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
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Нормативные документы и стандарты по информационной безопасности

Направление подготовки	10.03.01 «Информационная безопасность»
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	6

Введение

1. Назначение. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Нормативные документы и стандарты по информационной безопасности» студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

2. ФОС является приложением к программе дисциплины (модуля) «Нормативные документы и стандарты по информационной безопасности» в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

3. Разработчик (и) Бисюков В.М., доцент кафедры

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены комиссии: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «СГУ-Инфоком»

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Нормативные документы и стандарты по информационной безопасности».

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 компетенции(й),			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ПК-4 Способен внедрять системы защиты информации в автоматизированных системах				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-1 разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах	На низком уровне знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации	В основном знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации	Знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации	В полном объёме знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации
ИД-2 внедряет организационные меры по защите информации в автоматизированных системах	На низком уровне знает состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах. Умеет внедрять организационные меры в систему защиты автоматизированной системы организации	В основном знает состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах. Умеет внедрять организационные меры в систему защиты автоматизированной системы организации	Знает состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах. Умеет внедрять организационные меры в систему защиты автоматизированной системы организации	В полном объёме знает состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах. Умеет внедрять организационные меры в систему защиты автоматизирован

				ной системы организации

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 очная, семестр 6	
1.	b	Сколько всего принципов положено ФЗ №52 в обработку персональных данных (ПДн): a) 2, b) 3, c) 4, d) 5.	ПК-4
2.	b	Всегда ли, при обработке ПДн, необходимо соблюдать требования их конфиденциальности: a) да, b) нет.	ПК-4
3.	c	В какой статье ФЗ №52 изложены меры по обеспечению безопасности ПДн: a) 17, b) 18, c) 19, d) 20.	ПК-4
4.	b	Кто устанавливает уровни защищённости ПДн, в соответствии с требованиями ФЗ №52: a) президент, b) правительство РФ, c) оператор ПДн, d) ФЗ.	ПК-4
5.	c	Каким постановлением правительства РФ устанавливаются особенности обработки ПДн без использования средств автоматизации: a) №211, b) №1119, c) №687, d) №17	ПК-4
6.	a	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, это: a) информационные технологии, b) информационная система, c) информационная телекоммуникационная система, d) автоматизированная система.	ПК-4

7.	a	Информация в зависимости от категории доступа к ней подразделяется на: a) 2 вида, b) 3 вида, c) 4 вида, d) 5 видов.	ПК-4
8.	c	Информация в зависимости от порядка ее предоставления или распространения подразделяется на: a) 2 вида, b) 3 вида, c) 4 вида, d) 5 видов.	ПК-4
9.	b	Гражданин имеет право на получение от государственных органов: a) любой информации, b) только информации непосредственно затрагивающей его права и свободы, c) информации касающейся всего общества в целом.	ПК-4
10.	c	Условия отнесения информации к сведениям, составляющим тайну, устанавливаются: a) правительством, b) президентом, c) федеральными законами, d) первым руководителем предприятия.	ПК-4
11.	b	Сколько всего видов информационных систем: a) 2, b) 3, c) 4, d) 5.	ПК-4
12.	b	Сколько групп мер входит в процесс защиты информации: a) 2, b) 3, c) 4, d) 5.	ПК-4
13.	c	Какие, из перечисленных, групп мер не входят в процесс защиты информации: a) правовые, b) организационные,	ПК-4

		c) административные, d) технические.	
14.	b	Действие или бездействие, в результате которых информация, составляющая КТ становится известной третьим лицам без согласия обладателя такой информации, это: a) утечка информации, b) разглашение информации, c) утеря информации, d) несанкционированный доступ.	ПК-4
15.	b	Режим коммерческой тайны может быть установлен: a) к любой информации в фирме, b) не любой информации в фирме.	ПК-4
16.	d	Сколько мер необходимо осуществить, чтобы обеспечить сохранность конфиденциальной информации: a) 3, b) 4, c) 5, d) 6.	ПК-4
17.	c	Максимальный срок уголовного преследования за нарушения работником режима КТ: a) 3 года, b) 5 лет, c) 7 лет, d) 10 лет.	ПК-4
18.	c	Кем разрабатывается перечень сведений, составляющих КТ: a) руководителем фирмы, b) начальником службы делопроизводства, c) специальной комиссией, d) службой защиты информации.	ПК-4
19.	b	Кто проводит экспертизу ценности конфиденциальных документов: a) служба безопасности, b) постоянно действующая экспертная комиссия, c) отдел конфиденциального делопроизводства.	ПК-4
20.	c	Разрешение на доступ к конкретной конфиденциальной информации может быть дано при соблюдении:	ПК-4

