МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Зам. директора по учебной работе
Пятигорского института (филиал)
СКФУ
Н.В. Данченко

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Безопасность компьютерных систем
Год начала обучения	2024
Форма обучения	очная
Реализуется в семестре	8

РАЗРАБОТАНО:

Профессор кафедры СУиИТ,
Чернышев А.Б.

Пятигорск 2024 г.

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Основы управления информационной безопасностью». 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 «Основы управления информационной безопасностью» и в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 Информационная безопасность.

3. Разработчик: Чернышев Александр Борисович, профессор кафедры систем управления и информационных технологий, доктор технических наук, доцент

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Цаплева В.В.– и.о. зав. кафедрой систем управления и информационных технологий

Члены комиссии:
Флоринский О.С. – доцент кафедры систем управления и информационных технологий
Мишин В.В.– доцент кафедры систем управления и информационных технологий

Представитель организации-работодателя:
Афанасов Владимир Христофорович - директор ООО «Сателлит»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 Информационная безопасность и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Основы управления информационной безопасностью».

«____»_____ 2024 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции 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
Компетенция: ОПК-5				
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-1 ОПК-5** Знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	Не знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации	На недостаточном знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации	На достаточном знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации	В совершенстве знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-2 ОПК-5** Понимает, как определять необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	Не понимает, как определять необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	На недостаточном уровне понимает, как определять необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации	На достаточном уровне понимает, как определять необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации	В совершенстве понимает, как определять необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.
Результаты обучения по дисциплине (модулю):	Не обладает навыками применения	На недостаточном навыками	Обладает навыками применения	В совершенстве обладает

Индикатор: **ИД-3 ОПК-5** Наделен навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в организации	нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в организации	применения нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в организации	нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в организации	навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в организации
Компетенция: ОПК-1.1				
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-1 ОПК-1.1** Знает процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах	Не знает процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах.	На недостаточном уровне знает процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах	На достаточном уровне знает процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах	В совершенстве знает процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-2 ОПК-1.1** Умеет проводить процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах	Не умеет проводить процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах	На недостаточном умеет проводить процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах	Обладает достаточными умениями проводить процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах	В совершенстве обладает умениями проводить процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-3 ОПК-1.1** Имеет практический опыт планирования	Не обладает опытом планирования и применения комплекса мер по	На недостаточном уровне обладает опытом планирования и применения	Обладает достаточным опытом планирования и применения комплекса мер по	В совершенстве обладает опытом планирования и применения комплекса

и применения комплекса мер по обеспечению управления доступом в компьютерных системах	обеспечению управления доступом в компьютерных системах	комплекса мер по обеспечению управления доступом в компьютерных системах	обеспечению управления доступом в компьютерных системах	мер по обеспечению управления доступом в компьютерных системах
Компетенция: ОПК-1.2				
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-1 ОПК-1.2** Знает принципы администрирования подсистемы информационной безопасности объекта защиты в компьютерных системах и сетях.	Не знает принципы администрирования подсистемы информационной безопасности и объекта защиты в компьютерных системах и сетях.	Плохо знает, принципы администрирования подсистемы информационной безопасности объекта защиты в компьютерных системах и сетях.	Хорошо знает принципы администрирования подсистемы информационной безопасности объекта защиты в компьютерных системах и сетях.	Отлично знает принципы администрирования подсистемы информационной безопасности объекта защиты в компьютерных системах и сетях.
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-2 ОПК-1.2** Умеет выбирать алгоритмы обеспечения работы средств обеспечения информационной безопасности в компьютерных системах и сетях.	Не способен выбирать алгоритмы обеспечения работы средств обеспечения информационной безопасности в компьютерных системах и сетях	Слабые способности выбирать алгоритмы обеспечения работы средств обеспечения информационной безопасности в компьютерных системах и сетях.	Достаточные способности выбирать алгоритмы обеспечения работы средств обеспечения информационной безопасности в компьютерных системах и сетях.	Отличные способности выбирать алгоритмы обеспечения работы средств обеспечения информационной безопасности в компьютерных системах и сетях.
Результаты обучения по дисциплине (модулю): *Индикатор:* **ИД-3 ОПК-1.2** Имеет практический опыт настройки и администрирования средств обеспечения информационной безопасности различных объектов	Не обладает навыками настройки и администрирования средств обеспечения информационной безопасности различных объектов	На недостаточном уровне обладает навыками настройки и администрирования средств обеспечения информационной безопасности	Обладает достаточными навыками настройки и администрирования средств обеспечения информационной безопасности различных объектов	В совершенстве обладает навыками настройки и администрирования средств обеспечения информационной безопасности различных

защиты в компьютерных системах и сетях.	защиты в компьютерных системах и сетях.	различных объектов защиты в компьютерных системах и сетях	защиты в компьютерных системах и сетях.	объектов защиты в компьютерных системах и сетях.

