МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

**УТВЕРЖДАЮ**
Зам. директора по учебной работе
Пятигорского института (филиал)
СКФУ
Н.В. Данченко

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

# КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

| | |
|---|---|
| Направление подготовки | 10.03.01 Информационная безопасность |
| Направленность (профиль) | Безопасность компьютерных систем |
| Год начала обучения | 2025 |
| Форма обучения | очная |
| Реализуется в семестре | 7, 8 |

Пятигорск 2025 г.

**Введение**

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Научно-исследовательская работа ». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информации о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.
2. ФОС является приложением к программе дисциплины «Научно-исследовательская работа » и в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 Информационная безопасность.

3. Разработчик: Першин И.М., профессор кафедры систем управления и информационных технологий, доктор технических наук, профессор

4. Проведена экспертиза ФОС.
Члены экспертной группы:

Председатель _____
(*Ф.И.О., должность*)
Члены комиссии: _____
(*Ф.И.О., должность*)
_____
(*Ф.И.О., должность*)

Представитель организации-работодателя _____
(*Ф.И.О., должность*)

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 Информационная безопасность и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Научно-исследовательская работа ».
«____»_____ 2025 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

## 1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

| Компетенция (ии), индикатор (ы) | Уровни сформированности компетенци(ий) | | | |
|---|---|---|---|---|
| | Минимальный уровень не достигнут (Неудовлетворительно) 2 балла | Минимальный уровень (удовлетворительно) 3 балла | Средний уровень (хорошо) 4 балла | Высокий уровень (отлично) 5 баллов |
| *Компетенция: ОПК-9(ИД-1,2,3)* | | | | |
| ИД-1 ОПК-9 Понимать корректность криптографической алгоритмов в современных программных комплексах. | Не понимает корректность криптографической алгоритмов в современных программных комплексах. | недостаточно понимает корректность криптографической алгоритмов в современных программных комплексах. | Достаточно понимает корректность криптографической алгоритмов в современных программных комплексах. | В совершенстве понимает корректность криптографической алгоритмов в современных программных комплексах. |
| ИД-2 ОПК-9 Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. | Не Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. | недостаточно Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. | Достаточно Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. | В совершенстве Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. |
| ИД-3 ОПК-9 Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах. | Не Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах. | недостаточно Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах. | Достаточно Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах. | В совершенстве Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах. |
| *Компетенция: ОПК-12(ИД-1,2,3)* | | | | |
| ИД-1 ОПК-12 Понимает принципы работы средств обеспечения защиты | Не понимает принципы работы средств обеспечения защиты информации; | Недостаточно понимает принципы работы средств обеспечения | Достаточно понимает принципы работы средств обеспечения защиты | В совершенстве понимает принципы работы средств обеспечения защиты |

| | | | | |
|---|---|---|---|---|
| информации; основные стандарты информационной безопасности; общие принципы организации информационных систем. | основные стандарты информационной безопасности; общие принципы организации информационных систем. | защиты информации; основные стандарты информационной безопасности; общие принципы организации информационных систем. | информации; основные стандарты информационной безопасности; общие принципы организации информационных систем. | информации; основные стандарты информационной безопасности; общие принципы организации информационных систем. |
| ИД-2 ОПК-12 Способен готовить исходные данные для проектирования информационных систем. | Не способен готовить исходные данные для проектирования информационных систем. | Недостаточно способен готовить исходные данные для проектирования информационных систем. | Достаточно способен готовить исходные данные для проектирования информационных систем. | В совершенстве способен готовить исходные данные для проектирования информационных систем. |
| ИД-3 ОПК-12 Владеет методами экономического обоснования проектных решений в области информационной безопасности; методами оценки рисков; методами предотвращения угроз конфиденциальности, целостности и доступности информации. | Не владеет методами экономического обоснования проектных решений в области информационной безопасности; методами оценки рисков; методами предотвращения угроз конфиденциальности, целостности и доступности информации. | Недостаточно владеет методами экономического обоснования проектных решений в области информационной безопасности; методами оценки рисков; методами предотвращения угроз конфиденциальности, целостности и доступности информации. | Достаточно владеет методами экономического обоснования проектных решений в области информационной безопасности; методами оценки рисков; методами предотвращения угроз конфиденциальности, целостности и доступности информации. | В совершенстве владеет методами экономического обоснования проектных решений в области информационной безопасности; методами оценки рисков; методами предотвращения угроз конфиденциальности, целостности и доступности информации. |
| *Компетенция: ОПК-1.4(ИД-1,2,3)* | | | | |
| **ИД1 ОПК-1.4** Знает процедуру анализа информационной безопасности | Не Знает процедуру анализа информационной | Недостаточно Знает процедуру анализа информацион | Достаточно Знает процедуру анализа информационн | В совершенстве Знает процедуру анализа информационной безопасности |

