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 «Организационное и правовое обеспечение информационной безопасности»

Специальность	Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	8-9

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Организационное и правовое обеспечение 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 «Организационное и правовое обеспечение 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 математикой и кибернетики

Члены комиссии:

Пелешенко В.С. доцент кафедры вычислительной математикой и кибернетики

Пелешенко Т. А. доцент кафедры вычислительной математикой 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-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации				
ИД-1ОПК-5 Знаком с действующим законодательством Российской Федерации в области информационной безопасности и защиты информации; системами защиты государственной тайны; определяет перечень сведений, относящихся к конфиденциальной информации и способы ее 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	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 интеллектуальн	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	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;	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 конфиденциальной информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальн

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.	ой собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.	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	международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.	ой 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 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.	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-	Предоставляет неполный план по организации защиты на объекте; организации работы персонала с конфиденциальн ой информацией; разработке проектов нормативных документов, регламентиру ю щих работу по защите информации, а также положений, инструкций и других организацион но-	Предоставляет план по организации защиты на объекте; организации работы персонала с конфиденциальн ой информацией; разработке проектов нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационн о- распорядительн	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

	распорядительных документов	распорядительных документов	ых документов	- распорядительны х документов
ИД-3ОПК-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, регламентирую щие 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, регламентирующи е деятельность по защите информации
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				
ИД-1ОПК-6 Знаком с нормативно-правовыми механизмами лицензирования, сертификации и аттестации; принципами организационного обеспечения информационной безопасности; основными угрозами информационной безопасности на объекте (в организации); порядком	С грубыми ошибками определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по	С небольшими ошибками определяет критерии технологических процессов защиты информации для сопоставлени я с требованиями нормативных документов Федеральной службы безопасности Российской	Некорректно определяет критерии технологическ их процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому	определяет критерии технологически х процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному

организации службы безопасности на объекте; типовыми структурами службы безопасности, ее основными задачами и функциями должностных лиц; роль персонала в обеспечении информационной безопасности на объекте; основами организационной защиты информации, ее современные проблемы и терминологию; основными руководящими документами по обеспечению режима и конфиденциальности на объекте; основными документами, регламентирующими организационную безопасность на объекте.	техническому и экспортному контролю	Федерации, Федеральной службы по техническому и экспортному контролю	и экспортному контролю	контролю
ИД-2ОПК-6 Эффективно применяет знания теории и методики курса при раскрытии компьютерных преступлений, при работе с конфиденциальной информацией и государственной тайной, при	С грубыми ошибками разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации;	С небольшими ошибками разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в	Некорректно разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет	разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику

работе с организационно-правовым обеспечением, при работе с ЭП, при защите авторского и международного права, при проведении экспертизы преступлений в сфере компьютерной информации; применять нормативно-правовые акты при защите информации; оценивать состояние организационной защиты информации на объекте.	определяет политику контроля доступа работников к информации ограниченного доступа	организации; определяет политику контроля доступа работников к информации ограниченного доступа	политику контроля доступа работников к информации ограниченного доступа	контроля доступа работников к информации ограниченного доступа
ИД-ЗОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по	С грубыми ошибками применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей	С ошибками применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей	Некорректно применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей	применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей

техническому и экспортному контролю.				

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-5, ОПК-6
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-5, ОПК-6
3.	a	Числовая информация? a) количественная мера объектов и их свойств в окружающем мире; b) информация, представленная в виде последовательности цифр.	ОПК-5, ОПК-6
4.	a	Текстовая информация - способ кодирования речи человека специальными символами - буквами? a) да; b) нет.	ОПК-5, ОПК-6
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-5, ОПК-6
6.	a,b	В зависимости от носителей информация информационные	ОПК-5, ОПК-6

		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.	
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-5, ОПК-6
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-5, ОПК-6
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-5, ОПК-6
10.	a,b	К защищаемой относят информацию: a) секретную (сведения, содержащие государственную тайну); b) конфиденциальную (сведения, содержащие коммерческую	ОПК-5, ОПК-6

		тайну, а также тайну, касающуюся личной, неслужебной деятельности граждан); c) сведения о загрязнениях окружающей среды.	
11.	a	Под угрозой (вообще) обычно понимают … 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. c) компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.	ОПК-5, ОПК-6
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-5, ОПК-6
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-5, ОПК-6
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-5, ОПК-6

15.	a,b,c	Причинами разрушения информации могут быть: a) компьютерные вирусы; b) несанкционированные действия; c) ошибки программ; d) резервное копирование	ОПК-5, ОПК-6
16.	a	Доступность информации – … 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).	ОПК-5, ОПК-6
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-5, ОПК-6
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-5, ОПК-6
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-5, ОПК-6
20.	a	Должностные лица обязаны предоставлять по запросам граждан ... a) общедоступную информацию;	ОПК-5, ОПК-6

		b) информацию с ограниченным доступом; c) информацию, не подлежащая распространению.	
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? a) информация, не подлежащая распространению; b) Информация с ограниченным доступом; c) информация, доступ к которой не может быть ограничен.	ОПК-5, ОПК-6
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-5, ОПК-6
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-5, ОПК-6
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-5, ОПК-6
25.	a	Естественные угрозы– … a) угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, не зависящих от человека;	ОПК-5, ОПК-6

		b) угрозы информационной безопасности АС, вызванные деятельностью человека.	
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 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	ОПК-5, ОПК-6
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-5, ОПК-6
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-5, ОПК-6
29.	a,c,d	К Информационным каналам утечки информации относятся	ОПК-5, ОПК-6

		a) Канал коммутируемых линий связи b) Канал аудиальный c) Канал выделенных линий связи d) Канал локальной сети e) Канал визуальный	
30.	а	ПЭМИ это а) паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными b) побочных электромагнитных излучений технических средств приема, обработки, хранения и передачи информации	ОПК-5, ОПК-6

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 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, регламентирующих работу по защите информации, а также положений, инструкций и других организационно - распорядительных документов. Предоставляет детальный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирущие деятельность по защите информации определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей

Оценка «**хорошо**» выставляется студенту в случае, когда он 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 конфиденциальной 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 конфиденциальной информацией; разработке проектов нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. Предоставляет отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. Некорректно определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской

Федерации, Федеральной службы по техническому и экспортному контролю. Некорректно разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа. Некорректно применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей

Оценка «**удовлетворительно**» выставляется студенту, если он 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; 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 неполный 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. Предоставляет неполный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. С небольшими ошибками определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. С небольшими ошибками разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа. С ошибками применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей

Оценка «**неудовлетворительно**» выставляется, если студент: 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. С грубыми ошибками определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. С грубыми ошибками разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации

ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа. С грубыми ошибками применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей