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
«Комплексное обеспечение информационной безопасности автоматизированных систем»

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

Введение

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

3. Разработчик: Пелешенко Т.А., 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
Компетенция: ПК-1. Способен оценивать уровень безопасности компьютерных систем и сетей				
ИД-1$_{ПК-1}$ Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Не предоставляет отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Предоставляет неполный отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Предоставляет отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Предоставляет детальный отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.
ИД-2$_{ПК-1}$ Разрабатывает требования по защите, формирование политик безопасности компьютерных систем и сетей.	Не предоставляет отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей.	Предоставляет неполный отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей.	Предоставляет отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей.	Предоставляет детальный отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей.
ИД-3$_{ПК-1}$ Проводит анализ безопасности компьютерных систем.	Не предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем.	Предоставляет неполный отчёт по результатам проведения анализа безопасности компьютерных систем.	Предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем.	Предоставляет детальный отчёт по результатам проведения анализа безопасности компьютерных систем.

ИД-4$_{ПК-1}$ Проводит сертификацию программно-аппаратных средств защиты информации и анализ результатов.	Не предоставляет отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет неполный отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.
ИД-5$_{ПК-1}$ Проводит инструментальный мониторинг защищенности компьютерных систем и сетей.	Не предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет неполный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет детальный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.
ИД-6$_{ПК-1}$ Проводит экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов.	Не предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет неполный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет отчет по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет детальный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.
Компетенция: ПК-8. Способен разрабатывать системы защиты информации автоматизированных систем				
ИД-1$_{ПК-8}$ Тестирует системы защиты информации автоматизированных систем.	Не может тестировать системы защиты информации автоматизированных систем.	С ошибками тестирует системы защиты информации автоматизированных систем.	Не до конца тестирует системы защиты информации автоматизированных систем.	Тестирует системы защиты информации автоматизированных систем.
ИД-2$_{ПК-8}$ Разрабатывает проектные решения по защите информации в автоматизированных системах.	Не может разрабатывать проектные решения по защите информации в автоматизированных системах.	С ошибками разрабатывает проектные решения по защите информации в автоматизированных системах.	Не до конца разрабатывает проектные решения по защите информации в автоматизированных системах.	разрабатывает проектные решения по защите информации в автоматизированных системах.

ИД-3$_{ПК-8}$ Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем.	Не может разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем.	С ошибками разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем.	Не до конца разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем.	Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем.
ИД-4$_{ПК-8}$ Разрабатывает программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.	Не может разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.	С ошибками разрабатывает программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.	Не до конца разрабатывает программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.	Разрабатывает программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.
Компетенция: ПК-9. Способен формировать требования к защите информации в автоматизированных системах				
ИД-1$_{ПК-9}$ Обосновывает необходимость защиты информации в автоматизированной системе.	Не предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет неполный отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет детальный отчет с обоснованием необходимости защиты информации в автоматизированной системе.
ИД-2$_{ПК-9}$ Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой.	Не предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет неполный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет детальный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.
ИД-3$_{ПК-9}$ Разрабатывает архитектуру системы защиты информации автоматизированной системы.	Не предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.	Предоставляет неполный отчёт по результатам разработки архитектуры системы защиты информации	Предоставляет отчёт по результатам разработки архитектуры системы защиты информации	Предоставляет детальный отчёт по результатам разработки архитектуры системы защиты информации