		a) 3-х условий, b) 4-х условий, c) 5-ти условий, d) 6-ти условий.	
21.	a	Сколько всего основных документов, регламентирующих правовые отношения собственника конфиденциальной информации с работниками предприятия: a) 3, b) 4, c) 5, d) 6.	ПК-4
22.	b	На материальные носители, содержащие коммерческую тайну, наносится гриф конфиденциальности: a) служебная тайна, b) коммерческая тайна, c) для служебного пользования, d) секретно.	ПК-4
23.	c	На материальные носители, содержащие сведения, отнесенные к служебной тайне, наносится гриф конфиденциальности: a) служебная тайна, b) коммерческая тайна, c) для служебного пользования, d) секретно.	ПК-4
24.	a	Сколько всего направлений обеспечения информационной безопасности: a) 3, b) 4, c) 5, d) 6.	ПК-4
25.	d	Какого, из перечисленных, направлений обеспечения информационной безопасности нет: a) организационная защита, b) правовая защита, c) инженерно-техническая защита, d) компьютерная защита.	ПК-4

26.	c	Сколько всего блоков в структуре правовых актов, ориентированных на правовую защиту информации: a) 5, b) 6, c) 7, d) 8.	ПК-4
27.	a	Порядок построения системы защиты информации в ГИС определяет приказ №: a) 17, b) 21, c) 31, d) все перечисленные.	ПК-4
28.	b	Меры защиты информации в ГИС направлены на защиту: a) 2-х свойств информации, b) 3-х, c) 4-х.	ПК-4
29.	a	Сколько групп организационных и технических мер определяет приказ ФСТЭК №17: a) 13, b) 15, c) 23.	ПК-4
30.	a	Модель угроз разрабатывается при: a) уточнении базовых мер защиты, b) адаптации базовых мер защиты, c) усилении базовых мер защиты.	ПК-4
31.	b	Сколько всего классов защиты ГИС: a) 2, b) 3, c) 4.	ПК-4
32.	b	Базовый набор мер защиты в ГИС по приказу 17 определяется исходя из: a) уровня защищённости, b) класса защищённости, c) степени ущерба.	ПК-4
33.	b	Структурно-функциональные характеристики ГИС определяются на этапе: a) уточнении базовых мер защиты, b) адаптации базовых мер защиты, c) усилении базовых мер защиты.	ПК-4
34.	a	Банк угроз ФСТЭК применяется на этапе: a) уточнении базовых мер защиты,	ПК-4

		b) адаптации базовых мер защиты, c) усилении базовых мер защиты.	
35.	a	Сколько всего направлений нормативного регулирования деятельности по защите информации: a) 2, b) 3, c) 4, d) 5.	ПК-4
36.	b	Без применения аппаратного или программного обеспечения реализуются: a) нормативные меры защиты, b) организационные меры защиты, c) правовые меры защиты, d) технические меры защиты.	ПК-4
37.	b	Такая мера защиты информации, как ограничение доступа лиц на территорию относится к: a) нормативным мерам защиты, b) организационным мерам защиты, c) правовым мерам защиты, d) техническим мерам защиты.	ПК-4
38.	c	Всего подсистем в составе системы защиты информации: a) 2, b) 3, c) 4, d) 5.	ПК-4
39.	b	Какой, из перечисленных, подсистемы защиты информации не существует: a) управления доступом, b) антивирусной, c) криптографической, d) обеспечения целостности	ПК-4
40.	c	Всего классов защищённости для средств вычислительной техники (СВТ): a) 4, b) 5, c) 6, d) 7.	ПК-4

