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
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Персональная кибербезопасность
название дисциплины (модуля)

Направление подготовки	10.03.01 «Информационная безопасность»
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	1

Введение

1. Назначение. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Персональная кибербезопасность» студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

2. ФОС является приложением к программе дисциплины (модуля) «Персональная кибербезопасность» в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

3. Разработчик (и) Ванина А.Г., доцент кафедры

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены комиссии: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «СГУ-Инфоком»

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Персональная кибербезопасность».

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 компетенции(й),			
	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 обеспечивать защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи (за исключением сетей связи специального назначения) в процессе их эксплуатации (06.030 В)				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-3 ПК-1 Способен к управлению персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД	в недостаточном объёме способен к управлению персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД	в минимальном объёме способен к управлению персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД	в достаточном объёме способен к управлению персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД	в полном объёме способен к управлению персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД
Компетенция: ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях Способен администрировать средства защиты информации в компьютерных системах и сетях (06. 032 В)				

Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-2 ПК-2 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	в недостаточном объёме способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	в минимальном объёме способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	в достаточном объёме способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	в полном объёме способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-3 ПК-2 Способен администрировать средства защиты информации прикладного и системного программного обеспечения	в недостаточном объёме способен администрировать средства защиты информации прикладного и системного программного обеспечения	в минимальном объёме способен администрировать средства защиты информации прикладного и системного программного обеспечения	в достаточном объёме способен администрировать средства защиты информации прикладного и системного программного обеспечения	в полном объёме способен администрировать средства защиты информации прикладного и системного программного обеспечения

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 ОФО семестр 1	
1.	б	Наиболее распространенные средства воздействия на сеть офиса: а) Слабый трафик, информационный обман, вирусы в интернет б) Вирусы в сети, логические мины (закладки), информационный перехват в) Компьютерные сбои, изменение администрирования, топологии	ПК-1
2.	в	Название информации, которую следует защищать (по нормативам, правилам сети, системы): а) Регламентированной б) Правовой в) Защищаемой	ПК-1
3.	а	Что такое политика безопасности в системе (сети)? Это комплекс: а) Руководств, требований обеспечения необходимого уровня безопасности б) Инструкций, алгоритмов поведения пользователя в сети в) Нормы информационного права, соблюдаемые в сети	ПК-1
4.	в	Наиболее важным при реализации защитных мер политики безопасности является следующее: а) Аудит, анализ затрат на проведение защитных мер б) Аудит, анализ безопасности в) Аудит, анализ уязвимостей, риск-ситуаций	ПК-1
5.	а	Что такое источник угрозы? а) потенциальный злоумышленник б) злоумышленник в) нет правильного ответа	ПК-1
6.	а	Что такое окно опасности? а) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется. б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области	ПК-1

		в) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере	
7.	а	Информационная безопасность: а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия в) нет верного ответа	ПК-1
8.	б	Защита информации: а) небольшая программа для выполнения определенной задачи б) комплекс мероприятий, направленных на обеспечение информационной безопасности в) процесс разработки структуры базы данных в соответствии с требованиями пользователей	ПК-1
9.	а	Информационная безопасность зависит от следующих факторов: а) компьютеров, поддерживающей инфраструктуры б) пользователей в) информации	ПК-1
10.	в	Основные источники внутренних отказов: а) отступление от установленных правил эксплуатации б) разрушение данных в) все ответы правильные	ПК-1
11.	а	По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы: а) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности б) обрабатывать большой объем программной информации в) нет правильного ответа	ПК-1
12.	а	Утечка информации в системе — ситуация, характеризуемая: а) Потерей данных в системе б) Изменением формы информации	ПК-1

