МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой «Информационной
безопасности, систем и технологий»
_____ В.Ф. Антонов
«__» _____ 202_ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

По дисциплине	**Основы управления информационной безопасностью**	
Направление подготовки	**10.03.01 Информационная безопасность**	
Направленность (профиль)	**Комплексная защита объектов информатизации**	
Квалификация выпускника	бакалавр	
Форма обучения	очная	
Учебный план	2020	
Объем занятий: Итого	81 ч.	3з.е.
В т.ч. аудиторных	36 ч.	
Из них:		
Лекций	18 ч.	
Лабораторных работ	18 ч.	
Самостоятельной работы	18ч.	
Контроль	27 ч.	
Экзамен	8 семестр	

Дата разработки: _____

Предисловие

1. Назначение: для проверки знаний, умений и навыков текущего контроля и промежуточной аттестации.

Фонд оценочных средств текущего контроля и промежуточной аттестации на основе рабочей программы дисциплины «Основы управления информационной безопасностью» в соответствии с образовательной программой по направлению подготовки 10.03.01 «Информационная безопасность», утвержденной на заседании Учебно-методического совета ФГАОУ ВО «СКФУ» протокол № 1от «29» сентября 2020г.

2. Разработчик Калиберда И.В., старший преподаватель

3. ФОС рассмотрен и утвержден на заседании кафедры «Информационная безопасность, системы и технологии», Протокол № _2_ от «4» сентября 2020г.

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

Председатель _____В.Ф. Антонов, зав. кафедрой ИБСиТ
_____А.Б. Чернышев, профессор кафедры ИБСиТ
_____П.П. Мулкиджанян, начальник отдела проектирования ООО "Комби-Сервис"

Экспертное заключение: данные оценочные средства соответствуют требованиям федерального государственного образовательного стандарта высшего образования, рекомендуются для использования в учебном процессе.

«____»_____ _____(подпись)

1. Срок действия ФОС 1 год.

Паспорт фонда оценочных средств
Для проведения текущего контроля и промежуточной аттестации

По дисциплине **Основы управления информационной безопасностью**

Направление подготовки **10.03.01 Информационная безопасность**
Направленность (профиль) **Комплексная защита объектов информатизации**
Квалификация выпускника бакалавр
Форма обучения очная
Учебный план 2020

Код оцениваемой компетенции (или её части)	Модуль, раздел, тема(в соответствии с Программой)	Тип контроля	Вид контроля	Компонент фонда оценочных средств	Количествозаданий для каждого уровня, шт.	
					Базовый	Повышенный
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	Тема 1-9	текущий	письменный	Темы индивидуальных заданий для практических занятий	4	4
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	Тема 1-9	текущий	устный	Вопросы для собеседования	35	35
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	Тема 1-9	промежуточный	устный	Вопросы к экзамену	33	32
				Вопросы для проверки уровня знаний	26	25
				Вопросы (задания) для проверки умений и навыков	7	7

Составитель _____ И.В. Калиберда
(подпись)

«___»_____202 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой «Информационной
безопасности, систем и технологий»
_____ В.Ф. Антонов
«__» _____ 2020г.

Вопросы для собеседования

по дисциплине

Основы управления информационной безопасностью

8 семестр

Базовый уровень

Тема 1. Организационно-правовые нормы защиты информации на предприятии.

1. Виды информации.
2. Несанкционированный доступ и утечка информации.
3. Методы и средства организационной защиты информации.
4. Уровни правового обеспечения информационной безопасности.

Тема 2. Угрозы информационной безопасности и каналы утечки информации.

5. Виды угроз.
6. Непреднамеренные угрозы.
7. Умышленные угрозы.
8. Косвенные каналы утечки информации.
9. Непосредственные каналы утечки информации.

Тема 3. Морально этические нормы защиты информации на предприятии.

10. Морально этические нормы защиты информации на предприятии.
11. Виды морально этических мероприятий.

Тема 4. Документация по комплексной правовой защите информации на предприятии.Инженерно-технические методы и средства защиты информации.

12. Цели инженерно-технической защиты информации.

Тема 5. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.

13. Основные аппаратные средства защиты информации.
14. Вспомогательные аппаратные средства защиты информации.
15. Основные программные средства защиты информации.
16. Вспомогательные программные средства защиты информации.

Тема 6. Процесс оценки риска информационной безопасности.

