

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет Математики и информационных технологий
Кафедра Математического моделирования

Оценочные материалы по дисциплине (модулю)

дисциплина Проектирование систем обеспечения информационной безопасности

Блок Б1, обязательная часть, Б1.О.33

цикл дисциплины и его часть (обязательная часть или часть, формируемая участниками образовательных отношений)

Направление

10.03.01

Информационная безопасность

код

наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2021 г.

Разработчик (составитель)

кандидат физико-математических наук, доцент

Беляева М. Б.

ученая степень, должность, ФИО

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)	3
2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)	6
3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания	8

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
			1	2	3	4	
			неуд.	удовл.	хорошо	отлично	
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.1.	обучающийся должен знать: структуру систем документационного обеспечения; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; основные нормативные правовые акты в области информационно	Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.	Ответ слабо структурирован. Понимание отдельных положений из материала по теме. Удовлетворительное умение формулировать свои мысли, обсуждать дискуссионные положения.	Структура ответа в целом адекватна теме. Продемонстрирован хороший уровень понимания материала. Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.	Ответ хорошо структурирован. Продемонстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать дискуссионные положения.	Устный опрос

		<p>й безопасности и защиты информации; нормативные методические документы Федеральной службы по техническому и экспортному контролю в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации; задачи органов защиты государственной тайны;</p>					
	ОПК-12.2.	<p>обучающийся должен уметь: пользоваться нормативными документами по защите информации;</p>	<p>Задания выполнены менее чем наполовину. Продемонстрированы неудовлетворительный</p>	<p>Задания выполнены более чем наполовину. Присутствуют серьезные ошибки. Продемонстриро</p>	<p>Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки.</p>	<p>Правильно выполнены все задания. Продемонстрированы высокий уровень владения</p>	Реферат

		применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;	уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.	ван удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	
	ОПК-12.3.	обучающийся должен владеть: навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности.	Продемонстрирован неудовлетворительный уровень освоения навыков, недостаточный для решения задач профессиональной деятельности.	Продемонстрирован удовлетворительный уровень освоения навыков, достаточный для решения отдельных задач профессиональной деятельности.	Продемонстрирован хороший уровень освоения навыков, достаточный для решения большей части задач профессиональной деятельности.	Продемонстрирован высокий уровень освоения навыков, достаточный для успешного решения задач профессиональной деятельности	Контрольные вопросы

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)

Контрольные вопросы

1. Теория защиты информации.
2. Обеспечение информационной безопасности и направления защиты
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная)
4. Требования к системе защиты информации
5. Угрозы информации
6. Виды угроз. Основные нарушения
7. Характер происхождения угроз
8. Источники угроз. Предпосылки появления угроз
9. Система защиты информации
10. Классы каналов несанкционированного получения информации
11. Причины нарушения целостности информации
12. Методы и модели оценки уязвимости информации
13. Общая модель воздействия на информацию
14. Общая модель процесса нарушения физической целостности информации
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных
16. Методологические подходы к оценке уязвимости информации
17. Модель защиты системы с полным перекрытием
18. Рекомендации по использованию моделей оценки уязвимости информации
19. Допущения в моделях оценки уязвимости информации
20. Методы определения требований к защите информации
21. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации
22. Классификация требований к средствам защиты информации
23. Требования к защите, определяемые структурой автоматизированной системы обработки данных
24. Требования к защите, обуславливаемые видом защищаемой информации
25. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации
26. Анализ существующих методик определения требований к защите информации
27. Руководящий документ Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации"

28. Классы защищенности средств вычислительной техники от несанкционированного доступа
29. Функции защиты информации
30. Стратегии защиты информации
31. Способы и средства защиты информации
32. Архитектура систем защиты информации.
33. Требования общеметодологических принципов архитектуры системы защиты информации
34. Построение средств защиты информации
35. Ядро системы защиты
36. Средства защиты информации.
37. Антивирусы, средства анализа защищенности, средства обнаружения вторжений
38. Регуляторы в области защиты информации

Темы рефератов

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутривнутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.
2. Виды информации и основные методы ее защиты. Информационные ресурсы. Носители информации
3. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
4. Виды угроз информационной безопасности Российской Федерации.
5. Источники угроз информационной безопасности Российской Федерации.
6. Анализ информационной инфраструктуры государства.
7. Информационное оружие, его классификация и возможности.
8. Цели информационной войны в мирное и военное время.
9. Объекты информационного воздействия в информационной войне
10. Концепция защиты СВТ и АС от НСД к информации.
11. Парольная защита как средство защиты от НСД.
12. Критерии оценки защищенности СВТ, методы и средства обеспечения их информационной безопасности.
13. Критерии оценки защищенности АС, методы и средства обеспечения их информационной безопасности.
14. Оценка безопасности информационных технологий по Общим критериям.
15. Особенности обеспечения информационной безопасности компьютерных

систем при обработке информации, составляющей государственную тайну.

16. Технические каналы утечки информации при эксплуатации АС и их защита.

17. Защита АС и СВТ от внешнего электромагнитного воздействия.

18. Технические средства защиты сетей и систем связи от утечки конфиденциальной информации

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл = $k \times$ Максимальный балл,

где $k = 0,2$ при уровне освоения «неудовлетворительно», $k = 0,4$ при уровне освоения «удовлетворительно», $k = 0,8$ при уровне освоения «хорошо» и $k = 1$ при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов БашГУ:

На зачете выставляется оценка:

- зачтено - при накоплении от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
- не зачтено - при накоплении от 0 до 59 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.