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
«Менеджмент инцидентов информационной безопасности информационных 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 «Менеджмент инцидентов информационной безопасности информационных 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 «Менеджмент инцидентов информационной безопасности информационных систем»

3. Разработчик: Пелешенко В.С., 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-3. Способен разрабатывать средства защиты информации				
ИД-1ПК-3 Разрабатывает технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Не предоставляет отчёт по результатам разработки технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет неполный отчёт по результатам разработки технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет отчёт по результатам разработки технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет детальный отчёт по результатам разработки технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.
ИД-2ПК-3 Разрабатывает технические средства защиты акустической речевой информации от утечки по техническим каналам.	Не предоставляет отчёт по результатам разработки технических средств защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет неполный отчёт по результатам разработки технических средств защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет отчёт по результатам разработки технических средств защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет детальный отчёт по результатам разработки технических средств защиты акустической речевой информации от утечки по техническим каналам.
ИД-3ПК-3 Разрабатывает программно-технические средства защиты информации от несанкционированного доступа	Не предоставляет отчёт по результатам разработки программно-технических средств защиты информации от несанкционированного доступа.	Предоставляет неполный отчёт по результатам разработки программно-технических средств защиты информации от несанкционированного доступа.	Предоставляет отчёт по результатам разработки программно-технических средств защиты информации от несанкционированного доступа.	Предоставляет детальный отчёт по результатам разработки программно-технических средств защиты информации от несанкционированного доступа.

ИД-4ПК-3 Разрабатывает технические средства контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Не предоставляет отчёт по результатам разработки технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет неполный отчёт по результатам разработки технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет отчёт по результатам разработки технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет детальный отчёт по результатам разработки технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.
ИД-5ПК-3 Разрабатывает технические средства контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.	Не предоставляет отчёт по результатам разработки технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет неполный отчёт по результатам разработки технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет отчёт по результатам разработки технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет детальный отчёт по результатам разработки технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.
ИД-6ПК-3 Разрабатывает программные (программно-технических) средства контроля защищенности информации от несанкционированного доступа.	Не предоставляет отчёт по результатам разработки программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа.	Предоставляет неполный отчёт по результатам разработки программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа.	Предоставляет отчёт по результатам разработки программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа.	Предоставляет детальный отчёт по результатам разработки программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа.
Компетенция: ПК-7. Способен организовывать и проводить работы по технической защите информации				

ИД-1ПК-7 Создает системы защиты информации в организации.	Не предоставляет отчёт по результатам создания системы защиты информации в организации.	Предоставляет неполный отчёт по результатам создания системы защиты информации в организации.	Предоставляет отчёт по результатам создания системы защиты информации в организации.	Предоставляет детальный отчёт по результатам создания системы защиты информации в организации.
ИД-2ПК-7 Вводит в эксплуатацию систему защиты информации в организации.	Не предоставляет отчёт по результатам ввода в эксплуатацию системы защиты информации в организации.	Предоставляет неполный отчёт по результатам ввода в эксплуатацию системы защиты информации в организации.	Предоставляет отчёт по результатам ввода в эксплуатацию системы защиты информации в организации.	Предоставляет детальный отчёт по результатам ввода в эксплуатацию системы защиты информации в организации.
ИД-3ПК-7 Сопровождает системы защиты информации в ходе ее эксплуатации.	Не предоставляет отчёт по результатам сопровождения системы защиты информации в ходе ее эксплуатации.	Предоставляет неполный отчёт по результатам сопровождения системы защиты информации в ходе ее эксплуатации.	Предоставляет отчёт по результатам сопровождения системы защиты информации в ходе ее эксплуатации.	Предоставляет детальный отчёт по результатам сопровождения системы защиты информации в ходе ее эксплуатации.

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	ПК-3
1.	планирование, организацию, контроль и совершенствование процессов защиты информации, направленных на обеспечение конфиденциальности, целостности и доступности данных в соответствии с нормативными требованиями и бизнес-целями организации.	Менеджмент в сфере информационной безопасности включает в себя:	ПК-7
2.	угрозы утечки, модификации, уничтожения или блокирования доступа к информации, а также несанкционированные действия злоумышленников, технические сбои и человеческие ошибки, способные нанести ущерб организации.	Риски в сфере информационной безопасности включают в себя:	ПК-3
3.	одной из форм нарушения её	Разрушение информации является:	ПК-7

	целостности, приводящей к полной или частичной утрате данных, что может быть вызвано вредоносным ПО, аппаратными сбоями, природными катастрофами или преднамеренными действиями злоумышленников.		
4.	внешние (кибератаки, действия хакеров, стихийные бедствия) и внутренние (ошибки сотрудников, злоупотребление полномочиями, утечки по неосторожности), а также на преднамеренные и непреднамеренные угрозы.	Риски в сфере информационной безопасности разделяются на:	ПК-3
5.	a, b	В определении задач менеджмента в сфере информационной безопасности фигурируют такие понятия как: a) комплексность b) непрерывность нейтральность	ПК-7
6.	a, b	Комплексность решения задач информационной безопасности предполагает: a) исключение "узких мест" в системе защиты информации b) анализ всех возможных сценариев нарушения безопасности и способов защиты c) обеспечение круглосуточной ежедневной работы службы	ПК-3

