

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН

на заседании кафедры

«20» сентября 2024 г., протокол № 1

Исполняющий обязанности заведующего  
кафедрой

 \_\_\_\_\_ Осипов Г.С.

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

**Б1.В.01 Безопасные информационные технологии и системы**

**Направление подготовки**

09.04.03 Прикладная информатика

**Профиль подготовки:**

Искусственный интеллект и анализ данных

**Уровень высшего образования**

МАГИСТРАТУРА

Южно-Сахалинск, 2024

## 1. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий	ПКС-1.1 - Знает виды моделей бизнес-процессов, требования к информационной системе, виды архитектур ИС; технологии программирования, тестирования и внедрения ИС; ПКС-1.2 - Умеет разрабатывать модели бизнес-процессов, требования к информационной системе, архитектуру ИС, применять технологии программирования, тестирования и внедрения ИС; ПКС-1.3 – Владеет методами разработки модели бизнес-процессов, требований к информационной системе, архитектур ИС, технологиями программирования, тестирования и внедрения ИС
ПКС-2	Способен управлять проектированием, процессом, разработки компьютерного программного обеспечения, конфигурациями и выпусками программного продукта	ПКС-2.1 - Знает методы управления проектированием, процессом, разработки компьютерного программного обеспечения, конфигурациями и выпусками программного продукта ПКС-2.2 – Умеет применять методы управления проектированием, процессом, разработки компьютерного программного обеспечения, конфигурациями и выпусками программного продукта; ПКС-2.3 – Владеет методами управления проектированием, процессом, разработки компьютерного программного обеспечения, конфигурациями и выпусками программного продукта.
ПКС-3	Способен осуществлять организацию взаимодействия с заказчиком, планирования проекта ИС; руководить разработкой программного кода, верификацией и тестированием ИС	ПКС-3.1 - Знает методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.2 - Умеет применять методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.3 - Владеет методами организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС.

## 2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
-------	--	---	----------------------------------

1	Общая характеристика информационных систем Классификация информационных систем	ПКС-1 ПКС-2 ПКС-3	Лабораторный практикум, контрольные задания, вопросы к зачету/экзамену
2	Структура информационных систем. Модели жизненного цикла информационных систем	ПКС-1 ПКС-2 ПКС-3	Лабораторный практикум, контрольные задания, вопросы к зачету/экзамену
3	Безопасность информационных систем Информационное обеспечение информационной системы	ПКС-1 ПКС-2 ПКС-3	Лабораторный практикум, контрольные задания, вопросы к зачету/экзамену
4	Проектирование и совершенствование технологии обеспечения информационной безопасности	ПКС-1 ПКС-2 ПКС-3	Лабораторный практикум, контрольные задания, вопросы к зачету/экзамену
5	Автоматизированные системы. Методология обеспечения информационной безопасности автоматизированных систем	ПКС-1 ПКС-2 ПКС-3	Лабораторный практикум, контрольные задания, вопросы к зачету/экзамену
6	Анализ характеристик системы управления на основе информационного графа. Технология создания защищенных систем.	ПКС-1 ПКС-2 ПКС-3	Лабораторный практикум, контрольные задания, вопросы к зачету/экзамену
7	Анализ требований, угроз, уязвимостей объекта защиты. Особенности построения защищенных информационных систем»	ПКС-1 ПКС-2 ПКС-3	Лабораторный практикум, контрольные задания, вопросы к зачету/экзамену
8	Вычисление числовых характеристик системы управления с помощью задания числовой функции на структурном графе системы	ПКС-1 ПКС-2 ПКС-3	Лабораторный практикум, контрольные задания, вопросы к зачету/экзамену

### Контрольные задания

1. Что такое информация, субъекты информационных отношений?
2. Дайте определение Информационной технологии.
3. Компьютерная система-это...
4. Раскройте термин информационная безопасность
5. Что такое уязвимость?
6. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?
7. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?
8. Укажите модель управления доступом, к которой относится основная теорема безопасности.
9. Какие виды информации существуют в зависимости от категории доступа к ней?
10. Основные принципы системного подхода при создании сложных систем.
11. Перечислите основные объекты информационной безопасности. Дайте их определения.
12. Понятия ущерба, риска и угрозы.
13. Для чего нужна стандартизация в сфере информационной безопасности?

