Министерство науки и высшего образования российской федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Утверждаю
И.о. зав. кафедрой ИСЭА
_____ Колдаев А.И.
«___»_____2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Защита информации в системах управления
для проведения текущего контроля успеваемости и промежуточной аттестации
(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки 15.03.04 Автоматизация технологических процессов и производств
Профиль Информационно-управляющие системы
Квалификация выпускника бакалавр
Форма обучения очная
Год начала обучения 2019
Изучается в 4 семестре

	Астр. часов	
Объем занятий: Итого	81.00	3.00 з.е
В том числе аудиторных	36.00 ч.	
Из них:		
Лекций	12.00 ч.	
Лабораторных работ	24.00 ч.	
Самостоятельной работы	45.00ч.	

Зачет 6 семестр

Дата разработки:

1. Назначение: фонд оценочных средств по дисциплине «Защита информации в системах управления» предназначен для оценки знаний обучающихся при освоении ими дисциплины при проведении текущего контроля успеваемости и промежуточной аттестации. Фонд включает в себя вопросы для собеседования

2. Фонд оценочных средств текущего контроля успеваемости и промежуточной аттестации разработан на основе рабочей программы дисциплины «Защита информации в системах управления» и в соответствии с образовательной программой высшего образования по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств утвержденной на заседании Учебно-методического совета СКФУ, протокол № от «____»_____2019 г.

3. Разработчик Кочеров Ю. Н. доцент кафедры ИСЭА

4. ФОС рассмотрен и утвержден на заседании кафедры информационных систем, электропривода и автоматики , протокол № _____ от «___»_____2019 г.

5. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:

Председатель_____
_____
_____

Экспертное заключение_____
«_____ » _____ 2019г. _____

6. Срок действия ФОС_____

Паспорт фонда оценочных средств
для проведения текущего контроля успеваемости и промежуточной аттестации

По дисциплине Защита информации в системах управления
Направление подготовки 15.03.04 Автоматизация технологических процессов и производств
Профиль Информационно-управляющие системы
Квалификация выпускника бакалавр
Форма обучения очная
Год начала обучения 2019
Изучается в 4 семестре

Код оцениваемой компетенции	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Вид контроля, аттестация	Тип контроля	Наименование оценочного средства	Количество заданий для каждого уровня, шт	
						Базовый	Повышенный
ОПК-2	Тема 1.Защита информации в вычислительных системах	Собеседование	Устный	Текущий	Вопросы для собеседования	2	1
ОПК-2	Тема 2.Организационные меры защиты ЭВМ	Собеседование	Устный	Текущий	Вопросы для собеседования	1	2
ОПК-2	Тема 3.Анализ угроз сохранности информации	Собеседование	Устный	Текущий	Вопросы для собеседования	1	1
ОПК-2	Тема 4.Сопровождение комплексной системы защиты информации в автоматизированной системе (КСЗИ)	Собеседование	Устный	Текущий	Вопросы для собеседования	2	2
ОПК-2	Тема 5.Организационные основы защиты информации в автоматизированных системах на предприятии	Собеседование	Устный	Текущий	Вопросы для собеседования	1	1
ОПК-2	Тема 6.Защита информационных и сетевых ресурсов в сетях, подключенных к Интернет	Собеседование	Устный	Текущий	Вопросы для собеседования	1	2
ОПК-2	Тема 7.Меры непосредственной защиты ЭВМ	Собеседование	Устный	Текущий	Вопросы для собеседования	1	1
ОПК-2	Тема 8.Защита	Собеседо	Устны	Теку	Вопросы	1	1

	аппаратных средств	вание	й	щий	для собеседования		
ОПК-2	Тема 9.Криптографические методы защиты	Собеседование	Устный	Текущий	Вопросы для собеседования	2	1
ОПК-2	Тема 10. Симметричные системы шифрования	Собеседование	Устный	Текущий	Вопросы для собеседования	2	2
ОПК-2	Тема 11. Принципы построения программных шифров	Собеседование	Устный	Текущий	Вопросы для собеседования	1	1
ОПК-2	Тема 12. Типы шифров	Собеседование	Устный	Текущий	Вопросы для собеседования	2	2
ОПК-2	Тема 13. Несимметричные системы шифрования	Собеседование	Устный	Текущий	Вопросы для собеседования	2	2
ОПК-2	Тема 14. Защита операционной системы	Собеседование	Устный	Текущий	Вопросы для собеседования	2	1
ОПК-2	Тема 15. Защита информации в базах данных	Собеседование	Устный	Текущий	Вопросы для собеседования	1	1

Составитель _____ Кочеров Ю.Н.

«____»_____2019 г

Министерство науки и высшего образования российской федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Утверждаю
И.о. зав. кафедрой ИСЭА
_____ Колдаев А.И.
«___»_____2019 г.