| | | | | |
|---|---|---|---|---|
| компьютерных систем и сетей на соответствие требованиям стандартов | безопасности компьютерных систем и сетей на соответствие требованиям стандартов | ной безопасности компьютерных систем и сетей на соответствие требованиям стандартов | ой безопасности компьютерных систем и сетей на соответствие требованиям стандартов | компьютерных систем и сетей на соответствие требованиям стандартов |
| **ИД1 ОПК-1.4** Умеет проводить процедуру анализа информационной безопасности компьютерных систем и сетей на соответствие требованиям стандартов | Не Умеет проводить процедуру анализа информационн ой безопасности компьютерных систем и сетей на соответствие требованиям стандартов | Недостаточно Умеет проводить процедуру анализа информацион ной безопасности компьютерны х систем и сетей на соответствие требованиям стандартов | Достаточно Умеет проводить процедуру анализа информационн ой безопасности компьютерных систем и сетей на соответствие требованиям стандартов | В совершенстве Умеет проводить процедуру анализа информационно й безопасности компьютерных систем и сетей на соответствие требованиям стандартов |
| **ИД1 ОПК-1.4** Имеет практический опыт применения методов анализа информационной безопасности компьютерных систем и сетей на соответствие требованиям стандартов | Не Имеет практический опыт применения методов анализа информационн ой безопасности компьютерных систем и сетей на соответствие требованиям стандартов | Недостаточно Имеет практический опыт применения методов анализа информацион ной безопасности компьютерны х систем и сетей на соответствие требованиям стандартов | Достаточно Имеет практический опыт применения методов анализа информационн ой безопасности компьютерных систем и сетей на соответствие требованиям стандартов | В совершенстве Имеет практический опыт применения методов анализа информационно й безопасности компьютерных систем и сетей на соответствие требованиям стандартов |

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

## ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

| Номер задания | Правильный ответ | Содержание вопроса | Компетенция |
|---|---|---|---|
| | | **Форма обучения ОФО семестр 7, 8** | |
| 1. | | Понятие и сущность КСЗИ | ОПК-9 |
| 2. | | Перечислите методологические основы организации КСЗИ | ОПК-9 |
| 3. | | Методика определения состава защищаемой информации | ОПК-9 |
| 4. | | Значение носителей защищаемой информации как объектов защиты | ОПК-9 |
| 5. | | Как происходит определение источников дестабилизирующего воздействия на информацию и видов их воздействия? | ОПК-9 |
| 6 | | В чем заключается методика выявления каналов несанкционированного доступа к информации? | ОПК-9 |
| 7 | | Обеспечение полноты составляющих защиты | ОПК-9 |
| 8 | | Понятие модели объекта, основные виды моделей и их характеристика | ОПК-9 |
| 9. | | Модель как инструмент количественного и качественного анализа комплексной системы защиты информации | ОПК-9 |
| 10. | | Общее содержание работ по организации комплексной системы защиты информации | ОПК-9 |
| 11. | | В чем заключается организационное построение комплексной системы защиты информации? | ОПК-9 |

| | | | |
|---|---|---|---|
| 12. | | Как происходит определение состава кадрового обеспечения функционирования комплексной системы защиты информации? | ОПК-9 |
| 13. | | Значение материально-технического обеспечения функционирования комплексной системы защиты информации | ОПК-9 |
| 14. | | Понятие нормативно-методического обеспечения комплексной системы защиты информации | ОПК-9 |
| 15. | | Понятие и цели управления комплексной системы защиты информации | ОПК-9 |
| 16. | | Назовите особенности функций управления комплексной системой защиты информации | ОПК-12 |
| 17. | | Понятие и задачи планирования функционирования комплексной системы защиты информации | ОПК-12 |
| 18. | | Понятие и виды контроля функционирования комплексной системы защиты информации | ОПК-12 |
| 19. | | Понятие и основные виды чрезвычайных ситуаций | ОПК-12 |
| 20. | | Приведите классификацию подходов к оценке эффективности систем защиты информации | ОПК-12 |
| 21. | | Приведите классификационную структуру методов и моделей оценки | ОПК-12 |
| 22. | | В чём состоит назначение КСЗИ? | ОПК-12 |
| 23. | | КСЗИ как сложная человеко-машинная система | ОПК-12 |

