура фонда оценочных средств дисциплины

Обобщенная структура фонда оценочных средств по **дисциплине** Безопасность и защита информации в информационных системах представлена в Таблице. Результаты обучения по дисциплине соотнесены с уровнями сформированности компетенций и соотнесенных с ними индикаторов. Индикаторы достижения компетенций измеряемы с помощью средств текущей и промежуточной аттестации по дисциплине.

Таблица

Формируемые компетенции	**Индикаторы компетенций**	**Темы**	**Этапы оценки компетенций и соотнесенных с ними индикаторов**	
			Мероприятия текущего контроля (контрольная работа, курсовой проект, РГЗ(Р), реферат и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОПК-6 Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования	1. Знать: аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности	Введение. Информ. безопасность в системе национальной безопасности РФ. Федеральный закон "О безопасности". Государственная система правового обеспечения защиты информации в Российской Федерации. Информационные системы, классификация информационных систем. Причины, виды, каналы утечки информации. Классификация угроз информационной безопасности. Классификация источников угроз информационной безопасности. Методы и средства обеспечения безопасности информационных систем. Технические средства, организационная и правовая защита. Национальные интересы РФ в информационной сфере и их обеспечение. Источники угроз информационной безопасности. Оценка эффективности средств защиты информации (СЗИ). Понятие "политики информационной безопасности" предприятия. Причины, виды, каналы утечки информации. Угрозы нарушения конфиденциальности, целостности, доступности информации. Модели угроз.	РГЗ/ В рамках расчетно-графического задания (работы) по дисциплине студенты должны провести анализ предоставленного (выбранного самостоятельно) объекта информатизации, малого предприятия и.т.д., провести оценку рисков и анализ угроз информационной безопасности, обосновать результаты расчетов, предоставить способы устранения выявленных угроз безопасности. Обязательные структурные части РГЗ. 1) Анализ объекта; 2) Оценка рисков; 3) Анализ угроз; 4) Предложение способов	Экзамен, вопросы... 1. Понятие информационной безопасности. 2. Национальная безопасность. 3. Доктрина информационной безопасности Российской Федерации. 4. Национальные интересы РФ в информационной сфере и их обеспечение. 5. Виды угроз информационной безопасности РФ. 6. Источники угроз информационной безопасности РФ. 7. Информационные системы, классификация информационных систем. Причины, виды, каналы утечки информации. 8. Угрозы информационному обеспечению государственной политики РФ. 9. Методы и модели оценки угроз информации в информационных системах. 10. Причины, виды, каналы утечки информации. 11. Средства

			защиты;	обеспечения безопасности информационных систем. 12. Методы обеспечения безопасности информационных систем. Технические средства защиты. 13. Правовая защита информационных систем. 14. Направления и цели защиты информации и их взаимосвязь. 15. Угрозы информации. Виды угроз. 16. Классификация угроз информационной безопасности. Классификация источников угроз информационной безопасности. 17. Концептуальная модель безопасности продукции. 18. Концептуальная модель безопасности личности. 19. Концептуальная модель безопасности информации. 20. Организационная защита. 21. Технологии противодействие атакам на сетевые сервисы. Отказ а обслуживании (DOS) 22. Физические средства защиты информации. 23. Политика безопасности предприятия. 24. Способы и технологии противодействие атакам на WEB - прилижение. 25. Оценка эффективности средств защиты информации (СЗИ). 26. Принцип осуществления атак типа BRUTEFORCE. Подбор пароля через SMTP протокол. 27. Способы

				получения полного контроля над целевой машиной .

2. **Методика оценки этапов формирования компетенций по дисциплине**

Уровни сформированности компетенции проверяется при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины указанных в таблице раздела 1.

В 3 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Промежуточная аттестация по **дисциплине** проводится в 3 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОПК-6 и соотнесенных с ними индикаторов. (см. таблицу раздела 1).

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно оценить уровни сформированности компетенции ОПК-6, закрепленных за дисциплиной.

3. **Общая характеристика уровней освоения компетенций**

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено, необходимом для дальнейшей учебы и профессиональной деятельности. Некоторые практические навыки работы с сформированы с незначительными пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов, входящих в диапазон ниже порогового уровня.