		в) Изменением содержания информации	
13.	а, б	Свойством информации, наиболее актуальным при обеспечении информационной безопасности является: а) Целостность б) Доступность в) Актуальность	ПК-1
14.	в	Определите, когда целесообразно не предпринимать никаких действий в отношении выявленных рисков: а) когда риски не могут быть приняты во внимание по политическим соображениям б) для обеспечения хорошей безопасности нужно учитывать и снижать все риски в) когда стоимость контрмер превышает ценность актива и потенциальные потери	ПК-1
15.	б	Что такое политика безопасности? а) детализированные документы по обработке инцидентов безопасности б) широкие, высокоуровневые заявления руководства в) общие руководящие требования по достижению определенного уровня безопасности	ПК-1
16.	в	Выберите, какая из приведенных техник является самой важной при выборе конкретных защитных мер: а) анализ рисков б) результаты ALE в) анализ затрат / выгоды	ПК-1
17.	а	Угроза информационной системе (компьютерной сети): а) Вероятное событие б) Детерминированное (всегда определенное) событие в) Событие, происходящее периодически	ПК-1
18.	а	Разновидностями угроз безопасности (сети, системы) являются: а) Программные, технические, организационные, технологические б) Серверные, клиентские, спутниковые, наземные в) Личные, корпоративные, социальные, национальные	ПК-1
19.	а	Окончательно, ответственность за защищенность данных в компьютерной сети несет: а) Владелец сети б) Администратор сети в) Пользователь сети	ПК-1

20.	в	По механизму распространения П.О. различают: а) вирусы б) черви в) все ответы правильные	ПК-1
21.	а	Что такое отказ, ошибки, сбой? а) случайные угрозы б) преднамеренные угрозы в) природные угрозы	ПК-1
22.	а	Определите, что такое отказ: а) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций б) некоторая последовательность действий, необходимых для выполнения конкретного задания в) структура, определяющая последовательность выполнения и взаимосвязи процессов	ПК-1
23.	а	Определите, что такое ошибка: а) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций в) негативное воздействие на программу	ПК-1
24.	в	Конфиденциальность это: а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов б) описание процедур в) защита от несанкционированного доступа к информации	ПК-1
25.	а	Определите, для чего создаются информационные системы: а) получения определенных информационных услуг б) обработки информации в) оба варианта верны	ПК-1
26.	а	Процедура это: а) пошаговая инструкция по выполнению задачи б) обязательные действия	ПК-1

		в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах	
27.	б	Определите, какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании: а) проведение тренингов по безопасности для всех сотрудников б) поддержка высшего руководства в) эффективные защитные меры и методы их внедрения	ПК-1
28.	а	Что такое сбой? а) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния в) объект-метод	ПК-1
29.	а	Что такое побочное влияние? а) негативное воздействие на систему в целом или отдельные элементы б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент в) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций	ПК-1
30.	б	Относится к человеческому компоненту СЗИ: а) системные порты б) администрация в) программное обеспечение	ПК-1
31.	в	Выберите, что относится к правовым методам, которые обеспечивают информационную безопасность: а) Разработка аппаратных средств обеспечения правовых данных б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности	ПК-2
32.	б	Основные источники угроз информационной безопасности: а) Хищение жестких дисков, подключение к сети, инсайдерство б) Перехват данных, хищение данных, изменение архитектуры системы	ПК-2

		в) Хищение данных, подкуп системных администраторов, нарушение регламента работы	
33.	а	Определите виды информационной безопасности: а) Персональная, корпоративная, государственная б) Клиентская, серверная, сетевая в) Локальная, глобальная, смешанная	ПК-2
34.	а	Отметьте основную массу угроз информационной безопасности: а) Троянские программы б) Шпионские программы в) Черви	ПК-2
35.	б	Вид идентификации и аутентификации, который получил наибольшее распространение: а) системы PKI б) постоянные пароли в) одноразовые пароли	ПК-2
36.	в	Определите, под какие системы распространение вирусов происходит наиболее динамично: а) Windows б) Mac OS в) Android	ПК-2
37.	а	Цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети б) инсайдерства в организации в) чрезвычайных ситуаций	ПК-2
38.	а	Определите основные объекты информационной безопасности: а) Компьютерные сети, базы данных б) Информационные системы, психологическое состояние пользователей в) Бизнес-ориентированные, коммерческие системы	ПК-2
39.	в	Основные риски информационной безопасности: а) Искажение, уменьшение объема, перекодировка информации б) Техническое вмешательство, выведение из строя оборудования сети в) Потеря, искажение, утечка информации	ПК-2
40.	а, б	Предпосылки появления угроз (несколько вариантов ответа): а) объективные	ПК-2

		б) субъективные в) преднамеренные	
41.	а	Выберите, к какому виду угроз относится присвоение чужого права: а) нарушение права собственности б) нарушение содержания в) внешняя среда	ПК-2
42.	в	Выберите, что относится к ресурсам А.С. СЗИ: а) лингвистическое обеспечение б) техническое обеспечение в) все ответы правильные	ПК-2
43.	а, б	По активности реагирования СЗИ системы делят на (несколько вариантов ответа): а) пассивные б) активные в) полупассивные	ПК-2
44.	а	Основные принципы обеспечения информационной безопасности: а) Экономической эффективности системы безопасности б) Многоплатформенной реализации системы в) Усиления защищенности всех звеньев системы	ПК-2
45.	б	Основные субъекты информационной безопасности: а) руководители, менеджеры, администраторы компаний б) органы права, государства, бизнеса в) сетевые базы данных, фаерволлы	ПК-2
46.	б	Что такое ЭЦП? а) Электронно-цифровой преобразователь б) Электронно-цифровая подпись в) Электронно-цифровой процессор	ПК-2
47.	б	Наиболее распространены угрозы информационной безопасности корпоративной системы: а) Покупка нелицензионного ПО б) Ошибки эксплуатации и неумышленного изменения режима работы системы в) Сознательного внедрения сетевых вирусов	ПК-2
48.	в	Определите наиболее распространенные угрозы информационной безопасности сети: а) Распределенный доступ клиент, отказ оборудования	ПК-2

		б) Моральный износ сети, инсайдерство в) Сбой (отказ) оборудования, нелегальное копирование данных	
49.	в	Основные источники внутренних отказов: а) отступление от установленных правил эксплуатации б) разрушение данных в) все ответы правильные	ПК-2
50.	а	По отношению к поддерживающей инфраструктуре рекомендуется рассматривать такие угрозы: а) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности б) обрабатывать большой объем программной информации в) нет правильного ответа	ПК-2
51.	б	Наиболее распространенные средства воздействия на сеть офиса: а) Слабый трафик, информационный обман, вирусы в интернет б) Вирусы в сети, логические мины (закладки), информационный перехват в) Компьютерные сбои, изменение администрирования, топологии	ПК-2
52.	а	Что такое программные средства? а) специальные программы и системы защиты информации в информационных системах различного назначения б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла в) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними	ПК-2
53.	а	Определите, что такое криптографические средства: а) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования б) специальные программы и системы защиты информации в информационных системах различного назначения в) механизм, позволяющий получить новый класс на основе существующего	ПК-2
54.	а	Меры информационной безопасности направлены на защиту от:	ПК-2

		а) нанесения неприемлемого ущерба б) нанесения любого ущерба в) подглядывания в замочную скважину	
55.	г	Что из перечисленного не относится к числу основных аспектов информационной безопасности: а) доступность б) целостность в) конфиденциальность г) правдивое отражение действительности	ПК-2
56.	в	Компьютерная преступность в мире: а) остается на одном уровне б) снижается в) растет	ПК-2
57.	б	Что из перечисленного относится к числу основных аспектов информационной безопасности: а) подлинность - аутентичность субъектов и объектов б) целостность - актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения в) стерильность - отсутствие недекларированных возможностей	ПК-2
58.	в	Сложность обеспечения информационной безопасности является следствием: а) невнимания широкой общественности к данной проблематике б) все большей зависимости общества от информационных систем в) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним	ПК-2
59.	а	Сложность обеспечения информационной безопасности является следствием: а) комплексного характера данной проблемы, требующей для своего решения привлечения специалистов разного профиля б) наличия многочисленных высококвалифицированных злоумышленников в) развития глобальных сетей	ПК-2
60.	а, б, в, г	Какие существуют основные уровни обеспечения защиты информации? а) Законодательный	ПК-2