| | | | |
|---|---|---|---|
| 24. | | Охарактеризуйте этапы работы по выявлению состава защищаемой информации. | ОПК-12 |
| 25. | | В чем заключается методика выявления состава носителей защищаемой информации? | ОПК-12 |
| 26. | | В чем заключается методика выявления способов воздействия на информацию? | ОПК-12 |
| 27. | | Определение возможных методов несанкционированного доступа к защищаемой информации | ОПК-12 |
| 28. | | Перечислите факторы и обстоятельства, оказывающих влияние на качество защиты | ОПК-12 |
| 29. | | Значение моделирования процессов комплексной системы защиты информации | ОПК-12 |
| 30. | | Технологическое построение комплексной системы защиты информации | ОПК 1.4 |
| 31. | | Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними. | ОПК 1.4 |
| 31. | | Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними. | ОПК 1.4 |
| 32. | | Как происходит определение состава материально-технического обеспечения? От чего он зависит? | ОПК 1.4 |

| | | | |
|---|---|---|---|
| 33. | | Охарактеризуйте структуру нормативно-методического обеспечения комплексной системы защиты информации | ОПК 1.4 |
| 34. | | В чем сущность процессов управления комплексной системы защиты информации? | ОПК 1.4 |
| 35. | | Содержание функций управления комплексной системой защиты информации | ОПК 1.4 |
| 36. | | Перечислите и охарактеризуйте способы и стадии планирования | ОПК 1.4 |
| 37. | | Какова цель проведения контрольных мероприятий в комплексной системе защиты информации? | ОПК 1.4 |
| 38. | | Перечислите факторы, влияющие на принятие решений в условиях чрезвычайной ситуации | ОПК 1.4 |
| 39. | | Вероятностный подход: структуризация предметной области оценки, анализ вероятности реализации угроз безопасности, расчетные соотношения | ОПК 1.4 |
| 40. | | Перечислите базовые понятия и определения, используемые в моделях. | ОПК 1.4 |
| 41. | верно | Укажите верно или неверно представленное положение:<br>КСЗИ предприятия есть совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации | ОПК 1.4 |
| 42. | верно | Укажите верно или неверно представленное положение:<br>Главной целью КСЗИ является обеспечение непрерывности, устойчивого функционирования предприятия и предотвращения угроз его безопасности. | ОПК 1.4 |
| 43. | a<br>b<br>c | Выберите один или несколько ответов:<br>Комплексная система защиты информации направлена:<br>а) на защиту законных интересов организации от | ОПК-9 |

| | | | |
|---|---|---|---|
| | | противоправных посягательств<br>b) недопущение уничтожения имущества и ценностей<br>c) недопущение разглашения, утечки и несанкционированного доступа к служебной информации<br>d) изоляции работы технических средств обеспечения производственной деятельности, включая информационные технологии | |
| 44. | a<br>b<br>c<br>d | Выберите один или несколько ответов:<br>К задачам КСЗИ, можно отнести:<br>a) прогнозирование, своевременное выявление и устранение угроз безопасности персоналу и ресурсам предприятия, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития<br>b) эффективное пресечение угроз персоналу и посягательств на ресурсы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности<br>c) отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов — к различным уровням уязвимости (опасности), подлежащих сохранению<br>d) создание механизма и условий оперативного реагирования на угрозы безопасности проявления негативных тенденций в функционировании предприятия<br>e) создание условий для исключения возмещения и локализации наносимого ущерба неправомерными действиями | ОПК-9 |
| 45. | a<br>b<br>c<br>d | Выберите один или несколько ответов:<br>Обеспечение безопасности предприятия должно основываться на следующих основных принципах:<br>a) Принцип своевременности<br>b) Принцип комплексности | ОПК-9 |