		автоматизированной системы.	автоматизированной системы.	автоматизированной системы.
ИД-4$_{ПК-9}$ Моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Не предоставляет отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Предоставляет неполный отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Предоставляет отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Предоставляет детальный отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты 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
		Форма обучения очная/заочная/очно-заочная	
1.	c	Какие состояния защищенности информации являются основой безопасной IT-инфраструктуры? a) Конфиденциальность, доступность, подлинность b) Конфиденциальность, целостность, подлинность c) Конфиденциальность, целостность, доступность	ПК-1
2.	d	Какие существуют степени секретности сведений составляющих государственную тайну? a) Особой важности, абсолютно секретно, совершенно секретно b) Абсолютно секретно, совершенно секретно, секретно c) Особой важности, абсолютно секретно, секретно d) Особой важности, совершенно секретно, секретно	ПК-1
3.	c	Какие сведения НЕ относятся к конфиденциальной информации? a) Персональные данные b) Коммерческая тайна c) Сведения об имуществе организации d) Данные о ведении расследования и судебные документы	ПК-1
4.	d	«Что из перечисленного НЕ относится к объектам защиты конфиденциальной информации? a) Информация b) Ресурсные объекты c) Физические объекты d) Социальные объекты	ПК-1
5.	d	Какое свойство информации понимается под «состоянием ресурсов автоматизированной информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается». a) Целостность b) Доступность	ПК-1

		c) Подотчетность d) Подлинность	
6.	a	Какой термин понимается под «совокупностью условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации» a) Угроза b) Уязвимость c) Утечка d) Перехват	ПК-1
7.	d	Какие сведения НЕ относятся к государственной тайне? a) Сведения в военной области b) Сведения в области экономики, науки и техники c) Сведения в области внешней политики и экономики d) Сведения о государственных валютных резервах	ПК-1
8.	b	Какому принципу с позиции системного подхода НЕ обязана удовлетворять система защиты информации? a) Непрерывность b) Совершенность c) Целенаправленность и конкретность d) Надежность, универсальность и комплексность	ПК-1
9.	d	Что из перечисленного НЕ относится к основным задачам технической защиты информации? a) Предотвращение утечки информации через технические каналы b) Предотвращение несанкционированного доступа к информации c) Защита носителей информации от уничтожения d) Защита от несанкционированного использования программ	ПК-1
10.	c	Что из перечисленного НЕ относится к защищаемым объектам информатизации? a) Средства и системы информатизации b) Технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается c) Технические средства и системы, не обрабатывающие конфиденциальную информацию	ПК-1

		d) Защищаемые помещения	
11.	a	Какие сведения НЕ относятся к категории информации, доступ к которой нельзя ограничить в соответствии с федеральным законодательством (ст. 8 ФЗ № 149)? a) Сведения о методах и средствах защиты секретной информации b) Нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина c) Информация о деятельности государственных органов и органов местного самоуправления d) Информация о состоянии окружающей среды	ПК-8
12.	a	К какому классу информации по категориям доступа относится коммерческая тайна? a) Конфиденциальная информация b) Государственная тайна c) Общедоступная информация d) Информация, доступ к которой не может быть ограничен	ПК-8
13.	a	К какому классу информационных ресурсов относятся текстовые документы? a) Документированные b) Недокументированные c) Индивидуальные знания	ПК-8
14.	d	Расшифруйте аббревиатуру «ФСТЭК» a) Федеральная служба по техническому и экономическому контролю b) Федеральныйсовет технического и экспортного контроля c) Федеральный совет технического и экономического контроля d) Федеральная служба по техническому и экспортному контролю	ПК-8
15.	Конфиденциальная информация — сведения, доступ к которым ограничен законом и не подлежит свободному распространению без согласия владельц	Что понимается под термином «конфиденциальная информация»?	ПК-8

16.	a, b, c, d, e	Что из перечисленного НЕ относится к перечню сведений конфиденциального характера? a) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами b) сведения о состоянии окружающей среды c) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами d) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них e) сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности государства	ПК-8
17.	угрозы конфиденциальной информации	Какой термин понимается под «потенциальными или реально возможными действиями по отношению к информационным ресурсам, приводящими к неправомерному овладению охраняемыми сведениями»?	ПК-8
18.	a,d	Сопоставьте понятие и его определение. L1: злоумышленник L2: заинтересованные или незаинтересованные в возникновении угрозы лица L3: стороннее лицо R1: лицо, действующее в интересах конкурента, противника или в личных корыстных интересах R2: лицо, создающее угрозы несанкционированного уничтожения документов, ускорения угасание текста или изображения, подмена или изъятие документов, фальсификация текста или его части R3: любое лицо, не имеющее непосредственного отношения к деятельности фирмы, посетители фирмы, работники других организационных структур, а также сотрудники данной фирмы, не обладающие правом a) доступа в определенные помещения, к конкретному документу, информации, базе данных	ПК-8
19.	a, b, c, d	Какие из перечисленных обстоятельств провоцируют утрату информационных ресурсов?	ПК-8