		б) Организационно-административный в) Программно-технический (аппаратный) г) Физический д) Вероятностный е) Распределительный	
61.		Уровни обеспечения кибербезопасности	ПК-1
62.		Специалисты по кибербезопасности	ПК-1
63.		Пути распространения угроз	ПК-1
64.		Обучение новых специалистов	ПК-1
65.		Три грани куба кибербезопасности	ПК-1
66.		Состояния данных	ПК-1
67.		Средства противодействия угрозам	ПК-1
68.		Технология, политики и процедуры кибербезопасности	ПК-1
69.		Архитектура управления безопасностью ИТ-среды	ПК-1
70.		Вредоносное программное обеспечение и вредоносный код	ПК-1
71.		Мошенничество	ПК-1
72.		Атаки	ПК-1
73.		Криптография	ПК-1
74.		Разграничение доступа	ПК-1
75.		Сокрытие данных	ПК-1
76.		Виды средств контроля целостности данных	ПК-1
77.		Цифровые подписи	ПК-1
78.		Сертификаты	ПК-1
79.		Высокая доступность	ПК-1
80.		Меры по повышению доступности	ПК-1
81.		Реагирование на инциденты	ПК-1
82.		Аварийное восстановление	ПК-1
83.		Киберпреступники	ПК-1
84.		Области распространения угроз	ПК-1
85.		Сложность угроз	ПК-1
86.		Структура работ по обеспечению кибербезопасности	ПК-1
87.		Конфиденциальность	ПК-1

88.		Целостность	ПК-1
89.		Доступность	ПК-1
90.		Архитектура управления безопасностью	ПК-1
91.		Технологии кибербезопасности	ПК-1
92.		Политики кибербезопасности	ПК-1
93.		Процедуры кибербезопасности	ПК-1
94.		Методы шифрования	ПК-1
95.		Методы разграничение доступа	ПК-1
96.		Концепция сокрытия данных	ПК-1
97.		Процессы, используемые для обеспечения целостности	ПК-1
98.		Назначение цифровых подписей	ПК-1
99.		Назначение цифровых сертификатов	ПК-1

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 в полном объёме осуществляет патентный поиск и проводит патентные исследования для исследования технического уровня и тенденций развития объектов техники, оценки патентоспособности новых технических решений, проверки патентной чистоты объектов техники и анализа конкурентоспособности объектов техники, оформляет документы о проведенных патентных исследованиях в полном соответствии с предъявляемыми требованиями, уверенно выявляет изобретения, полезные модели, промышленные образцы, в полном объеме разрабатывает, оформляет, подает и сопровождает заявки на регистрацию прав на любые объекты интеллектуальной собственности.

Оценка «хорошо» выставляется студенту, если он в достаточном объёме осуществляет патентный поиск и проводит патентные исследования для исследования технического уровня и тенденций развития объектов техники, оценки патентоспособности новых технических решений, проверки патентной чистоты объектов техники и анализа конкурентоспособности объектов техники, оформляет документы о проведенных патентных исследованиях в достаточном соответствии с предъявляемыми требованиями, уверенно выявляет изобретения, полезные модели, в достаточном объеме разрабатывает, оформляет и подает заявки на регистрацию прав на любые объекты интеллектуальной собственности.

Оценка «удовлетворительно» выставляется студенту, если он в минимальном объёме осуществляет патентный поиск и проводит патентные исследования для исследования технического уровня и тенденций развития объектов техники, оценки патентоспособности новых технических решений, проверки патентной чистоты объектов техники и анализа конкурентоспособности объектов техники, оформляет документы о проведенных патентных исследованиях в минимальном соответствии с предъявляемыми требованиями, выявляет изобретения, полезные модели, в минимальном объеме разрабатывает и оформляет заявки на регистрацию прав на основные объекты интеллектуальной собственности.

Оценка «неудовлетворительно» выставляется студенту, если он в недостаточном объёме осуществляет патентный поиск и проводит патентные исследования для исследования технического уровня и тенденций развития объектов техники, оценки патентоспособности новых технических решений, проверки патентной чистоты объектов техники и анализа конкурентоспособности объектов техники, оформляет документы о проведенных патентных исследованиях в недостаточном соответствии с предъявляемыми требованиями, фрагментарно выявляет изобретения, полезные модели, в недостаточном объеме оформляет заявки на регистрацию прав на отдельные объекты интеллектуальной собственности.

**** в соответствии с результатами освоения дисциплины и видами заданий***