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

УТВЕРЖДАЮ
И.о. декана факультета
математики и компьютерных
наук имени профессора Н.И. Червякова
Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
«Основы информационной безопасности»

Специальность	Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	1

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Основы информационной безопасности». 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 «Основы информационной безопасности»

3. Разработчик: Лапина Мария Анатольевна, доцент кафедры вычислительной математики и кибернетики.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель

Бабенко М. Г. заведующий кафедрой вычислительной математики и кибернетики

Члены комиссии:

Пелешенко В.С. доцент кафедры вычислительной математики и кибернетики

Пелешенко Т. А. доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя Корниенко С. А. начальник управления филиала ФГУП «Главный радиочастотный центр» в Южном и Северо-Кавказском федеральных округах.

Экспертное заключение: фонд оценочных средств соответствует образовательной программе по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» и рекомендуется для проведения текущего контроля успеваемости и промежуточной аттестации студентов.

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**
ОПК-1. Способен оценивать роль информации, информационных технологий информационной безопасности в современном обществе, их значение обеспечения				
ИД-1ОПК-1 Понимает основные методологические принципы теории информационной безопасности; проблемы государственной и региональной информационной безопасности.	Не предоставляет отчёт с анализом роли информации и информационных технологий информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства	Предоставляет неполный отчёт с анализом роли информации и информационных технологий информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства.	Предоставляет отчёт с анализом роли информации и информационных технологий информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства.	Предоставляет отчёт с детальным анализом роли информации и информационных технологий информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства.
ИД-2ОПК-1 Применяет основные методологические принципы теории информационной безопасности.	Не предоставляет отчёт по результатам обеспечения информационной безопасности с использованием основных методологических принципов теории информационной безопасности.	Предоставляет неполный отчёт по результатам обеспечения информационной безопасности с использованием основных методологических принципов теории информацион	Предоставляет отчёт по результатам обеспечения информационной безопасности с использованием основных методологических принципов теории информационной безопасности.	Предоставляет детальный отчёт по результатам обеспечения информационной безопасности с использованием основных методологических принципов теории информационной безопасности.

		ной безопасности.		
ИД-3ОПК-1 Определяет роль информации, информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства.	Не предоставляет отчёт с анализом роли информации, информационн ой безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства	Предоставляе т неполный отчёт с неполным анализом роли информации, информацион но й безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства	Предоставляет отчёт с анализом роли информации, информационн о й безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства	Предоставляет детальный отчёт с детальным анализом роли информации, информационно й безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации				
ИД-1ОПК-5 Знаком с действующим законодательство м Российской Федерации в области информационной безопасности и защиты информации; системами защиты государственной тайны; определяет перечень сведений, относящихся к конфиденциально й информации и способы ее	Не предоставляет план по использованию Законодательст ва Российской Федерации в области информационн ой безопасности и защиты информации; систем защиты государственно й тайны с перечнем сведений относящихся к конфиденциаль	Предоставляе т не полный план по использовани ю Законодатель ства Российской Федерации в области информацион ной безопасности и защиты информации; систем защиты государствен ной тайны с перечнем сведений	Предоставляет план по использованию Законодательст в а Российской Федерации в области информационн о й безопасности и защиты информации; систем защиты государственн ой тайны с перечнем сведений относящихся к конфиденциал ьн ой информации и	Предоставляет детально проработанный план по использованию Законодательст ва Российской Федерации в области информационно й безопасности и защиты информации; систем защиты государственно й тайны с перечнем сведений относящихся к конфиденциаль но й

защиты; знаком с понятием и принципами электронной подписи (ЭП); определяет виды компьютерных вирусов; классифицирует компьютерные преступления; использует понятие и способы защиты интеллектуальной собственности; Знаком с действующим законодательством в области международного и российского права в области защиты информации; знаком со способами совершения преступлений в сфере компьютерной информации; знаком с правовыми режимами защиты информации.	ной информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.	относящихся к конфиденциальной информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятийи способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации	способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуально й собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.	информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.
ИД-2ОПК-5 Определяет рациональные меры по обеспечению организационной защите на	Не предоставляет план по организации защиты на объекте; организации	Предоставляет неполный план по организации защиты на объекте; организации	Предоставляет план по организации защиты на объекте; организации работы	Предоставляет детально проработанный план по организации защиты на объекте;

объекте; организует работу персонала с конфиденциальной информацией; разрабатывает проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.	работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов	работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующ их работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов	персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов	организации работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов
ИД-ЗОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	Не предоставляет отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Предоставляет неполный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующ ие деятельность по защите информации	Предоставляет отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Предоставляет детальный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