41.		Зарубежное законодательство в области информационной безопасности	ПК-4
42.		Российское законодательство в области информационной безопасности	ПК-4
43.		Международная организация по стандартизации ISO. История создания и организационная структура	ПК-4
44.		Международная организация по стандартизации ISO. Состав комитетов и их деятельность.	ПК-4
45.		Федеральная служба по техническому и экспортному контролю РФ (ФСТЭК). История создания и решаемые задачи	ПК-4
46.		ФЗ «О государственной тайне». Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты	ПК-4
47.		ФЗ «О государственной тайне». Перечень сведений, составляющих государственную тайну. Прядок отнесения сведений к категории государственная тайна	ПК-4
48.		ФЗ «О государственной тайне». Порядок защиты государственной тайны.	ПК-4
49.		ФЗ «Об информации, информационных технологиях и о защите информации».Основные положения. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.	ПК-4
50.		ФЗ «Об информации, информационных технологиях и о защите информации». Информация, как объект правовых отношений.	ПК-4
51.		ФЗ «Об информации, информационных технологиях и о защите информации». Государственное регулирование в сфере применения информационных технологий. Информационные системы.	ПК-4
52.		ФЗ «Об информации, информационных технологиях и о защите информации».Защита информации. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.	ПК-4
53.		ФЗ «О коммерческой тайне». Основные положения закона. Термины и определения.	ПК-4
54.		ФЗ «О коммерческой тайне». Понятие режима коммерческой тайны.	ПК-4
55.		ФЗ «О персональных данных». Общие положения и терминология закона.	ПК-4
56.		ФЗ «О персональных данных». Принципы и условия обработки персональных данных	ПК-4

57.		ФЗ «О персональных данных». Конфиденциальность персональных данных	ПК-4
58.		ФЗ «О персональных данных». Меры по обеспечению безопасности персональных данных при их обработке	ПК-4
59.		ФЗ «О техническом регулировании». Общие положения и терминология закона.	ПК-4
60.		ФЗ «О техническом регулировании». Принципы технического регулирования	ПК-4
61.		ФЗ «О техническом регулировании». Цели и принципы стандартизации.	ПК-4
62.		ФЗ «О техническом регулировании». Формы подтверждения соответствия.	ПК-4
63.		ФЗ «О цифровой подписи». Общее положения и терминология закона	ПК-4
64.		ФЗ «О цифровой подписи». Принципы использования электронной подписи.	ПК-4
65.		ФЗ «О цифровой подписи». Виды электронных подписей и порядок их использования	ПК-4
66.		ФЗ «О цифровой подписи». Средства электронной подписи. Сертификат ключа проверки электронной подписи	ПК-4
67.		Понятие и правовые основы стандартизации в РФ.	ПК-4
68.		Понятие и правовые основы сертификации в РФ.	ПК-4
69.		Контроль за сертифицированными продукцией, работами и услугами в РФ.	ПК-4
70.		Система стандартов по защите информации ГОСТ Р 52069.0. Назначение, состав и основные термины документа.	ПК-4
71.		Система стандартов по защите информации ГОСТ Р 52069.0. Структура системы стандартов по защите информации	ПК-4
72.		Система менеджмента информационной безопасности ISO/IEC 27001. Разработка системы менеджмента информационной безопасности. Управление системой менеджмента информационной безопасности	ПК-4
73.		Система менеджмента информационной безопасности ISO/IEC 27001. Требования к документации.	ПК-4
74.		Система менеджмента информационной безопасности ISO/IEC 27001. Анализ системы менеджмента информационной безопасности со стороны руководства	ПК-4
75.		Практические правила управления информационной безопасностью. ГОСТ ИСО/МЭК 17799-2005. Организационные вопросы безопасности	ПК-4

76.		Практические правила управления информационной безопасностью. ГОСТ ИСО/МЭК 17799-2005. Классификация информации	ПК-4
77.		Практические правила управления информационной безопасностью. ГОСТ ИСО/МЭК 17799-2005. Физическая защита и защита от воздействий окружающей среды	ПК-4
78.		Практические правила управления информационной безопасностью. ГОСТ ИСО/МЭК 17799-2005. Процедуры в отношении инцидентов нарушения информационной безопасности.	ПК-4
79.		Практические правила управления информационной безопасностью. ГОСТ ИСО/МЭК 17799-2005. Управление передачей данных и операционной деятельностью	ПК-4
80.		Практические правила управления информационной безопасностью. ГОСТ ИСО/МЭК 17799-2005. Контроль доступа	ПК-4
81.		Обеспечение информационной безопасности организации. ГОСТ Р – 53114-2008. Основные положения документа	ПК-4
82.		Обеспечение информационной безопасности организации. ГОСТ Р – 53114-2008. Требования к документации по информационной безопасности организации.	ПК-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 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 на высоком уровне знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации, внедрять организационные меры в систему защиты автоматизированной системы организации

Оценка «хорошо» выставляется студенту, если он на хорошем уровне знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации, внедрять организационные меры в систему защиты автоматизированной системы организации

Оценка «удовлетворительно» выставляется студенту, если он в основном знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации, внедрять организационные меры в систему защиты автоматизированной системы организации

Оценка «неудовлетворительно» выставляется студенту, если он на низком уровне знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации, внедрять организационные меры в систему защиты автоматизированной системы организации.