17. Основные требования к комплексной системе защиты информации.
18. Основные категории требованийк защищенности КС из «Оранжевой книги».

Тема 7. Идентификация уязвимостей и построение модели нарушителя.

19. Основные способы несанкционированного доступа к информации в КС.
20. Уровни возможностей нарушителя.

21. Вспомогательные способы несанкционированного доступа к информации в КС.

Тема 8. Предварительный анализ информационной безопасности предприятия.

22. Параметры политики учетных записей при использовании парольной аутентификации.

Тема 9. Существующие и планируемые средства контроля.

23. Анализ существующих средств контроля.

24. Анализ планируемых средств контроля..

Тема 10. Программные средства защиты информации на предприятии.

25. Двухфакторная аутентификация с элементами аппаратного обеспечения (диски, карты, маркеры и т.п.).

Тема 11. Аппаратные средства защиты информации на предприятии.

26. Процедура парольной инициализации.

27. Причины, облегчающие нарушителю реализацию угроз безопасности информации в распределенных КС.

28. Основные понятия криптологии (открытый и шифртекст, криптография, криптология и криптоанализ, криптостойкость и ее характеристики).

29. Классы защищенности КС из «Оранжевой книги».

30. Потоковые и блочные шифры, их виды и характеристики.

31. Свойства абсолютно стойкого шифра.

Тема 12. Построение структурного подразделения информационной безопасности.

32. Анализ рисков информационной безопасности предприятия.

33. Последовательность действий по созданию СОИБ.

34. Правила противодействия системы попыткам подбора пароля.

35. Подразделения по информационной безопасности.

Повышенный уровень

Тема 1. Организационно-правовые нормы защиты информации на предприятии.

1. Политика безопасности.

Тема 2. Угрозы информационной безопасности и каналы утечки информации.

2. Побочные электромагнитные излучения и наводки (ПЭМИН).

3. Системно-концептуальный подход защиты информации.

4. Основные группы методов и средств защиты информации.

Тема 3. Морально этические нормы защиты информации на предприятии.

5. Международные договоры первого уровня правового обеспечения информационной безопасности.

6. Подзаконные акты второго уровня правового обеспечения информационной безопасности.

7. Государственные стандарты третьего уровня правового обеспечения информационной безопасности.

8. Локальные нормативные документы четвертого уровня правового обеспечения информационной безопасности.

Тема 4. Документация по комплексной правовой защите информации на предприятии. Инженерно-технические методы и средства защиты информации.

9. Методы и средства защиты информации от утечки по каналам ПЭМИН.

Тема 5. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.

10. Преимущества и недостатки аппаратных и программныхсредств защиты информации.

Тема 6. Процесс оценки риска информационной безопасности.

11. Классы защищенности КС из «Оранжевой книги».
12. Группы классов защищенности АС из документов Гостехкомиссии России.

Тема 7. Идентификация уязвимостей и построение модели нарушителя.

13. Основные функции системы разграничения доступа.
14. Функции обеспечивающих средств для системы разграничения доступа.
15. Три группы способов аутентификации.

Тема 8. Предварительный анализ информационной безопасности предприятия.

16. Правила противодействия системы попыткам подбора пароля.
17. Правила ввода или смены пароля пользователем.
18. Недостатки схемы одноразовых паролей.

Тема 9. Существующие и планируемые средства контроля.

19. Процедура настройки на клавиатурный почерк регистрируемого пользователя.
20. Варианты процедуры аутентификации по клавиатурному почерку.
21. Процедура настройки на роспись мышью регистрируемого пользователя.

Тема 10. Программные средства защиты информации на предприятии.

22. Модель нарушителя.

Тема 11. Аппаратные средства защиты информации на предприятии.

23. Методы создания безопасных распределенных КС.
24. Разновидности межсетевых экранов (фильтрующие маршрутизаторы, шлюзы сеансового и прикладного уровней), их достоинства и недостатки.
25. Области применения криптографии.
26. Схема алгоритма DES.
27. Четыре режима работы на основе алгоритма DES.
28. Схема алгоритма ГОСТ 28147-89.
29. Три основных и один дополнительный режимы ГОСТ 28147-89.
30. Имитовставка.

Тема 12. Построение структурного подразделения информационной безопасности.

31. Группы классов защищенности АС из документов Гостехкомиссии России.
32. Наиболее известные системы ЭЦП.
33. Наиболее известные функции хэширования.
34. Принципы создания системы информационной безопасности ИС организации.
35. Правила ввода или смены пароля пользователем.

Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он в ходе собеседования правильно ответил на вопрос по теме собеседования, сопровождая наглядными примерами.

Оценка «хорошо» выставляется студенту, если он в ходе собеседования ответил на вопрос по теме собеседования, при этом есть неуверенность с практическими примерами.

Оценка «удовлетворительно» выставляется студенту, если он ходе собеседования ответил неуверенно на вопросы по теме собеседования, не смог привести практические примеры.

Оценка «неудовлетворительно» выставляется студенту, если он не ответил на вопрос по теме собеседования.

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**

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

Процедура проведения данного оценочного мероприятия включает в себя:

Студенту выдается вопрос на собеседование, он готовит ответ (можно в письменной или устной форме) и отсчитывается перед преподавателем по заданному вопросу.

Предлагаемые студенту задания позволяют проверить компетенции ОК-5, ОПК-7, ПК-3,4,5,6,13,14,15.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

При проверке задания, оцениваются:

- последовательность и рациональность выполнения задания;
- точность вычислений;
- знания технологий, использованныхпри решение задания.

Составитель _____ И. В. Калиберда

«____»_____2020 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой «Информационной
безопасности, систем и технологий»
_____ В.Ф. Антонов
«__» _____ 202_ г.

Темы индивидуальные заданий для практических занятий по дисциплине «Основы управления информационной безопасностью»(8 семестр)

Индивидуальные задания:

Базовый уровень

1. Анализ рисков информационной безопасности.
2. Обеспечение информационной безопасности в ведущих зарубежных странах.
3. Пакеты антивирусных программ.
4. Программная реализация криптографических алгоритмов.

Повышенный уровень

1. Построение концепции информационной безопасности предприятия.
2. Процедура аутентификации пользователя на основе пароля.
3. Алгоритмы поведения вирусных и других вредоносных программ.
4. Механизмы контроля целостности данных.

Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, еслиотчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнениюпрактических занятий, а также раскрыты полностью все вопросы по заданию.

Оценка «хорошо» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению практических занятий, а также частично раскрыты вопросы по заданию.

Оценка «удовлетворительно» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическимирекомендациями по выполнению практических занятий, а также раскрыт не полностью перечень необходимых вопросов по заданию.

Оценка «неудовлетворительно» выставляется студенту, если отчет по работе выполнен не в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению практических занятий, а также не раскрыты вопросы по заданию.

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**

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

Процедура проведения данного оценочного мероприятия включает в себя: выполнение индивидуального задания и оформление отчета по практическим занятиям. Предлагаемые студенту задания позволяют проверить компетенции ОК-5, ОПК-7, ПК-3,4,5,6,13,14,15.

Для подготовки к данному оценочному мероприятию необходимо к концу текущегопрактического занятияпредоставить преподавателю материалы по выполнению практического занятия.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- точность вычислений;
- знания технологий, использованных при выполнении задания.

Составитель _____ И.В.Калиберда

«____»_____20 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой «Информационной
безопасности, систем и технологий»
_____ В.Ф. Антонов
«__» _____ 202_ г.

Вопросы к экзамену

по дисциплине «Основы управления информационной безопасностью» (8семестр)

Базовый уровень

Вопросы (задача, задание) для проверки уровня обученности.

Знать

1. Виды информации.
2. Несанкционированный доступ и утечка информации.
3. Виды угроз.
4. Непреднамеренные угрозы.
5. Умышленные угрозы.
6. Косвенные каналы утечки информации.
7. Непосредственные каналы утечки информации.
8. Виды организационных мероприятий.
9. Уровни правового обеспечения информационной безопасности.
10. Цели инженерно-технической защиты информации.
11. Основные аппаратные средства защиты информации.
12. Основные программные средства защиты информации.
13. Основные требования к комплексной системе защиты информации.
14. Основные способы несанкционированного доступа к информации в КС.
15. Уровни возможностей нарушителя.
16. Параметры политики учетных записей при использовании парольной аутентификации.
17. Двухфакторная аутентификация с элементами аппаратного обеспечения (диски, карты, маркеры и т.п.).
18. Процедура парольной инициализации.
19. Причины, облегчающие нарушителю реализацию угроз безопасности информации в распределенных КС.
20. Основные понятия криптологии (открытый и шифртекст, криптография, криптология и криптоанализ, криптостойкость и ее характеристики).
21. Шифрование перестановкой, его достоинства и недостатки.