14. Какую информацию относят к секретной, конфиденциальной?
15. Перечислите основные риски ИБ. Дайте их определения.
16. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
17. Охарактеризуйте понятие большие данные.
18. Какую информацию относят к секретной, конфиденциальной?
19. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
20. Какие применяются методы защиты информации от промышленного шпионажа?
21. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
22. Какие организационные меры обеспечения безопасности Вы знаете?
23. Какие технические меры обеспечения безопасности Вы знаете?
24. Основные принципы обеспечения ИБ
25. Основные функции системы безопасности.
26. Защищаемая информация – это..

### Тест

- 1 Какой вид идентификации и аутентификации получил наибольшее распространение:
  - а) системы PKI
  - б) постоянные пароли
  - в) одноразовые пароли
- 2 Заключительным этапом построения системы защиты является:
  - а) сопровождение
  - б) планирование
  - в) анализ уязвимых мест
- 3 Какие угрозы безопасности информации являются преднамеренными:
  - а) ошибки персонала
  - б) открытие электронного письма, содержащего вирус
  - в) неавторизованный доступ
- 4 Какой подход к обеспечению безопасности имеет место:
  - а) теоретический
  - б) комплексный
  - в) логический
- 5 Таргетированная атака — это:
  - а) атака на сетевое оборудование
  - б) атака на компьютерную систему крупного предприятия
  - в) атака на конкретный компьютер пользователя
- 6 Кто является основным ответственным за определение уровня классификации информации:
  - а) руководитель среднего звена
  - б) владелец
  - в) высшее руководство
- 7 Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует обычно предпринять руководству:
  - а) снизить уровень защищенности этой информации
  - б) улучшить контроль за безопасностью этой информации
  - в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

- 8 Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
- а) владельцы данных
  - б) руководство
  - в) администраторы
- 9 Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
- а) хакеры
  - б) контрагенты
  - в) сотрудники
- 10 Процедурой называется:
- а) пошаговая инструкция по выполнению задачи
  - б) обязательные действия
  - в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

### **Примерный перечень вопросов к экзамену за 1 семестр**

1. Перечислите основные риски ИБ. Дайте их определения.
2. Какие требования предъявляются к комплексной системе безопасности объекта?
3. В чем суть гарантированного уничтожения?
4. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
5. Охарактеризуйте понятие большие данные.
6. Какую информацию относят к секретной, конфиденциальной?
7. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
8. Какие применяются методы защиты информации от промышленного шпионажа?
9. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
10. Какие организационные меры обеспечения безопасности Вы знаете?
11. Какие технические меры обеспечения безопасности Вы знаете?
12. Основные принципы обеспечения ИБ
13. Основные функции системы безопасности.
14. Основные принципы политики ИБ.
15. Какое свойство информации является наиболее актуальным при обеспечении ИБ? Дайте его определение.
16. Свойство информации при котором невозможно ее искажение...
17. Охарактеризуйте ИТ поиска информации.
18. Охарактеризуйте ИТ обработки данных.
19. Охарактеризуйте эмерджентные технологии.
20. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?

### **Примерный перечень вопросов к экзамену за 2 семестр**

1. Элементы и подсистемы, управление и информация, самоорганизация.
2. Основные угрозы безопасности информации АС и их классификация.
3. Какие требования предъявляются к комплексной системе безопасности объекта?
4. В чем суть гарантированного уничтожения?

5. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
6. Охарактеризуйте понятие большие данные.
7. Какую информацию относят к секретной, конфиденциальной?
8. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
9. Какие применяются методы защиты информации от промышленного шпионажа?
10. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
11. Какие организационные меры обеспечения безопасности Вы знаете?
12. Какие технические меры обеспечения безопасности Вы знаете?
13. Основные принципы обеспечения ИБ
14. Основные функции системы безопасности.
15. Правовые методы обеспечения ИБ
16. Способы представления информации о правах доступа.
17. Характеристика качества
18. Показатели и критерии эффективности
19. Методические вопросы оценки эффективности сложных систем.
20. Дайте определение понятию «ядро безопасности»
21. Кратко опишите архитектуру защищенной системы.

Составитель

«12» сентября 2024 г.

Мазур И.К., доцент кафедры  
информатики