| | | | |
|---|---|---|---|
| | | c) Принцип непрерывности<br>d) Принцип системности<br>e) Принцип сложности применения | |
| 46. | a<br>b<br>c<br>d | Выберите один или несколько ответов:<br>Информация — это:<br>a) сведения о явлениях и процессах независимо от формы их представления b) сведения о лицах<br>c) упорядоченный набор структурированной информации<br>d) сведения о предметах<br>e) сведения о фактах и событиях | ОПК-9 |
| 47. | a<br>b<br>c | Выберите один или несколько ответов:<br>С точки зрения потребителя качество используемой информации позволяет:<br>a) получать дополнительный моральный эффект<br>b) получать дополнительный физический эффект<br>c) получать дополнительный информационный эффект<br>d) получать дополнительный экономический эффект | ОПК-9 |
| 48. | a<br>b<br>c<br>d | Выберите один или несколько ответов:<br>Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют:<br>a) наличие значительного практического опыта и наработок<br>b) весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе<br>c) не достаточно четко очерченная система взглядов на эту проблему<br>d) значительное число фирм, специализирующихся на решении | ОПК-9 |
| 49. | a<br>b<br>c | Выберите один или несколько ответов:<br>Защита информации – это:<br>a) деятельность, направленная на предотвращение утечки защищаемой информации | ОПК-9 |

| | | | |
|---|---|---|---|
| | | b) деятельность, направленная на организационное и техническое сопровождение информационных процессов в организации<br>c) деятельность, направленная на предотвращение несанкционированных воздействий на защищаемую информацию<br>d) деятельность, направленная на предотвращение непреднамеренных воздействий на защищаемую информацию | |
| 50. | a<br>b<br>c<br>d | Выберите один или несколько ответов:<br>Организация и функционирование комплексной системы безопасности должны осуществляться на основе следующих принципов:<br>a) Оперативность<br>b) Своевременность<br>c) Комплексность<br>d) Непрерывность<br>e) Активность | ОПК-9 |
| 51. | Неверно | Выберите один ответ:<br>Обеспечение безопасности информации - это фрагментарный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких мест и потенциальных угроз фирме. | ОПК-9 |
| 52. | Неверно | Выберите один ответ:<br>Информационная безопасность может быть обеспечена лишь при избирательном использовании арсенала средств защиты и противодействия во всех структурных элементах производственной системы | ОПК-9 |
| 53. | Неверно | Выберите один ответ:<br>Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм | ОПК-12 |
| 54. | Верно | Выберите один ответ:<br>Никакая фирма не может обеспечить требуемый уровень безопасности без надлежащий подготовки персонала и пользователей, соблюдения ими всех | ОПК-12 |

| | | | |
|---|---|---|---|
| | | установленных правил, направленных на обеспечение информационной безопасности. | |
| 55. | a<br>b<br>c | Выберите один или несколько ответов:<br>Организация и функционирование комплексной системы защиты информации осуществляется на основе принципа комплексности, сущность которого состоит:<br>a) в упреждающем характере мер обеспечения информационной безопасности<br>b) в обеспечении безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования<br>c) в способности системы к развитию и совершенствованию в соответствии с изменениями условий функционирования фирмы<br>d) в обеспечении безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями | ОПК-12 |
| 56. | b<br>c<br>d | Выберите один или несколько ответов:<br>Своевременность предполагает постановку задач:<br>a) на основе анализа обстановки<br>b) на стадиях разработки системы безопасности в режиме реального времени<br>c) на основе разработки эффективных мер предупреждения посягательств на законные интересы<br>d) на основе прогнозирования обстановки | ОПК-12 |
| 57. | c<br>d | Выберите один или несколько ответов:<br>Комплексная система защиты информации на предприятии – это:<br>a) совокупность мероприятий, осуществляемых в целях защиты предприятия от реальных или потенциальных действий физических или юридических лиц, которые могут привести к существенным потерям<br>b) совокупность мероприятий исключительно правового характера | ОПК-12 |

| | | | |
|---|---|---|---|
| | | c) совокупность взаимосвязанных мероприятий организационно-правового характера<br>d) совокупность мероприятий исключительно технического характера | |
| 58. | a<br>b<br>c | Выберите один или несколько ответов:<br>Целями комплексной системы защиты информации являются:<br>a) Создание условий для коренного изменения технологического процесса на предприятии<br>b) Повышение имиджа и роста прибылей за счет обеспечения качества услуг и безопасности клиентов<br>c) Защита прав предприятия, его структурных подразделений и сотрудников<br>d) Сохранение и эффективное использование финансовых, материальных и информационных ресурсов | ОПК-12 |
| 59. | a<br>b<br>d | Выберите один или несколько ответов:<br>Задачами комплексной системы защиты информации являются:<br>a) Своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам фирмы, нарушению ее нормального функционирования и развития<br>b) Создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании фирмы<br>c) Исключение пресечения посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности<br>d) Отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования) и других ресурсов — к различным уровням уязвимости (опасности) и подлежащих сохранению | ОПК-12 |
| 60. | a<br>b<br>c | Выберите один или несколько ответов:<br>К требованиям, предъявляемым к комплексной системе защиты информации | ОПК-12 |

