МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Декан факультета
математики и компьютерных
наук имени профессора
Н.И. Червякова
Т.А. Гробова.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Технологии построения защищенных компьютерных сетей

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)	Математическое и программное обеспечение защиты информации
Форма обучения	очная
Год начала обучения	2026
Реализуется в 3 семестре	

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Технологии построения защищенных компьютерных сетей». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информацию 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 «Технологии построения защищенных компьютерных сетей»
3. Разработчик: Рябцев С.С., старший преподаватель кафедры вычислительной математики и кибернетики

4. Проведена экспертиза ФОС. Члены экспертной группы:

Председатель Тебуева Ф.Б., профессор кафедры вычислительной математики и кибернетики

Члены комиссии: Осипов Д.Л., доцент кафедры вычислительной математики и кибернетики

Гусева Л.Л., доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя: Березницкий А.С., кандидат экономических наук, главный аналитик ФБУ «Северо-Кавказского регионального центра судебной экспертизы Министерства юстиции РФ» ФГБУ Кабардино-Балкарской лаборатории судебной экспертизы Министерства юстиции Российской Федерации.

Экспертное заключение: Представленный ФОС по дисциплине «Технологии построения защищенных компьютерных сетей» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по направлению 10.04.01 Информационная безопасность направленность (профиль) «Математическое и программное обеспечение защиты информации», а также целям и задачам рабочей программы реализуемой учебной дисциплины. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации представлены в полном объеме.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. **Описание показателей и критериев оценивания на различных этапах их формирования, описание шкал оценивания**

Уровни сформированности компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ИД-1 УК-2 формулирует цель проекта, определяет совокупность взаимосвязанных задач, обеспечивающих ее достижение на всех этапах его жизненного цикла	Имеет слабое представление о способах разработки частной политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Имеет частичное представление о способах разработки частной политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Имеет представление о способах разработки частной политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Имеет полное представление о способах разработки частной политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
ИД-2 УК-2 разрабатывает план действий по управлению проектом на всех этапах его жизненного цикла	Имеет слабое представление о планах действий по управлению проектом на всех этапах его жизненного цикла	Имеет частичное представление о планах действий по управлению проектом на всех этапах его жизненного цикла	Имеет представление о планах действий по управлению проектом на всех этапах его жизненного цикла	Имеет полное представление о планах действий по управлению проектом на всех этапах его жизненного цикла
ИД-1 ПК-2 оценивает работоспособность применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	Имеет слабое представление о способах разработки систем управления базами данных с учетом требований по обеспечению защиты информации, о способах настройки и применяет современные системы управления базами данных, пользуется средствами защиты, предоставляемыми системами управления базами данных	Имеет частичное представление о способах разработки систем управления базами данных с учетом требований по обеспечению защиты информации, о способах настройки и применяет современные системы управления базами данных, пользуется средствами защиты, предоставляемыми системами управления базами данных	Имеет представление о способах разработки систем управления базами данных с учетом требований по обеспечению защиты информации, о способах настройки и применяет современные системы управления базами данных, пользуется средствами защиты, предоставляемыми системами управления базами данных	Имеет полное представление о способах разработки систем управления базами данных с учетом требований по обеспечению защиты информации, о способах настройки и применяет современные системы управления базами данных, пользуется средствами защиты, предоставляемыми системами управления базами данных

ИД-2 ПК-2 оценивает эффективность применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	Имеет слабое представление о способах проведения анализа и оценивает механизмы защиты баз данных	Имеет частичное представление о способах проведения анализа и оценивает механизмы защиты баз данных	Имеет представление о способах проведения анализа и оценивает механизмы защиты баз данных	Имеет полное представление о способах проведения анализа и оценивает механизмы защиты баз данных
ИД-3 ПК-2 определяет уровень защищенности и доверия программно-аппаратных средств защиты информации	Имеет слабое представление о способах оценки уровня защищенности и доверия программно-аппаратных средств защиты информации	Имеет частичное представление о способах оценки уровня защищенности и доверия программно-аппаратных средств защиты информации	Имеет представление о способах оценки уровня защищенности и доверия программно-аппаратных средств защиты информации	Имеет полное представление о способах оценки уровня защищенности и доверия программно-аппаратных средств защиты информации

Оценочные средства для проверки уровня сформированности компетенций

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1.		Что такое брандмауэр?	УК-2
2.		Что такое отказ в обслуживании?	УК-2
3.		Чем такое система обнаружения вторжений?	УК-2
4.		Что такое система предотвращения вторжений?	УК-2
5.		Что такое аутентификация?	УК-2
6.		Что такое вектор атаки?	УК-2
7.		Что происходит при гиперджекинге?	УК-2
8.		Что такое сниффер?	УК-2
9.		Что такое программа-вымогатель?	УК-2
10.		Что такое внутренняя угроза	УК-2
11.		Что такое фишинг	УК-2
12.		Что такое эксплойт нулевого дня?	УК-2
13.		Что такое сертификат SSL	УК-2
14.		Как создать нумерованный расширенный список управления доступом?	УК-2

15.		Как создать именованный расширенный список управления доступом?	УК-2
16.		Что такое список контроля доступа?	УК-2
17.	host	_____ - применяется для маски 0.0.0.0. Эта маска подразумевает соответствие всех битов IPv4-адреса. Таким образом, фильтруется единственный адрес хоста.	УК-2
18.	any	_____ - замещает маску 255.255.255.255 Эта маска указывает игнорировать весь IPv4-адрес или принять любой адрес.	УК-2
19.		Что такое туннелирование в компьютерных сетях?	ПК-2
20.		Что такое TLS?	ПК-2
21.		Что такое SSH?	ПК-2
22.		Что такое SSL?	ПК-2
23.		Что такое IPsec?	ПК-2
24.		Что означает подмена DHCP сервера?	ПК-2
25.		Что такое атака посредника, или атака «человек посередине»?	ПК-2
26.		Что такое SenderBase?	ПК-2
27.		Что такое Root Guard?	ПК-2
28.		Что такое программы-вымогатели?	ПК-2
29.	a	На каком уровне модели OSI передаются кадры? a: Канальный b: Сетевой c: Физический d: Транспортный	ПК-2
30.	c	Объясните следующую команду: # access-list 3 permit 10.0.0.9 0.0.0.0 # access-list 3 denyany: a: Здесь правило разрешает доступ только адресу 0.0.0.0, остальным доступ запрещен b: Здесь правило запрещает доступ к адресу 10.0.0.9, остальным доступ разрешен c: Здесь правило разрешает доступ только адресу 10.0.0.9, остальным доступ запрещен d: Здесь два списка управления доступом: адрес 0.0.0.0 запрещен, а адрес 10.0.0.9 разрешен	ПК-2
31.	a,c	Поясните назначение следующих списков доступа: access-list 1 deny 192.168.1.0 0.0.0.255 access-list 1 permit 192.168.0.0 0.0.255.255 a: Разрешается прохождение пакетов с адресов в блоке 192.168.0.0/16 за исключением адресов 192.168.1.0/24 b: Разрешается прохождение пакетов с адресов в блоке 192.168.1.0/24 за исключением адресов 192.168.0.0/16 c: Диапазон адресов 192.168.0.0 0.0.255.255 запрещен, а диапазон 192.168.1.0 0.0.0.255 разрешен	ПК-2
32.	a,c,d	Укажите на правильные ответы: a: ACL (Access Control List) – это набор текстовых выражений, которые что-то разрешают, либо что-то запрещают b: В основном применение списков доступа рассматривают для	ПК-2

		пакетной фильтрации c: Обычно вы размещаете ACL на входящем направлении и блокируете не нужные виды трафика d: Правила зависят от того, куда ACL применяется. Например, если ACL применяется на интерфейсе, то присутствует пакетная фильтрация, а если для NAT, то мы решаем вопрос о том, какие адреса транслировать	
33.	c	Есть следующий список доступа ip access-list 111 deny tcp any any eq 80. Как он работает? a: Запретить трафик на порту 80 (ftp-трафик) b: Разрешить трафик на порту 80 c: Запретить трафик на порту 80 (www-трафик) d: Разрешить любой трафик в соответствии с правилом 111	ПК-2
34.	a,c	Почему хаб в плане безопасности и производительности сети хуже, чем свитч? a: Потому, что хаб подает пакет на все порты, а свитч – только получателю пакета b: Потому, что свитч подает пакет на все порты, а хаб – только получателю пакета c: Потому, что на один из портов хаба (все равно, на какой) может подключиться злоумышленник d: Постановка вопроса не верна: на самом деле хаб в плане безопасности и производительности сети лучше, чем свитч?	ПК-2
35.	d	Механизм безопасности передачи, определенный в 802.11x, называется: a: DHCP b: DNS c: SSL d: WEP	ПК-2
36.	a,c	Какая длина ключей поддерживается в WEP? a: 40 бит b: 80 бит c: 128 бит d: 256 бит e: 512 бит	ПК-2
37.	c	Недостатком какого метода является невозможность обнаружения вируса в файлах, которые поступают в систему уже зараженными? a: сканирование b: эвристический анализ c: обнаружение изменений d: использование резидентных сторожей	ПК-2
38.	b	Что такое коллизия? a: ситуация, когда открытый ключ неизвестен получателю сообщения b: ситуация, когда двум сообщениям соответствует один и тот же хэш c: ситуация, когда из хэша можно восстановить исходный текст d: результат преобразования входных данных произвольной длины в данные фиксированной длины	ПК-2

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».

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он на высоком уровне: анализирует компьютерную сеть с целью определения необходимого уровня защищенности и доверия; формулирует задания по безопасности и разрабатывает рекомендации по эксплуатации системы защиты информации; проектирует и разрабатывает компьютерные системы с соответствием отечественным и зарубежным стандартам в области компьютерной безопасности; учитывает проблемы информационной безопасности при проектировании и оптимизации функционирования компьютерных сетей.

Оценка «хорошо» выставляется студенту, если на среднем уровне: анализирует компьютерную сеть с целью определения необходимого уровня защищенности и доверия; формулирует задания по безопасности и разрабатывает рекомендации по эксплуатации системы защиты информации; проектирует и разрабатывает компьютерные системы с соответствием отечественным и зарубежным стандартам в области компьютерной безопасности; учитывает проблемы информационной безопасности при проектировании и оптимизации функционирования компьютерных сетей.

Оценка «удовлетворительно» выставляется студенту, если на минимальном уровне: анализирует компьютерную сеть с целью определения необходимого уровня защищенности и доверия; формулирует задания по безопасности и разрабатывает рекомендации по эксплуатации системы защиты информации; проектирует и разрабатывает компьютерные системы с соответствием отечественным и зарубежным стандартам в области компьютерной безопасности; учитывает проблемы информационной безопасности при проектировании и оптимизации функционирования компьютерных сетей.

Оценка «неудовлетворительно» выставляется студенту, если он с грубыми ошибками: анализирует компьютерную сеть с целью определения необходимого уровня защищенности и доверия; формулирует задания по безопасности и разрабатывает рекомендации по эксплуатации системы защиты информации; проектирует и разрабатывает компьютерные системы с соответствием отечественным и зарубежным стандартам в области компьютерной безопасности; учитывает проблемы информационной безопасности при проектировании и оптимизации функционирования компьютерных сетей.