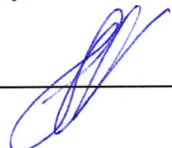


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«19» марта 2024 г, протокол № 8
Исполняющий обязанности
заведующего кафедрой

 Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.О.23 Основы управления информационной безопасностью

Направление подготовки

10.03.01 Информационная безопасность

профиль

Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования

БАКАЛАВРИАТ

Южно-Сахалинск
2024 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	<p>УК-3.1. Знать основные приемы и нормы социального взаимодействия; основные понятия и методы конфликтологии, технологии межличностной и групповой коммуникации в деловом взаимодействии.</p> <p>УК-3.2. Уметь устанавливать и поддерживать контакты, обеспечивающие успешную работу в коллективе; применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри команды.</p> <p>УК-3.3. Владеть простейшими методами и приемами социального взаимодействия и работы в команде.</p>
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	<p>ОПК-1.1 - Знает сущность и понятие информационной безопасности, характеристику ее составляющих, а также основные средства и способы обеспечения информационной безопасности;</p> <p>ОПК-1.2 - Умеет проводить анализ и выбор средств и способов обеспечения информационной безопасности;</p> <p>ОПК-1.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности.</p>
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	<p>ОПК-5.1 - Знает основные виды и порядок применения нормативных и методических документов, а также порядок соблюдения законодательных ограничений в сфере профессиональной деятельности;</p> <p>ОПК-5.2 - Умеет использовать основные методы правовой оценки различных подходов решения задач в сфере профессиональной деятельности;</p> <p>ОПК-5.3 - Владеет навыками разработки текстовой документации в области профессиональной деятельности в соответствии с нормативными требованиями, регламентирующими деятельность по защите информации.</p>
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение	<p>ОПК-10.1 - Знает принципы формирования политики информационной безопасности автоматизированных систем;</p> <p>ОПК-10.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по</p>

	комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	обеспечению информационной безопасности в организации; ОПК-10.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем
ОПК-4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1 - Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; ОПК-4.1.2 - Умеет определять подлежащие защите информационные ресурсы, определять параметры настройки программного обеспечения, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; ОПК-4.1.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Анализ объекта защиты	УК-3; ОПК-1; ОПК-5; ОПК-10; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету
2.	Модель угроз и модель нарушителя	УК-3; ОПК-1; ОПК-5; ОПК-10; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету
3.	Основы управления рисками информационной безопасности	УК-3; ОПК-1; ОПК-5; ОПК-10; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету
4.	Система управления информационной безопасностью	УК-3; ОПК-1; ОПК-5; ОПК-10; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету
5.	Политика информационной безопасности	УК-3; ОПК-1; ОПК-5; ОПК-10; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету

Лабораторное занятие №1 (6 ч.)

Тема **Анализ объекта защиты**

Вопросы для обсуждения:

1. Стандартизация систем и процессов управления информационной безопасностью
2. Формальное описание структуры информационной системы.
3. Определение типа системы и требований к ней по уровню защиты информации
4. Оценка ущерба от реализации угроз информационной безопасности

Лабораторное занятие №2 (6 ч.)

Тема **Модель угроз и модель нарушителя**

Вопросы для обсуждения:

1. Определение угроз и каналов утечки информации от действий нарушителя.

2. Построение модели угроз для выбранного объекта информатизации.
3. Отбор параметров модели

Лабораторное занятие №3 (6 ч.)

Тема Основы управления рисками информационной безопасности

Вопросы для обсуждения:

1. Анализ рисков информационной безопасности на основе построения модели информационных потоков.
2. Разработка методики оценки рисков информационной безопасности
3. Выделение типов информации и формирование требований по защите

Лабораторное занятие №4 (6 ч.)

Тема Система управления информационной безопасностью

Вопросы для обсуждения:

1. Формирование требований к системе защиты информации.
2. Концептуальные основы построения защиты информационных процессов от несанкционированного доступа в компьютерных системах
3. Управление персоналом в контексте обеспечения информационной безопасности.

Лабораторное занятие №5 (6 ч.)

Тема Политика информационной безопасности

Вопросы для обсуждения:

1. Цели Политики СУИБ. Структура и содержание Политики СУИБ
2. Формирование требований к политике информационной безопасности.
3. Источники информации для разработки Политики СУИБ.

Задания для текущего контроля

№ раздела дисциплины	Наименование лабораторных работ
1.	Стандарты информационной безопасности. Моделирование деятельности организации Модель автоматизированной ИС
2.	Состав и особенности информационных потоков организации Оценка информационных потоков организации по уровню конфиденциальности Модель угроз и модель нарушителя
3.	Методика оценки рисков информационной безопасности Оценка вероятности реализации каждого вида угроз и оценка усредненных убытков (рисков). Формирование требований по защите информации
4.	Формирование концепции информационной безопасности Требования к системе защиты информации Организационные меры информационной безопасности автоматизированных систем
5.	Разработка политики информационной безопасности: область действия; Объект защиты; стратегия защиты; организационная структура.

