

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Порохня Андрей Алексеевич
Должность: И.о. директора института перспективной инженерии
Дата подписания: 19.06.2026 16:13:01
Уникальный программный ключ:
990bea3aeec48c23bd8699e48288f8d1960c600

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

УТВЕРЖДАЮ

И. о директора института
перспективной инженерии
кандидат технических
наук, доцент
Порохня А. А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Персональная кибербезопасность
название дисциплины (модуля)

Направление подготовки/специальность	09.03.02 «Информационные системы и технологии»
Направленность (профиль)/специализация	Прикладное программирование и интернет-технологии
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 09.03.02 «Информационные системы и технологии», направленность (профиль) «Прикладное программирование и интернет-технологии».

2. ФОС является приложением к программе дисциплины (модуля) «Персональная кибербезопасность» в соответствии с образовательной программой высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии», направленность (профиль) «Прикладное программирование и интернет-технологии».

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 09.03.02 «Информационные системы и технологии», направленность (профиль) «Прикладное программирование и интернет-технологии» 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 (неудовлетворит ельно) 2 балла	Минимальный уровень (удовлетворител ьно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>Компетенция:</i> ОПК-3 способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				
Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-1 ОПК-3 Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	в недостаточном объеме использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	в минимальном объеме использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	в достаточном объеме использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	в полном объеме использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-2 ОПК-3 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	в недостаточном объеме решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	в минимальном объеме решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	в достаточном объеме решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	в полном объеме решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-3 ОПК-3 Осуществляет подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	в недостаточном объеме осуществляет подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	в минимальном объеме осуществляет подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	в достаточном объеме осуществляет подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	в полном объеме осуществляет подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

ой безопасности				
--------------------	--	--	--	--

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	ОПК-3
2.	в	Название информации, которую следует защищать (по нормативам, правилам сети, системы): а) Регламентированной б) Правовой в) Защищаемой	ОПК-3
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	ОПК-3
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	ОПК-3
5.	а	Что такое источник угрозы? а) потенциальный злоумышленник б) злоумышленник в) нет правильного ответа	ОПК-3
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	ОПК-3

		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	ОПК-3
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	ОПК-3
9.	а	Информационная безопасность зависит от следующих факторов: а) компьютеров, поддерживающей инфраструктуры б) пользователей в) информации	ОПК-3
10.	в	Основные источники внутренних отказов: а) отступление от установленных правил эксплуатации б) разрушение данных в) все ответы правильные	ОПК-3
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	ОПК-3
12.	а	Утечка информации в системе — ситуация, характеризующаяся: а) Потерей данных в системе б) Изменением формы информации	ОПК-3

		в) Изменением содержания информации	
13.	а, б	Свойством информации, наиболее актуальным при обеспечении информационной безопасности является: а) Целостность б) Доступность в) Актуальность	ОПК-3
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	ОПК-3
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	ОПК-3
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	ОПК-3
17.	а	Угроза информационной системе (компьютерной сети): а) Вероятное событие б) Детерминированное (всегда определенное) событие в) Событие, происходящее периодически	ОПК-3
18.	а	Разновидностями угроз безопасности (сети, системы) являются: а) Программные, технические, организационные, технологические б) Серверные, клиентские, спутниковые, наземные в) Личные, корпоративные, социальные, национальные	ОПК-3
19.	а	Окончательно, ответственность за защищенность данных в компьютерной сети несет: а) Владелец сети б) Администратор сети в) Пользователь сети	ОПК-3

20.	в	По механизму распространения П.О. различают: а) вирусы б) черви в) все ответы правильные	ОПК-3
21.	а	Что такое отказ, ошибки, сбой? а) случайные угрозы б) преднамеренные угрозы в) природные угрозы	ОПК-3
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	ОПК-3
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	ОПК-3
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	ОПК-3
25.	а	Определите, для чего создаются информационные системы: а) получения определенных информационных услуг б) обработки информации в) оба варианта верны	ОПК-3
26.	а	Процедура это: а) пошаговая инструкция по выполнению задачи б) обязательные действия	ОПК-3

		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	ОПК-3
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 следствии специфического состояния в) объект-метод	ОПК-3
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	ОПК-3
30.	б	Относится к человеческому компоненту СЗИ: а) системные порты б) администрация в) программное обеспечение	ОПК-3
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	ОПК-3
32.	б	Основные источники угроз информационной безопасности: а) Хищение жестких дисков, подключение к сети, инсайдерство б) Перехват данных, хищение данных, изменение архитектуры системы	ОПК-3

		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	ОПК-3
34.	а	Отметьте основную массу угроз информационной безопасности: а) Троянские программы б) Шпионские программы в) Черви	ОПК-3
35.	б	Вид идентификации и аутентификации, который получил наибольшее распространение: а) системы PKI б) постоянные пароли в) одноразовые пароли	ОПК-3
36.	в	Определите, под какие системы распространение вирусов происходит наиболее динамично: а) Windows б) Mac OS в) Android	ОПК-3
37.	а	Цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети б) инсайдерства в организации в) чрезвычайных ситуаций	ОПК-3
38.	а	Определите основные объекты информационной безопасности: а) Компьютерные сети, базы данных б) Информационные системы, психологическое состояние пользователей в) Бизнес-ориентированные, коммерческие системы	ОПК-3
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	ОПК-3
40.	а, б	Предпосылки появления угроз (несколько вариантов ответа): а) объективные	ОПК-3

		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	ОПК-3
42.	в	Выберите, что относится к ресурсам А.С. СЗИ: а) лингвистическое обеспечение б) техническое обеспечение в) все ответы правильные	ОПК-3
43.	а, б	По активности реагирования СЗИ системы делят на (несколько вариантов ответа): а) пассивные б) активные в) полупассивные	ОПК-3
44.	а	Основные принципы обеспечения информационной безопасности: а) Экономической эффективности системы безопасности б) Многоплатформенной реализации системы в) Усиления защищенности всех звеньев системы	ОПК-3
45.	б	Основные субъекты информационной безопасности: а) руководители, менеджеры, администраторы компаний б) органы права, государства, бизнеса в) сетевые базы данных, фаерволлы	ОПК-3
46.	б	Что такое ЭЦП? а) Электронно-цифровой преобразователь б) Электронно-цифровая подпись в) Электронно-цифровой процессор	ОПК-3
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	ОПК-3
48.	в	Определите наиболее распространенные угрозы информационной безопасности сети: а) Распределенный доступ клиент, отказ оборудования	ОПК-3

		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	ОПК-3
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	ОПК-3
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	ОПК-3
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	ОПК-3
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	ОПК-3
54.	а	Меры информационной безопасности направлены на защиту от:	ОПК-3

		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	ОПК-3
56.	в	Компьютерная преступность в мире: а) остается на одном уровне б) снижается в) растет	ОПК-3
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 недеklarированных возможностей	ОПК-3
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	ОПК-3
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	ОПК-3
60.	а, б, в, г	Какие существуют основные уровни обеспечения защиты информации? а) Законодательный	ОПК-3

		б) Организационно-административный в) Программно-технический (аппаратный) г) Физический д) Вероятностный е) Распределительный	
--	--	---	--

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 объеме 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 объеме 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 объеме 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 объеме 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*