22. Шифрование подстановкой (моно- и многоалфавитной), его достоинства и недостатки.
23. Свойства абсолютно стойкого шифра.
24. Свойства однонаправленной функции.
25. Схема использования симметричной КС для создания защищенного канала связи.
26. Три группы способов аутентификации.

Уметь

1. Шифровать тексты с помощью классических шифров.
2. Использовать перестановки, подстановки и их комбинации.
3. Определять каналы утечки информации.
4. Определять преимущества и недостатки аппаратных и программных средств защиты информации.

Владеть

1. Методами и средствами защиты информации от утечки по каналам ПЭМИН.
2. Методами и средствами организационной защиты информации.
3. Основными методами и средствами защиты информации.

Повышенный уровень

Вопросы (задача, задание) для проверки уровня обученности.

Знать

1. Политика безопасности.
2. Побочные электромагнитные излучения и наводки (ПЭМИН).
3. Системно-концептуальный подход защиты информации.
4. Международные договоры первого уровня правового обеспечения информационной безопасности.
5. Подзаконные акты второго уровня правового обеспечения информационной безопасности.
6. Государственные стандарты третьего уровня правового обеспечения информационной безопасности.
7. Локальные нормативные документы четвертого уровня правового обеспечения информационной безопасности.
8. Вспомогательные аппаратные средства защиты информации.
9. Вспомогательные программные средства защиты информации.
10. Основные категории требований к защищенности КС из «Оранжевой книги».
11. Основные способы несанкционированного доступа к информации в КС.
12. Вспомогательные способы несанкционированного доступа к информации в КС.
13. Параметры политики учетных записей при использовании парольной аутентификации.

14. Двухфакторная аутентификация с элементами аппаратного обеспечения (диски, карты, маркеры и т.п.).
15. Процедура парольной инициализации.
16. Шифрование гаммированием, его достоинства и недостатки.
17. Потоковые и блочные шифры, их виды и характеристики.
18. Причины, облегчающие нарушителю реализацию угроз безопасности информации в распределенных КС.
19. Схема использования симметричного и асимметричного шифрования для создания защищенного канала связи.
20. Классы защищенности КС из «Оранжевой книги».
21. Группы классов защищенности АС из документов Гостехкомиссии России.
22. Основные функции системы разграничения доступа.
23. Функции обеспечивающих средств для системы разграничения доступа.
24. Правила противодействия системы попыткам подбора пароля.
25. Правила ввода или смены пароля пользователем.

Уметь
1. Описывать модель нарушителя.
2. Выбирать разновидности межсетевых экранов.
3. Осуществлять анализ рисков информационной безопасности предприятия.

Владеть
1. Приемами противодействия системы попыткам подбора пароля.
2. Методами создания безопасных распределенных КС.
3. Способами создания структуры обеспечения информационной безопасности организации.
4. Способами отражения атак на криптографические протоколы.

Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал, все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

Описание шкалы оценивания

Промежуточная аттестация в форме **экзамена** предусматривает проведение обязательной экзаменационной процедуры и оценивается 45 баллами из 100. Минимальное количество баллов, необходимое для допуска к экзамену, составляет 33 балла. Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **45** (**20**$\leq S_{экз} \leq$**45**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
37 – 45	Отлично
28 – 36	Хорошо
20 – 27	Удовлетворительно

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

Процедура проведения **экзамена** осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ.

В экзаменационный билет включаются два теоретических вопроса.

Для подготовки по билету отводиться от 40 до 60 минут.

При подготовке к ответу студенту предоставляется право пользования собственными лекциями, а также любой справочной литературой в течение 3-5 минут.

Составитель _____ И.В. Калиберда
(подпись)

«____»_____20 г.

№ п/п	Ф.И.О. студента	Параметры состояния образованности									Итоговый балл
		Предметно-информационная составляющая образованности				Деятельностно-коммуникативная составляющая образованности			Ценностно-ориентационная составляющая образованности		
		Контрольно-методический срез	Общеучебные умения и навыки			Уровень развития устной речи	Умение работать с информацией	Грамотность	Умение использовать полученные знания в повседневной жизни	Уровень адекватности самооценки	
			Умение анализировать	Умение доказывать	Умение делать выводы						
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											

Составитель _____ И.В.Калиберда
(подпись)

«____»_____20 г.