| | | | |
|---|---|---|---|
| | | можно отнести:<br>a) Четкость определения полномочий и прав пользователей на доступ к определенным видам информации<br>b) Сведения к минимуму числа общих для нескольких пользователей средств защиты<br>c) Учет случаев и попыток НСД к конфиденциальной информации<br>d) Исключение предоставления пользователям минимальных полномочий, необходимых для выполнения порученной работы | |
| 61. | Верно | Выберите один ответ:<br>Системы защиты информации относятся к классу сложных систем. | ОПК-12 |
| 62. | a<br>b<br>c | Выберите один или несколько ответов:<br>Для комплексных систем защиты информации характерны следующие принципы построения:<br>a) Фиксированная архитектура КСЗИ<br>b) Параллельная разработка комплексных систем и систем защиты информации<br>c) Многоуровневая структура построения КСЗИ<br>d) Системный подход к построению КСЗИ | ОПК-12 |
| 63. | a<br>b<br>c | Выберите один или несколько ответов:<br>Комплексность защиты информации позволяет использовать в оптимальном сочетании:<br>a) Технических методов и средств защиты<br>b) Программных методов и средств защиты<br>c) Нормативных методов защиты<br>d) Криптографических методов и средств защиты | ОПК-1.4 |
| 64. | Неверно | Выберите один ответ:<br>Комплексные системы защиты информации не должны иметь централизованное управление | ОПК-1.4 |

| | | | |
|---|---|---|---|
| 65. | a<br>b<br>c<br>d | Выберите один или несколько ответов:<br>Основными этапами создания КСЗИ являются:<br>a) Рабочее проектирование<br>b) Техническое проектирование<br>c) Организационное проектирование<br>d) Разработка технического задания<br>e) Эскизное проектирование | ОПК-1.4 |
| 66. | e | Выберите один или несколько ответов:<br>Современный опыт решения проблем информационной безопасности показывает, что для достижения наибольшего эффекта при организации защиты информации необходимо руководствоваться рядом принципов.<br>К какому принципу мы можем отнести это содержание:<br>a) принцип комплексности<br>b) принцип прозрачности<br>c) принцип непрерывности<br>d) принцип многоразовости<br>e) нет такого принципа | ОПК-1.4 |
| 67. | b | Выберите один или несколько ответов:<br>Современный опыт решения проблем информационной безопасности показывает, что для достижения наибольшего эффекта при организации защиты информации необходимо руководствоваться рядом принципов. К какому принципу мы можем отнести это содержание: использование всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла обработки информации<br>a) принцип комплексности<br>b) принцип прозрачности<br>c) принцип непрерывности<br>d) принцип многоразовости | ОПК-1.4 |
| 68. | a | Выберите один или несколько ответов:<br>Что характеризует это определение: организованная совокупность органов, средств, методов и мероприятий, обеспечивающих защиту информации | ОПК-1.4 |

| | | | |
|---|---|---|---|
| | | от разглашения, утечки и несанкционированного доступа к ней.<br>a) Информационная система<br>b) Информационная технология<br>c) Система информационной безопасности<br>d) Государственная система обеспечения безопасности | |
| 69. | a<br>b<br>c<br>d | Выберите один или несколько ответов:<br>К важнейшим условиям обеспечения информационной безопасности можно отнести:<br>a) ответственность персонала и руководства<br>b) соблюдение баланса интересов личности и предприятия<br>c) достаточность<br>d) законность<br>e) высокий профессионализм представителей службы информационной безопасности | ОПК-1.4 |
| 70. | c | Выберите один или несколько ответов:<br>С позиций системного подхода для реализации принципов обеспечения информационной безопасности процесс, да и сама система защиты информации должны отвечать некоторой совокупности требований, а именно:<br>a) активной<br>b) конкретной и целенаправленной<br>c) стандартной<br>d) централизованной<br>e) плановой | ОПК-1.4 |

**2. Описание шкалы оценивания**

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на положениях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

*Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.*

**3. 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.