		a) наличие интереса конкурента, учреждений, фирм или лиц к конкретной информации b) наличие системной аналитической и контрольной работы по выявлению и изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов c) наличие эффективной системы защиты информации d) неупорядоченный подбор персонала и периодическая смене кадров	
20.	a, c	Какое из перечисленных утверждений является верным? a) утрата информации характеризуется тем, что информация переходит непосредственно к заинтересованному лицу – конкуренту, злоумышленнику – или к случайному лицу b) утрата информации характеризуется тем, что информация переходит непосредственно к конкуренту, злоумышленнику c) утрата информации характеризуется тем, что информация переходит непосредственно к случайному лицу d) нет правильного варианта ответа	ПК-4
21.	c	Какие из перечисленных ситуаций провоцируют угрозу непреднамеренного перехода информации к третьему лицу? a) утеря или неправильное уничтожения документа, пакета с документами, дела, конфиденциальных записей b) отсутствия в документах излишней информации ограниченного доступа c) разглашение конфиденциальной информации сотрудниками d) осуществление работы с документами ограниченного доступа без посторонних лиц	ПК-9
22.	b	Какие из перечисленных ситуаций НЕ провоцируют угрозу непреднамеренного перехода информации к третьему лицу? a) игнорирование или умышленное невыполнение сотрудником требований по защите документированной информации b) использование сведений ограниченного доступа в открытых документациях, публикациях, интервью, личных записях, дневниках и т.п. c) маркировка информации и документов ограниченного доступа	ПК-9
23.	b	Какое из перечисленных утверждений является верным?	ПК-9

		a) каналы несанкционированного доступа могут быть трех типов: организационные, информационные и технические b) каналы несанкционированного доступа могут быть двух типов: организационные и технические c) каналы несанкционированного доступа могут быть одного типа – это технические d) нет правильного варианта	
24.	a, b	Что из перечисленного является техническим каналом утечки информации? a) поступление злоумышленника на работу в фирму, как правило, на техническую или вспомогательную должность b) физический путь утечки информации от источника или канала объективного распространения информации к злоумышленнику c) участие злоумышленника в работе фирмы в качестве партнера, посредника, клиента, использование разнообразных обманных способов d) получение нужной информации от третьего (случайного) лица	ПК-9
25.		Сопоставьте понятия и действие (ситуацию), его характеризующее (ую). R1: утечка по организационным каналам R2: утечка по техническим каналам R3: легальные способы получения информации R4: нелегальные способы получения информации L1: установление доверительных взаимоотношений с сотрудником учреждения, фирмы или посетителем L2: анализ физических полей и излучений, появляющихся в процессе работы вычислительной и другой офисной техники	ПК-9
26.		Сопоставьте понятия и действие (ситуацию), его характеризующее (ую). R1: утечка по организационным каналам R2: утечка по техническим каналам R3: легальные способы получения информации R4: нелегальные способы получения информации L1: поиск сообщника, работающего в интересующей фирме L2: перехват информации, имеющей звуковую, зрительную или иную форму отображения L3: изучение продукции фирмы, рекламных изданий L4: подслушивание разговоров	ПК-9
27.		Сопоставьте понятия и действие (ситуацию), его характеризующее (ую). R1: утечка по организационным каналам R2: утечка по техническим каналам	ПК-9