		информационной безопасности	
7.	b, c	Принципы работы IEEE включают в себя: a) принцип солидарной ответственности участников организации принцип добровольности участия в организации c) принцип открытости результатов деятельности организации	ПК-3
8.	c	Сектором ITU, ответственным за стандартизацию технологий безопасности, является: a) ITU-R b) ITU-D ITU-T	ПК-7
9.	c	Членами ISO являются: a) университеты и компании, специализирующиеся на стандартизации b) независимые эксперты по стандартизации государственные органы по стандартизации	ПК-3
10.	a	В организационную структуру ACM входят: a) группы специальных интересов b) комитеты по стандартам отраслевые департаменты	ПК-7
11.	a, b	Задачи консорциума W3C включают в себя: a) стандартизацию подключения технических устройств к интернет b) стандартизацию структур и форматов информации в интернет стандартизация аппаратных средств защиты информации в интернет	ПК-3
12.	a, c	Центр CERT/CC собирает информацию об уязвимостях из внешних источников с целью: a) содействия в нейтрализации уязвимостей b) дальнейшего взимания платы с разработчиков ПО, допустивших появление уязвимостей исследования возможных последствий уязвимости	ПК-7
13.	b, c	Технологические альянсы компаний-поставщиков в сфере информационной безопасности получают преимущества на рынке за счет:	ПК-3

		больших возможностей для скупки конкурентов удешевления разработки новых продуктов координации маркетинговой и информационной политики	
14.	a, d	Цели менеджмента крупных поставщиков информационных систем в сфере взаимодействия с внешними субъектами по вопросам информационной безопасности включают в себя: a) создание благоприятного имиджа в сообществе пользователей информационных систем b) снижение затрат на разработку продукции c) уменьшение числа уязвимостей во вновь выпускаемых продуктах d) занятие новых рыночных ниш	ПК-7
15.	a, b, c	Взаимодействие компаний-производителей информационных систем с пользователями по вопросам нейтрализации уязвимостей включает в себя: a) сбор информации о выявленных уязвимостях b) рассылку уведомлений о выявленных уязвимостях c) распространение программных "заплаток" для устранения уязвимостей	ПК-3
16.	b	Методология SDL нацелена на: a) упрощение процесса нейтрализации выявляемых уязвимостей b) повышение уровня безопасности разрабатываемого ПО c) ускорение сбора информации о вновь выявляемых уязвимостях	ПК-7
17.	c	Программа GSP корпорации Microsoft предполагает: a) оказание правительствам бесплатных услуг по вопросам защиты информации b) передачу правительствам бесплатных лицензий на программные средства обеспечения безопасности c) передачу правительствам исходных кодов ОС и приложений	ПК-3
18.	b	Со стороны РФ в программе GSP участвует: a) ФСБ b) ФСТЭК c) Роскомнадзор	ПК-7

19.	a, c	На формирование политики безопасности предприятия непосредственно влияют такие факторы как: a) требования законодательства b) информационная политика предприятий- конкурентов c) использование в работе предприятия сведений составляющих государственную или банковскую тайну	ПК-3
20.	b	Информирование персонала предприятия об основных целях в сфере информационной безопасности осуществляется с помощью: a) аудита безопасности b) политики безопасности положения о департаменте информационной безопасности	ПК-7
21.	a, c	Целями верхнего уровня политики безопасности предприятия являются: a) демонстрация руководством предприятия своего отношения к вопросам защиты информации определение структуры департамента информационной безопасности b) информирование персонала об основных приоритетах в сфере защиты информации c) формирование требований к поставщикам средств защиты информации	ПК-3
22.	c	Долгосрочное развитие политики информационной безопасности предприятия предполагает: a) статичность b) пропорциональность цикличность	ПК-7
23.	a, c	Детализация наиболее общих положений политики информационной безопасности осуществляется с помощью: a) правил и ограничений использования отдельных технологий и средств защиты b) маркетинговой политики предприятия политики опубликования информационных материалов в открытых источниках	ПК-3
24.	a	Работа со сведениями, составляющими государственную тайну регламентируется	ПК-7

		a) Федеральным законодательством b) Международными соглашениями Нормативными актами субъектов РФ	
25.	b	Перечень сведений, относимых к государственной тайне утверждается: a) Правительством РФ b) Президентом РФ c) ФСБ ФСТЭК	ПК-3
26.	a, b, c	a) Допуск к сведениям, составляющим государственную тайну, предполагает: проведение проверочных мероприятий в отношении лица, получающего допуск b) ознакомление лица, получающего допуск, с соответствующими нормами законодательства c) получение согласия на временное ограничение прав от лица, получающего допуск d) предоставление льгот и компенсационных ыплат родственникам лица, получающего допуск	ПК-7
27.	a	Проверочные мероприятия, связанные с получением допуска к государственной тайне, осуществляет a) ФСБ b) МВД c) ФСТЭК Служба безопасности предприятия	ПК-3
28.	a	Допуск персонала к государственной тайне осуществляет: a) руководитель предприятия b) органы ФСБ органы МВД	ПК-7
29.	b	Президент РФ: a) утверждает передачу другим государствам документов, относимых к государственной тайне b) утверждает перечень сведений, относимых к государственной тайне	ПК-3

		с) утверждает перечень лиц, имеющих доступ к сведениям, составляющим государственную тайну	

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.