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
1.	a,b,c	Наиболее важными в практическом плане свойствами информации является: a) ценность b) достоверность c)своевременность d)практичность	ОПК-1, ОПК-5
2.	a,b,c	Основные виды информации по ее форме представления, способам ее кодирования и хранения^ a) графическая или изобразительная информация; b) звуковая информация; c) числовая информация; d) тактильная информация.	ОПК-1, ОПК-5
3.	a	Числовая информация? a) количественная мера объектов и их свойств в окружающем мире; b) информация, представленная в виде последовательности цифр.	ОПК-1, ОПК-5

4.	a	Текстовая информация - способ кодирования речи человека специальными символами - буквами? a) да; b) нет.	ОПК-1, ОПК-5
5.	a,b	В зависимости от носителей информация информационные ресурсы делятся на классы: a) документы всех видов, на любых видах носителей; b) персонал (память людей), обладающий знаниями и квалификацией в различных областях науки и техники; b) СМИ.	ОПК-1, ОПК-5

6.	a,b	В зависимости от носителей информация информационные ресурсы делятся на классы: a) научный инструментарий (в том числе автоматизированные системы научных исследований); b) промышленные образцы (любые материальные объекты, созданные в процессе производства); c) художественная литература.	ОПК-1, ОПК-5
7.	a,b,c	Для удовлетворения законных прав субъектов (обеспечения их информационной безопасности) необходимо постоянно поддерживать следующие свойства информации и систем ее обработки: a) доступность информации; b) целостность информации; c) конфиденциальность информации; d) актуальность информации.	ОПК-1, ОПК-5

8.	a	Информационные ресурсы - это вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях и в любой другой форме, обеспечивающей ее передачу во времени и пространстве между различными потребителями? a) да; b) нет	ОПК-1, ОПК-5
9.	a	Конфиденциальность информации – … a) субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации; b) существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)	ОПК-1, ОПК-5
10.	a,b	К защищаемой относят информацию: a) секретную (сведения, содержащие государственную тайну); b) конфиденциальную (сведения, содержащие коммерческую тайну, а также тайну, касающуюся личной, неслужебной деятельности граждан); c) сведения о загрязнениях окружающей среды.	ОПК-1, ОПК-5
		Под угрозой (вообще) обычно понимают …	

11.	a	потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам; b) сведения о фактах, событиях, процессах и явлениях, о состоянии объектов в некоторой предметной области. a) компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.	ОПК-1, ОПК-5
12.	d	Угрозы информационной безопасности АС: a) несанкционированное копирование носителей информации; b) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной; c) игнорирование организационных ограничений (установленных правил) при определении ранга системы; d) все ответы верны.	ОПК-1, ОПК-5

13.	a	Засекречивать информацию, т. е. ограничивать к ней доступ, может только её собственник или уполномоченное им на то лицо; a) да; b) нет.	ОПК-1, ОПК-5
14.	a	Целостность информации – … a) существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию); b) субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации.	ОПК-1, ОПК-5

15.	a,b,c	Причинами разрушения информации могут быть: a) компьютерные вирусы; b) несанкционированные действия; c) ошибки программ; d) резервное копирование	ОПК-1, ОПК-5
16.	a	Доступность информации – …	ОПК-1, ОПК-5
		a) свойство системы, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации; b) существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).	

17.	a,b,c	По доступности информация подразделяется на: a) общедоступную информацию; b) информацию ограниченного доступа; c) информацию, доступ к которой не может быть ограничен; d) абсолютно секретная.	ОПК-1, ОПК-5
18.	a,b,c	Открытая информация имеет следующие разновидности: a) информация как объект гражданских прав; b) массовая информация; c) официальные документы; d) информация о гражданах.	ОПК-1, ОПК-5

19.	a,b,c	Информация ограниченного доступа может быть представлена в следующих видах: a) информация о гражданах; b) информация, содержащая государственную тайну; c) информация, составляющая коммерческую тайну; d) научно-юридическая информация.	ОПК-1, ОПК-5
20.	a	Должностные лица обязаны предоставлять по запросам граждан ... a) общедоступную информацию; b) информацию с ограниченным доступом; c) информацию, не подлежащая распространению.	ОПК-1, ОПК-5
21.	a,b	Информация, которая не может быть отнесена к конфиденциальной, но в то же время она требует ограничения своего распространения в силу негативного влияния на состояние общества?	ОПК-1, ОПК-5

		a) информация, не подлежащая распространению; b) Информация с ограниченным доступом; c) информация, доступ к которой не может быть ограничен.	
22.	b	Под угрозой (вообще) обычно понимают компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления? a) да; b) нет.	ОПК-1, ОПК-5
23.	a,b	Под информацией понимается: a) сведения о фактах, событиях, процессах и явлениях, о состоянии объектов в некоторой предметной области; b) набор последовательностей 0,1; c) набор символов алфавита.	ОПК-1, ОПК-5