Примерные темы самостоятельной работы

1. Международные и отечественные стандарты информационной безопасности.
2. Моделирование деятельности организации
3. Моделирование автоматизированной ИС
4. Определение состава информационных потоков организации
5. Оценка информационных потоков организации по уровню конфиденциальности
6. Модель угроз и модель нарушителя
7. Методика оценки рисков информационной безопасности
8. Оценка вероятности реализации каждого вида угроз и оценка усредненных убытков (рисков).
9. Формирование требований по защите информации
10. Формирование концепции информационной безопасности
11. Требования к системе защиты информации
12. Организационные меры информационной безопасности автоматизированных систем
13. Определение области действия в политике информационной безопасности.
14. Определение объекта защиты в политике информационной безопасности.
15. Определение стратегии защиты информации в политике информационной безопасности.
16. Определение организационной структуры в политике информационной безопасности

Примерные темы рефератов:

1. Анализ объекта защиты
2. Технология анализа объекта защиты.
3. Типы информационных систем.
4. Методы оценки ущерба от реализации угроз информационной безопасности.
5. Комплекс стандартов в области информационной безопасности.
6. Модель угроз и модель нарушителя
7. Подходы к формированию модели нарушителя и модели угроз.
8. Требования регуляторов к формированию модели нарушителя и модели угроз.
9. Основы управления рисками информационной безопасности
10. Основные определения и положения рисками.
11. Цель процесса анализа рисков ИБ.
12. Этапы и участники процесса анализа рисков ИБ.
13. Методики анализа рисков ИБ.
14. Источники информации об активах организации.
15. Оценка рисков ИБ.
16. Планирование мер по обработке выявленных рисков ИБ.
17. Использование результатов анализа рисков ИБ.
18. Основные положения стандартов в области управления рисками информационной безопасности.
19. Система управления информационной безопасностью
20. Место системы управления информационной безопасностью в рамках общей системы управления предприятием.
21. Этапы разработки и функционирования системы управления информационной безопасностью.
22. Организация управления персоналом в контексте обеспечения информационной безопасности.

Примерные вопросы к экзамену.

1. Цель и этапы анализа объектов защиты.
2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.
3. Идентификация и классификация объектов защиты.
4. Подходы к разграничению доступа в рамках организации. Структура документов, регламентирующих разграничение доступа.

5. Подходы к построению модели нарушителя.
6. Классификация нарушителей (ФСТЭК).
7. Классификация угроз безопасности персональных данных (ФСТЭК).
8. Методика определения актуальных угроз (ФСТЭК).
9. Методика оценки ущерба, нанесённого при реализации угроз информационной безопасности.
10. Предоставление сотруднику доступа к конфиденциальной информации. Основные разделы Инструкции по внесению изменений в списки пользователей.
11. Обязанности сотрудников Службы безопасности при обучении и увольнении сотрудников.
12. Упрощённая модель классификации субъектов.
13. Основные положения регламента контроля использования технических средств обработки и передачи информации.
14. Основные положения инструкции по организации парольной защиты.
15. Классификация объектов при составлении аварийного плана.
16. Требования к различным классам объектов и их резервированию.
17. Основные положения плана обеспечения непрерывной работы и восстановления работоспособности.
18. Приведите примеры источников информации об инцидентах информационной безопасности.
19. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.
20. Создание СУИБ на предприятии.
21. Методики и технологии управления рисками.
22. Современные методы и средства анализа и управления рисками информационных систем компаний.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (зачет)			20	43
Итого за семестр			60	100

Критерии оценивания:

Критерием оценивания является выполнение самостоятельных заданий, контрольных и лабораторных работ.

Самостоятельные задания, контрольные и лабораторные работы по результатам выполнения и защиты оцениваются с учетом следующих основных параметров:

- своевременное выполнение работы;
- полнота и правильность ответов на вопросы, заданные в ходе защиты работы.

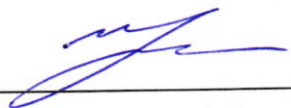
В случае выполнения данных условий, студент имеет возможность сдавать теоретический зачет по вопросам.

Оценка «отлично» выставляется студенту, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

Оценка «хорошо» выставляется студенту, твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.

Оценка «удовлетворительно» выставляется студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач. оценка «не зачтено» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в ответе или в решении задач грубые ошибки.

Составитель _____



Мазур И. К.

«19» марта 2024 г.