		R3: легальные способы получения информации R4: нелегальные способы получения информации L1: использование ошибочных действий персонала L2: использование специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию без непосредственного контакта с персоналом фирмы, документами, делами и базами данных L3: изучение сведений, полученных в процессе официальных и неофициальных бесед и переговоров с сотрудниками фирмы L4: подделка идентифицирующих документов	
28.		Сопоставьте понятия и действие (ситуацию), его характеризующее (ую). R1: утечка по организационным каналам R2: утечка по техническим каналам R3: легальные способы получения информации R4: нелегальные способы получения информации L1: тайное или по фиктивным документам проникновение в здание фирмы и помещения L2: физический путь утечки информации L3: изучения материалов пресс-конференций, презентаций фирмы и продукции, научных симпозиумов и семинаров L4: инсценировка или организация экстремальных ситуаций	ПК-9
29.	Утечка информации — это несанкционированный доступ, неконтролируемое распространение или потеря конфиденциальных данных, которые могут быть личными, коммерческими или государственными.	Что понимается под термином «утечка информации»?	ПК-9

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 он: предоставляет детальный отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; предоставляет детальный отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей; предоставляет детальный отчёт по результатам проведения анализа безопасности компьютерных систем; предоставляет детальный отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов; предоставляет детальный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей; предоставляет детальный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов; предоставлен детальный отчёт с результатами тестирования систем защиты информации автоматизированных систем; предоставлен детальный отчёт с результатами разработки проектных решений по защите информации в автоматизированных системах; предоставлен детальный отчёт с результатами разработки эксплуатационной документации на системы защиты информации автоматизированных систем; предоставлен детальный отчёт с результатами разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем; предоставляет детальный отчет с обоснованием необходимости защиты информации в автоматизированной системе; предоставляет детальный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой; предоставляет детальный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы; предоставляет детальный отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

Оценка *«***хорошо***»* выставляется студенту, если он: предоставляет отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; предоставляет отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей; предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем; предоставляет отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов; предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей; предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов; предоставлен отчёт с результатами тестирования систем защиты информации автоматизированных систем; предоставлен отчёт с результатами разработки проектных решений по защите информации в автоматизированных системах; предоставлен отчёт с результатами разработки эксплуатационной документации на системы защиты информации автоматизированных систем; предоставлен отчёт с результатами разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем; предоставляет отчет с обоснованием необходимости защиты

информации в автоматизированной системе; предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой; предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы; предоставляет отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

Оценка *«***удовлетворительно***»* выставляется студенту, если он: предоставляет неполный отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; предоставляет неполный отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей; предоставляет неполный отчёт по результатам проведения анализа безопасности компьютерных систем; предоставляет неполный отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов; предоставляет неполный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей; предоставляет неполный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов; предоставлен неполный отчёт с результатами тестирования систем защиты информации автоматизированных систем; предоставлен неполный отчёт с результатами разработки проектных решений по защите информации в автоматизированных системах; предоставлен неполный отчёт с результатами разработки эксплуатационной документации на системы защиты информации автоматизированных систем ;предоставлен неполный отчёт с результатами разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем; предоставляет неполный отчет с обоснованием необходимости защиты информации в автоматизированной системе; предоставляет неполный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой; предоставляет неполный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы; предоставляет неполный отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

Оценка *«***неудовлетворительно***»* выставляется студенту, если он: не предоставляет отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; не предоставляет отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей; не предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем; не предоставляет отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов; не предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей; не предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов; не предоставлен отчёт с результатами тестирования систем защиты информации автоматизированных систем; не предоставлен отчёт с результатами разработки проектных решений по защите информации в автоматизированных системах; не предоставлен отчёт с результатами разработки эксплуатационной документации на системы защиты информации автоматизированных систем; не предоставлен отчёт с результатами разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем; не предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе; не предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой; не предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы; не предоставляет отчёт по результатам моделирования

защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.