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
Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Системы управления инцидентами информационной безопасности

Специальность	10.05.01 Компьютерная безопасность
Специализация	Информационно-аналитическая и техническая экспертиза компьютерных систем
Форма обучения	очная
Год начала обучения	2026
Реализуется в семестре	10

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля и промежуточной аттестации по дисциплине «Системы управления инцидентами информационной безопасности». 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 (модуля) «Системы управления инцидентами информационной безопасности»

3. Разработчик: Березницкий А.С., доцент 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., заместитель директора ФБУ «Северо-Кавказский региональный центр судебной экспертизы Министерства юстиции РФ».

Экспертное заключение: Представленный ФОС по дисциплине «Системы управления инцидентами информационной безопасности» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля и промежуточной аттестации адекватны целям и задачам реализации образовательной программы высшего образования по специальности 10.05.01 Компьютерная безопасность, 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
Компетенция: ПК-4				
Индикатор: ИД-1 $_{ПК-4}$ выполняет анализ защищенности компьютерных систем с использованием сканеров безопасности, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	С грубыми ошибками использует средства автоматического реагирования на инциденты информационной безопасности.	На минимальном уровне использует средства автоматического реагирования на инциденты информационной безопасности.	На среднем уровне использует средства автоматического реагирования на инциденты информационной безопасности.	На высоком уровне сопровождение разработки программ и методик аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации
Индикатор: ИД-2 $_{ПК-4}$ осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения	С грубыми ошибками использует современные технологии и средства поиска уязвимостей.	На минимальном уровне использует современные технологии и средства поиска уязвимостей.	На среднем уровне использует современные технологии и средства поиска уязвимостей.	На высоком уровне документирует этапы разработки технологии защищенности компьютерных систем предприятия. Выполняет испытания на соответствие требованиям защиты информации
Компетенция: ПК-5				
Индикатор: ИД-2 $_{ПК-5}$ использует формализованные модели, методы и алгоритмы решения типовых задач автоматизированной информационно-аналитической поддержки процессов принятия решений	С грубыми ошибками осуществляет сопровождение и разработку средств информационно-аналитической поддержки процессов принятия решений.	На минимальном уровне осуществляет сопровождение и разработку средств информационно-аналитической поддержки процессов принятия решений.	На среднем уровне осуществляет сопровождение и разработку средств информационно-аналитической поддержки процессов принятия решений.	На высоком уровне осуществляет сопровождение и разработку средств информационно-аналитической поддержки процессов принятия решений.
Индикатор: ИД-2 $_{ПК-5}$ оценивает эффективность и качество в задачах	С грубыми ошибками способен принимать решения по управлению	На минимальном уровне способен принимать решения по управлению	На среднем уровне способен принимать решения по	На высоком уровне способен принимать решения по управлению

прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации	информационной безопасности на предприятии при различной априорной неопределенности имеющейся информации.	информационной безопасности на предприятии при различной априорной неопределенности имеющейся информации.	управлению информационной безопасности на предприятии при различной априорной неопределенности имеющейся информации.	информационной безопасности на предприятии при различной априорной неопределенности имеющейся информации.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1.		Что такое инцидент информационной безопасности низкого уровня?	ПК-4
2.		Что такое анализ инцидентов информационной безопасности?	ПК-4
3.		Что такое конфиденциальность?	ПК-4
4.		Что такое система управления инцидентами информационной безопасности (SIEM)?	ПК-4
5.		Что такое неличная информация?	ПК-4
6.		Что такое DDoS-атака?	ПК-4
7.		Что такое инцидент информационной безопасности высокого уровня?	ПК-4
8.		Что такое процедура восстановления после инцидента?	ПК-4
9.		Что такое конфиденциальная информация?	ПК-4
10.		Что такое хакерская атака?	ПК-4
11.		Что такое потенциальный инцидент информационной безопасности?	ПК-4
12.		Что такое инцидент-расследование?	ПК-4
13.		Что такое ИБИ?	ПК-4
14.		Как называется процесс управления ИБИ?	ПК-4
15.		Что такое оценка рисков ИБ?	ПК-4
16.	Активы, уязвимости, угрозы	Какие три элемента учитываются при оценке рисков ИБ?	ПК-4
17.	APT	Как называется длительная кибератака на конкретную организацию?	ПК-4
18.	SIEM	Как называется система, которая собирает и анализирует данные из разных источников, чтобы обнаружить угрозы безопасности?	ПК-4
19.	CVE	Как называется уникальный идентификатор, присваиваемый уязвимости программного обеспечения, чтобы облегчить идентификацию и отслеживание уязвимостей?	ПК-4
20.	NIST	Как называется организация, которая разрабатывает и рекомендует стандарты и руководства по информационной безопасности?	ПК-4
21.	Phishing	Как называется вид мошенничества, при котором злоумышленник пытается получить конфиденциальную информацию, используя ложные электронные письма?	ПК-4
22.	Firewall	Как называется система, которая фильтрует трафик между внутренней и внешней сетями на основе установленных правил безопасности?	ПК-4