Вопросы для собеседования
по дисциплине Защита информации в системах управления
Базовый уровень

Тема 1.Защита информации в вычислительных системах
1. Защита информации в вычислительных системах.
2. Введение в вопросы защиты информации. Информационная безопасность человека и общества.
Тема 2.Организационные меры защиты ЭВМ
1. Организационные меры защиты ЭВМ.
Тема 3.Анализ угроз сохранности информации
1. Анализ угроз сохранности информации.
Тема 4.Сопровождение комплексной системы защиты информации в автоматизированной системе (КСЗИ)
1. Сопровождение комплексной системы защиты информации в автоматизированной системе (КСЗИ).
2. Разработка и реализация плана защиты информации. Суть задачи сопровождения КСЗИ в АС. Служба защиты информации в АС как основной механизм организации сопровождения КСЗИ.
Тема 5.Организационные основы защиты информации в автоматизированных системах на предприятии
1. Организационные основы защиты информации в автоматизированных системах на предприятии.
Тема 6.Защита информационных и сетевых ресурсов в сетях, подключенных к Интернет
1. Защита информационных и сетевых ресурсов в сетях, подключенных к Интернет.
Тема 7.Меры непосредственной защиты ЭВМ
1. Меры непосредственной защиты ЭВМ.
Тема 8.Защита аппаратных средств
1. Защита аппаратных средств.
Тема 9.Криптографические методы защиты
1. Криптографические методы защиты.
2. Значение криптографии в информационном обществе.
Тема 10. Симметричные системы шифрования
1. Симметричные системы шифрования.
2. Основы одно-ключевых криптосистем.
Тема 11. Принципы построения программных шифров
1. Принципы построения программных шифров.
Тема 12. Типы шифров
1. Типы шифров.
2. Шифры с управляемыми операциями. Способ шифрования на основе управляемых перестановок.
Тема 13. Несимметричные системы шифрования
1. Несимметричные системы шифрования.

2. Двухключевые шифры. Система открытого распределения ключей.
Тема 14. Защита операционной системы
1. Защита операционной системы.
2. Процедуры проверки. Контроль доступа.
Тема 15. Защита информации в базах данных
1. Защита информации в базах данных.

Повышенный уровень

Тема 1.Защита информации в вычислительных системах
1. Нормативно-правовые документы, регламентирующие деятельность в области информационной безопасности. Государственная система защиты информации.
Тема 2.Организационные меры защиты ЭВМ
1. Проблемы организации работы вычислительного центра. Организационно-управленческие меры.
2. Экономические проблемы. Цели защиты ЭВМ и ответственность.
Тема 3.Анализ угроз сохранности информации
1. Характеристика методов и средств защиты информации. Порядок обеспечения защиты информации в автоматизированной системе (АС)
Тема 4.Сопровождение комплексной системы защиты информации в автоматизированной системе (КСЗИ)
1. Правовые основы создания и деятельности службы защиты информации, ее основные задачи и функции.
2. Состав и содержание плана защиты, содержание мер и порядок его формирования и реализации.
Тема 5.Организационные основы защиты информации в автоматизированных системах на предприятии
1. Основные технические каналы утечки информации в автоматизированных системах. Меры и средства защиты элементов автоматизированных систем от утечки информации по техническим каналам.
Тема 6.Защита информационных и сетевых ресурсов в сетях, подключенных к Интернет
1. Классификация уязвимостей; подходы определения уязвимостей безопасности сетей; сканеры для проверки уязвимостей фирм ISS, CISCO, NMAP и другие; защита сетей от компьютерных атак.
2. Распространенные атаки на системы связи (DoS, ping-of-death и т.д.). Методы и средства защиты; понятие адаптивного управления безопасностью сети.
Тема 7.Меры непосредственной защиты ЭВМ
1. Защита от стихийных бедствий. Защита от злоумышленников. Идентификация и установление личности.
Тема 8.Защита аппаратных средств
1. Защита памяти. Состояния выполнения программ. Применение микропроцессоров для защиты аппаратных средств.
Тема 9.Криптографические методы защиты
1. Проблематика криптографии.
Тема 10. Симметричные системы шифрования
1. Одно-ключевые шифры.
2. Одно-ключевые модели шифрования.
Тема 11. Принципы построения программных шифров
1. Недетерминированные программные шифры.
Тема 12. Типы шифров
1. Шифры с управляемыми подстановками.
2. Шифры на основе модифицирования подключей.
Тема 13. Несимметричные системы шифрования
1. Цифровая электронная подпись. Хэш-функции на основе блочных шифров.
2. Вероятностные шифры. Гомофонические шифры.
Тема 14. Защита операционной системы
1. Изоляция областей нарушения защиты операционной системы. Разработка и реализация операционных систем со средствами защиты.

Тема 15. Защита информации в базах данных

1. Принятие решений о доступе. Организация доступа к базе данных. Назначение полномочий.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

***2.* Описание шкалы оценивания**

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя: проведения собеседования.

Предлагаемые студенту задания позволяют проверить компетенции ОПК-2

Для подготовки к данному оценочному мероприятию необходимо 5-10 минут

При подготовке к ответу студенту предоставляется право пользования: запрещено пользоваться любой литературой и техническими средствами.

При проверке задания, оцениваются: последовательность и рациональность ответов на поставленные вопросы

Составитель _____ Кочеров Ю.Н.

«____»_____2019 г