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 8	
1.	в)	Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство в) Владелец г) Пользователь	ОПК-5, ОПК-1.1, ОПК-1.2
2.	а)	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)	ОПК-5, ОПК-1.1, ОПК-1.2
3.	в)	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации в) Улучшить контроль за безопасностью этой информации г) Снизить уровень классификации этой информации	ОПК-5, ОПК-1.1, ОПК-1.2
4.	б)	Что самое главное должно продумать руководство при классификации данных? а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным б) Необходимый уровень доступности, целостности и конфиденциальности в) Оценить уровень риска и отменить контрмеры	ОПК-5, ОПК-1.1, ОПК-1.2

		г) Управление доступом, которое должно защищать данные	
5.	г)	Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? а) Владельцы данных б) Пользователи в) Администраторы г) Руководство	ОПК-5, ОПК-1.1, ОПК-1.2
6.	б)	Что такое процедура? а) Правила использования программного и аппаратного обеспечения в компании б) Пошаговая инструкция по выполнению задачи в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах г) Обязательные действия	ОПК-5, ОПК-1.1, ОПК-1.2
7.	а)	Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? а) Поддержка высшего руководства б) Эффективные защитные меры и методы их внедрения в) Актуальные и адекватные политики и процедуры безопасности г) Проведение тренингов по безопасности для всех сотрудников	ОПК-5, ОПК-1.1, ОПК-1.2
8.	г)	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски б) Когда риски не могут быть приняты во внимание по политическим соображениям в) Когда необходимые защитные меры слишком сложны г) Когда стоимость контрмер превышает ценность актива и потенциальные потери	ОПК-5, ОПК-1.1, ОПК-1.2
9.		Несанкционированный доступ и утечка информации.	ОПК-5, ОПК-1.1, ОПК-1.2
10		Виды угроз.	ОПК-5, ОПК-1.1, ОПК-1.2

11.		Непреднамеренные угрозы.	ОПК-5, ОПК-1.1, ОПК-1.2
12.		Умышленные угрозы.	ОПК-5, ОПК-1.1, ОПК-1.2
13.		Косвенные каналы утечки информации.	ОПК-5, ОПК-1.1, ОПК-1.2
14.		Непосредственные каналы утечки информации.	ОПК-5, ОПК-1.1, ОПК-1.2
15.		Виды организационных мероприятий.	ОПК-5, ОПК-1.1, ОПК-1.2
16.		Уровни правового обеспечения информационной безопасности.	ОПК-5, ОПК-1.1, ОПК-1.2
17.		Цели инженерно-технической защиты информации.	ОПК-5, ОПК-1.1, ОПК-1.2
18.		Основные аппаратные средства защиты информации.	ОПК-5, ОПК-1.1, ОПК-1.2
19.		Основные программные средства защиты информации.	ОПК-5, ОПК-1.1, ОПК-1.2
20.		Основные требования к комплексной системе защиты информации.	ОПК-5, ОПК-1.1, ОПК-1.2
21.		Основные способы несанкционированного доступа к информации в КС.	ОПК-5, ОПК-1.1, ОПК-1.2
22.		Уровни возможностей нарушителя.	ОПК-5, ОПК-1.1, ОПК-1.2
23.		Параметры политики учетных записей при использовании парольной аутентификации.	ОПК-5, ОПК-1.1, ОПК-1.2
24.		Двухфакторная аутентификация с элементами аппаратного обеспечения (диски, карты, маркеры и т.п.).	ОПК-5, ОПК-1.1, ОПК-1.2
25.		Процедура парольной инициализации.	ОПК-5, ОПК-1.1, ОПК-1.2
26.		Причины, облегчающие нарушителю реализацию угроз безопасности	ОПК-5, ОПК-1.1, ОПК-1.2

		информации в распределенных КС.	
27.		Шифрование перестановкой, его достоинства и недостатки.	ОПК-5, ОПК-1.1, ОПК-1.2
28.		Шифрование подстановкой (моно- и многоалфавитной), его достоинства и недостатки.	ОПК-5, ОПК-1.1, ОПК-1.2
29.		Свойства абсолютно стойкого шифра.	ОПК-5, ОПК-1.1, ОПК-1.2
30.		Свойства однонаправленной функции.	ОПК-5, ОПК-1.1, ОПК-1.2
31.		Схема использования симметричной КС для создания защищенного канала связи.	ОПК-5, ОПК-1.1, ОПК-1.2
32.		Три группы способов аутентификации.	ОПК-5, ОПК-1.1, ОПК-1.2

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 положениях, 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 в ходе собеседования правильно ответил на вопрос по теме собеседования, сопровождая наглядными примерами.

Оценка «хорошо» выставляется студенту, если он в ходе собеседования ответил на вопрос по теме собеседования, при этом есть неуверенность с практическими примерами.

Оценка «удовлетворительно» выставляется студенту, если он ходе собеседования ответил неуверенно на вопросы по теме собеседования, не смог привести практические примеры.

Оценка «неудовлетворительно» выставляется студенту, если он не ответил на вопрос по теме собеседования.

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

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

УТВЕРЖДАЮ
Директор института (филиала)/
декан факультета

_____
Ф.И.О.

ЛИСТ ИЗМЕНЕНИЙ

в учебно-методический комплекс по дисциплине *(модулю, практике*) «_____»
по направлению подготовки/специальности _____
направленность (профиль)/специализация_____
на _____ учебный год

№ п/п	Элемент УМК	Перечень вносимых изменений	Дата изменений

РАЗРАБОТАНО:

Руководитель ОП ВО
_____Ф.И.О.

Рассмотрено УМК института (филиала)