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1.	Правила и процедуры для предотвращения инцидентов	Что такое профилактика ИБ?	ПК-5
2.	Анализ и реагирование на инциденты	Что включает в себя реагирование на ИБИ?	ПК-5
3.	Управление инцидентами	Что включает в себя управление ИБИ?	ПК-5
4.	Угрозы со стороны сотрудников	Какие угрозы могут исходить от внутренних пользователей?	ПК-5
5.	Международные стандарты ИБ	Какие международные стандарты существуют в области ИБ?	ПК-5
6.	Правовые аспекты ИБ	Какие правовые аспекты важны при управлении ИБИ?	ПК-5
7.	Системы оповещения об инцидентах	Что такое системы оповещения об ИБИ?	ПК-5
8.	Инцидентный менеджмент	Что такое инцидентный менеджмент в контексте ИБИ?	ПК-5
9.	Журнал событий безопасности	Что такое журнал событий безопасности?	ПК-5
10.	Информационный риск	Что такое информационный риск?	ПК-5
11.	Информационный актив	Что такое информационный актив?	ПК-5
12.	Конфиденциальность, целостность, доступность	Какие три аспекта ИБ необходимо учитывать?	ПК-5
13.	Безопасность периметра	Что такое безопасность периметра?	ПК-5
14.	Событие	Как называется любое изменение состояния системы, происходящее в определенный период времени?	ПК-5
15.	Уязвимость	Как называется слабое место в системе, которое может быть использовано злоумышленниками для нарушения безопасности?	ПК-5
16.	Инцидент	Как называется событие, при котором нарушается целостность, конфиденциальность или доступность информации, либо нарушаются требования информационной безопасности?	ПК-5
17.	Конфиденциальность	Какой принцип информационной безопасности обеспечивает защиту информации от несанкционированного доступа и раскрытия?	ПК-5
18.	Целостность	Какой принцип информационной безопасности обеспечивает защиту информации от несанкционированного изменения?	ПК-5
19.	Доступность	Какой принцип информационной безопасности обеспечивает доступность информации для авторизованных пользователей?	ПК-5
20.	SLA	Как называется документ, который определяет уровень обслуживания, предоставляемый поставщиком услуг заказчику?	ПК-5
21.	Инцидент информационной безопасности	Что такое Инцидент информационной безопасности?	ПК-5
22.	Идентификация	Что такое идентификация в рамках системы управления инцидентами информационной безопасности?	ПК-5
23.	Информационные ресурсы	Какие информационные ресурсы могут быть уязвимыми для инцидентов информационной безопасности?	ПК-5
24.	Инцидентный менеджмент	Что такое инцидентный менеджмент в рамках системы управления инцидентами информационной безопасности?	ПК-5
25.	Журналы аудита	Какую роль играют журналы аудита в системе управления инцидентами информационной безопасности?	ПК-5

26.	Оценка рисков	Что такое оценка рисков в контексте системы управления инцидентами информационной безопасности?	ПК-5
27.	Атака внедрения кода	Какой тип атаки осуществляется посредством обращения к уязвимому приложению с помощью вредоносного кода?	ПК-5
28.	SQL-инъекция	Какая уязвимость включает использование некорректного синтаксиса ввода данных, что может привести к выполнению SQL-запросов, заданных вредоносным пользователем?	ПК-5
29.		Что означает термин "закалка" в контексте тестирования уязвимостей?	ПК-5
30.	DDoS-атака	Какой тип атаки осуществляется путем навязывания системе большой нагрузки или использования всех доступных ресурсов системы?	ПК-5
31.		Какой тип уязвимости может быть использован для осуществления атак, направленных на ввод и выполнение вредоносного кода на сервере?	ПК-5
32.	Да	Можно ли использовать систему управления инцидентами для предотвращения инцидентов?	ПК-5
33.	Нет	Могут ли сотрудники службы безопасности получить доступ к личной информации пользователей в системе управления инцидентами?	ПК-5
34.	72 часа	Каково обычное время реагирования на инцидент в системе управления инцидентами?	ПК-5

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, если студент:

- знает полностью понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов;

- умеет полностью производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы атематической логики и теории алгоритмов к решению задач математической кибернетики;

- владеет полностью навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач.

Оценка «хорошо» выставляется, если студент:

- знает на хорошем уровне понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов;

- умеет на хорошем уровне производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы атематической логики и теории алгоритмов к решению задач математической кибернетики;

- владеет на хорошем уровне навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач.

Оценка «удовлетворительно» выставляется, если студент:

- знает понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов;

- в основном, умеет производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы атематической логики и теории алгоритмов к решению задач математической кибернетики;

- в основном, навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач.

Оценка «неудовлетворительно» выставляется, если студент:

- знает не все понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов;

- недостаточно умеет производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы атематической логики и теории алгоритмов к решению задач математической кибернетики;

- слабо владеет навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач.