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
«Организация защиты конфиденциальной информации на объектах информатизации»

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 «Организация защиты конфиденциальной информации на объектах информатизации». 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 «Организация защиты конфиденциальной информации на объектах информатизации»

3. Разработчик: Песков М.В., 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-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 автоматизированной системы.	Предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.	Предоставляет детальный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.
ИД-4$_{ПК-9}$ Моделирует защищенные автоматизированные системы с целью анализа их	Не предоставляет отчёт по результатам моделирования защищенных автоматизированных систем с	Предоставляет неполный отчёт по результатам моделирования защищенных автоматизиров	Предоставляет отчёт по результатам моделирования защищенных автоматизированных систем с	Предоставляет детальный отчёт по результатам моделирования защищенных автоматизиров

уязвимостей и эффективности средств и способов защиты информации.	целью анализа их уязвимостей и эффективности средств и способов защиты информации.	анных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	целью анализа их уязвимостей и эффективности средств и способов защиты информации.	анных 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.	Аппаратные требования Установка ОС Установка Secret Net Studio Настройка сети и безопасности Интеграция с инфраструктурой Настройка политик безопасности Дополнительные меры	Какие действия необходимо выполнить на компьютере, который будет использоваться в качестве сервера безопасности Secret Net Studio?	ПК-9
2.	a, b, e	Из каких программных пакетов состоит Secret Net Studio? a) Secret Net Studio Клиент b) Secret Net Studio Сервер безопасности c) Secret Net Studio Сервер обновлений d) Secret Net Studio Сервер защиты от НСД e) Secret Net Studio Центр управления	ПК-9
3.	a, d	В каких из следующих вариантов может выполняться установка сервера безопасности Secret Net Studio? a) установка с созданием нового леса и домена безопасности b) установка без создания нового леса и домена безопасности c) установка без включения сервера в состав имеющегося домена безопасности d) установка с созданием нового домена безопасности в имеющемся лесу доменов безопасности	ПК-9
4.	a	После установки программы управления Secret Net Studio нужно ли устанавливать пакет обновлений 8.5.5329.40?	ПК-9

		a) Да, в обязательном порядке b) Нет, не нужно	
5.	b	Альт 8 СП создана на основе операционной системы: a) Windows b) Linux c) MS DOS	ПК-9
6.	a	В качестве загрузчика в Альт 8 СП используется: a) GRUB b) Syslinux c)OS/2 d) LILO	ПК-9
7.	c	Альт 8 СП поставляется на: a) твердотельном жёстком диске b) магнитном жёстком диске c) лазерном компакт-диске d) flash-носителе	ПК-9
8.	d	В режиме ручного изменения времени в Альт 8 СП доступна активация функции синхронизации с сервером: a) FTP b) HTTPS c) SSL d) NTP	ПК-9
9.	b	Профиль установки сервера “Сервер Samba-: DC” предлагает группу пакетов для: a) развёртки на сервере веб-сайта b) конфигурации сервера в качестве контроллера домена c) конфигурации сервера в качестве локального сервера DNS	ПК-9
10.	c	При настройке сетевых параметров в Альт 8 СП доступно: a) ручное заполнение полей b) импорт полей с flash-накопителя c) ручное заполнение или получение от сервера DHCP d) ручная конфигурация сетевых параметров не предусмотрена	ПК-9
11.	c	Какой из перечисленных TCP/IP портов должен быть открыт на межсетевом экране для успешного обмена данными между Сервером безопасности и Клиентом Dallas	ПК-9

		Lock: a) 5436 b) 80 c) 17493 d) 443	
12.	b	Какое программное обеспечение необходимо для предоставления возможности удаленного подключения к Серверу безопасности Dallas Lock с рабочего места администратора безопасности: a) Сервер конфигураций Dallas Lock b) Консоль сервера безопасности c) Сервер лицензий d) Putty	ПК-9
13.	a	Какой компонент Dallas Lock необходимо установить на локальный компьютер перед установкой любого другого компонента Dallas Lock: a) Клиент Dallas Lock b) Сервер лицензий c) Сервер безопасности d) Консоль сервера безопасности	ПК-9
14.	c	Какой компонент Dallas Lock позволяет осуществлять централизованное управление политиками и управлять доменами безопасности в организации: a) Сервер лицензий b) Клиент Dallas Lock c) Сервер безопасности d) Консоль сервера безопасности	ПК-9
15.	a	К какой группе обязательно должен относится пользователь, осуществляющий установку Клиент Dallas Lock: a) Локальные администраторы b) Гостевая группа c) Сетевые администраторы d) Бухгалтерия	ПК-9
16.	b	Какая команда позволяет запустить редактор оснасток Клиент Dallas Lock, в котором можно добавить консоль управления пользователями и группами: a) ipconfig	ПК-9

		b) mmc c) mstsc d) shutdown	
17.	c	Какую роль автоматически получает пользователь, установивший Dallas Lock на локальном компьютере, в терминологии Dallas Lock: a) Администратор безопасности b) Администратор Dallas Lock c) Суперадминистратор d) Гостевой пользователь	ПК-9
18.	a	Какое действия обязательно должно быть выполнено сразу после установки клиента Dallas Lock: a) Перезагрузка компьютера b) Выход пользователя из системы c) Обновление операционной системы d) Отключение от локальной сети	ПК-9
19.	b	Какой из перечисленных способов размещения сервера баз данных Клиент Dallas Lock является наиболее рекомендуемым: a) Размещение сервера баз данных на виртуальной машине, запущенной на сервере безопасности b) Размещение сервера баз данных на выделенном физическом сервере c) Размещение сервера баз данных на виртуальной машине, запущенной в центре обработки данных облачного провайдера d) Размещение сервера баз данных непосредственно на сервере безопасности	ПК-9
20.	c	Что из себя представляет СЗИ Dallas Lock Linux? a) аппаратный межсетевой экран b) антивирусное ПО c) программный комплекс d) средство обнаружения вторжений	ПК-9
21.	c	Какие из перечисленных файловых систем поддерживает Dallas Lock Linux? a) fat32 b) NTFS c) etc3 d) APFS	ПК-9

22.	c	Соответствует ли Dallas Lock Linux требованиям ФСТЭК России по защищенности СВТ от НСД? a) соответствует, по 1 классу защищенности СВТ от НСД b) соответствует, по 3 классу защищенности СВТ от НСД c) соответствует, по 5 классу защищенности СВТ от НСД d) не соответствует	ПК-9
23.	b	Соответствует ли Dallas Lock Linux требованиям ФСТЭК России по уровню контроля отсутствия НДВ? a) соответствует, по 2 уровню контроля отсутствия НДВ b) соответствует, по 4 уровню контроля отсутствия НДВ c) соответствует, по 6 уровню контроля отсутствия НДВ d) не соответствует	ПК-9
24.	d	Какие аппаратные идентификаторы НЕ поддерживает Dallas Lock Linux? a) eToken b) Рутокен c) iButton d) Selfkey	ПК-9
25.	d	Какие из перечисленных функций НЕ поддерживает Dallas Lock Linux? a) защита конфиденциальной информации b) управление средствами аутентификации c) контроль целостности программного обеспечения d) отслеживание подозрительной активности в сетевом трафике	ПК-9
26.	d	Какие из перечисленных операционных систем официально НЕ поддерживает Dallas Lock Linux? a) Astra Linux Common Edition 2.12 b) Debian 8 c) Ubuntu 16.04 d) Arch Linux	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 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 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 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 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.