24.	a	Под угрозой (вообще) обычно понимают потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам? a) да; b) нет.	ОПК-1, ОПК-5
25.	a	Естественные угрозы– … a) угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, не зависящих от человека; b) угрозы информационной безопасности АС, вызванные деятельностью человека.	ОПК-1, ОПК-5
26.	a	Что такое утечка информации a) бесконтрольный выход за пределы организации (территории, здания, помещения) или крута лиц, которым она была доверена b) возможность возникновения на каком-либо этапе жизнедеятельности	ОПК-1, ОПК-5

		системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию c) не предоставление иформации d) бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц e) правильного ответа нет	
27.	c,e,f	Основные причины утечки информации a) Хищение носителей информации b) НСД c) Ведение противостоящей стороной технической и агентурной разведок d) Ошибки в процессе обработки информации e) Несоблюдение персоналом норм, требований, правил эксплуатации АС f) Ошибки в проектировании АС и защиты АС	ОПК-1, ОПК-5

28.	a,b,c	К Электромагнитным каналам утечки информации относятся a) Радиоканал b) Низкочастотный канал c) Канал заземления d) Телефонный канал e) Канал разведывательный	ОПК-1, ОПК-5
29.	a,c,d	К Информационным каналам утечки информации относятся a) Канал коммутируемых линий связи b) Канал аудиальный c) Канал выделенных линий связи d) Канал локальной сети e) Канал визуальный	ОПК-1, ОПК-5
30.	a	ПЭМИ это a) паразитные электромагнитные излучения радиодиапазона,	ОПК-1, ОПК-5

		создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными b) побочных электромагнитных излучений технических средств приема, обработки, хранения и передачи информации	

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 требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

3. Критерии оценивания компетенций

Оценка «**отлично**» выставляется студенту, если: Предоставляет отчёт с детальным анализом роли информации и информационных технологий информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства. Предоставляет детальный отчёт по результатам обеспечения информационной безопасности с использованием основных методологических принципов теории информационной безопасности. Предоставляет детальный отчёт с детальным анализом роли информации, информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства. Предоставляет детально проработанный план по использованию Законодательства Российской Федерации в области информационной безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциально й информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации. Предоставляет детально проработанный план по организации защиты на объекте; организации работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующи х работу по защите информации, а также положений, инструкций и других организационно-распорядительны х документов. Предоставляет детальный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующи е деятельность по защите информации.

Оценка «**хорошо**» выставляется студенту в случае, когда он: Предоставляет отчёт с анализом роли информации и информационны х технологий информационно й безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства. Предоставляет отчёт по результатам обеспечения информационно й безопасности с использованием основных методологическ их принципов теории информационной безопасности. Предоставляет отчёт с анализом роли информации, информационно й безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства. Предоставляет план по использованию Законодательств а Российской Федерации в области информационно й безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциальн ой информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуально й собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации. Предоставляет план по организации защиты на объекте; организации работы персонала с конфиденциальн ой

информацией; разработке проектов нормативных документов, регламентирую щих работу по защите информации, а также положений, инструкций и других организационно-распорядительн ых документов. Предоставляет отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирую щие деятельность по защите информации.

Оценка «**удовлетворительно**» выставляется студенту, если он: Предоставляет неполный отчёт с анализом роли информации и информационных технологий информационно й безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства. Предоставляет неполный отчёт по результатам обеспечения информационно й безопасности с использованием основных методологическ их принципов теории информационной безопасности. Предоставляет неполный отчёт с неполным анализом роли информации, информационно й безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства. Предоставляет не полный план по использованию Законодательства Российской Федерации в области информационной безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциальной информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятийи способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации. Предоставляет неполный план по организации защиты на объекте; организации работы персонала с конфиденциальн ой информацией; разработке проектов нормативных документов, регламентирую щих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. Предоставляет неполный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирую щие деятельность по защите информации.

Оценка «**неудовлетворительно**» выставляется, если студент: Не предоставляет отчёт с анализом роли информации и информационных технологий информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства. Не предоставляет отчёт по результатам обеспечения информационной безопасности с использованием основных методологических принципов теории информационной безопасности. Не предоставляет отчёт с анализом роли информации, информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства. Не предоставляет план по использованию Законодательства Российской Федерации в области информационной безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциальной информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации. Не предоставляет план по организации защиты на объекте; организации работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно- распорядительных документов. Не предоставляет отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.