

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

УТВЕРЖДЕН
на заседании кафедры
«22» мая 2025 г., протокол № 9
Заведующий кафедрой информатики


Осипов Г.С.

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

Б1.В.11 «Основы информационной безопасности»

Направление подготовки
09.03.03 Прикладная информатика

профиль
Автоматизированные системы обработки информации и управления

**Уровень высшего образования
БАКАЛАВРИАТ**

Южно-Сахалинск, 2025 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знать методы поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа. УК-1.2. Уметь применять методы поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач. УК-1.3. Владеть методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач.
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. УК-2.2. Умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты решений для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности. УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией.
ПКС-2	Способен проводить формализацию предметной области с целью создания информационной системы	ПКС-2.1 - Знает требования к компьютерному программному обеспечению; виды технической спецификации на программные компоненты и их взаимодействие; методы проектирование компьютерного программного обеспечения ПКС-2.2 – Умеет применять требования к компьютерному программному обеспечению; разрабатывать технические спецификации на программные компоненты и их взаимодействие; применять методы проектирования компьютерного программного обеспечения; ПКС-2.3 – Владеет методами разработки требований к компьютерному программному обеспечению, технических спецификаций на программные компоненты, методами проектирования компьютерного программного обеспечения.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Информационная безопасность в системе национальной безопасности Российской Федерации	УК-1; УК-2; ПКС-2	Задания к практическим работам, контрольные вопросы, вопросы к зачету
2.	Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации. Государственная тайна. Государственная система защиты информации	УК-1; УК-2; ПКС-2	Задания к практическим работам, контрольные вопросы, вопросы к зачету
3.	Методологические основы защиты информации	УК-1; УК-2; ПКС-2	Задания к практическим работам, контрольные вопросы, вопросы к зачету
4.	Угрозы информационной безопасности	УК-1; УК-2; ПКС-2	Задания к практическим работам, контрольные вопросы, вопросы к зачету
5.	Построение систем защиты информации	УК-1; УК-2; ПКС-2	Задания к практическим работам, контрольные вопросы, вопросы к зачету
6.	Нормативно правовое регулирование защиты информации	УК-1; УК-2; ПКС-2	Задания к практическим работам, контрольные вопросы, вопросы к зачету

3. Оценочные средства

Тестирование является одним из средств формального контроля качества обучения – методе, основанном на стандартизированных заданиях, которые позволяют оценить знания, умения и навыки испытуемого

Требования к составлению тестового задания

Тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

– **закрытая** форма – является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя один или несколько правильных ответов.

Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде.

Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

– **открытая** форма – вопрос представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие – части слова или буквы, условные обозначения, линии или изображения элементов схемы или графика.

Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

– **установление соответствия** – в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

– **установление последовательности** – предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

Примерный тест

Задания для проверки сформированности компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ПКС-2. Способен проводить формализацию предметной области с целью создания информационной системы

Вопрос 1 (Одиночный выбор)

Что понимается под информационной безопасностью?

1. Защита компьютеров от вирусов
2. Состояние защищённости национальных интересов в информационной сфере
3. Комплекс антивирусных программ
4. Шифрование всех данных

Ответ: 2. Состояние защищённости национальных интересов в информационной сфере

Вопрос 2 (Верно / Неверно)

УК-1.1 требует знания методов поиска, сбора и обработки информации.

1. Верно
2. Неверно

Ответ: 1. Верно

Вопрос 3 (Множественный выбор)

Какие из перечисленных свойств информации являются основными с точки зрения ИБ?

(Выберите **три** варианта)

1. Актуальность
2. Конфиденциальность
3. Доступность
4. Целостность
5. Полнота

Ответ: 2, 3, 4

Вопрос 4 (Открытый вопрос)

Дайте определение термину «персональные данные» согласно Федеральному закону.

Ответ: Любая информация, относящаяся к прямо или косвенно определённом, или определяемому физическому лицу (субъекту персональных данных).

Вопрос 5 (Одиночный выбор)

Какой федеральный закон регулирует отношения, связанные с государственной тайной?

1. ФЗ «Об информации, информационных технологиях и о защите информации»
2. ФЗ «О коммерческой тайне»
3. Закон РФ «О государственной тайне»
4. ФЗ «О персональных данных»

Ответ: 3. Закон РФ «О государственной тайне»

Вопрос 6 (Сопоставление)

Сопоставьте вид тайны и нормативный документ:

Вид тайны	Документ
1. Государственная тайна	А. ФЗ «О коммерческой тайне»
2. Коммерческая тайна	Б. ФЗ «О персональных данных»
3. Персональные данные	В. Закон РФ «О государственной тайне»
4. Служебная тайна	Г. Регулируется подзаконными актами

Ответ: 1–В, 2–А, 3–Б, 4–Г

Вопрос 7 (Верно / Неверно)

Доктрина информационной безопасности Российской Федерации — это федеральный закон.

1. Верно
2. Неверно

Ответ: 2. Неверно (это документ стратегического планирования, указ Президента)

Вопрос 8 (Одиночный выбор)

Что из перечисленного относится к организационным методам защиты информации?

1. Шифрование
2. Межсетевые экраны
3. Регламентация доступа
4. Антивирусный мониторинг

Ответ: 3. Регламентация доступа

Вопрос 9 (Множественный выбор)

Какие из перечисленных угроз относятся к нарушению целостности информации?

(Выберите **два** варианта)

1. Перехват данных
2. Модификация базы данных
3. Уничтожение файла
4. Несанкционированное копирование

Ответ: 2, 3

Вопрос 10 (Открытый вопрос)

В чём различие между идентификацией и аутентификацией?

Ответ: Идентификация — предъявление идентификатора (имя, логин).

Аутентификация — подтверждение подлинности (пароль, биометрия, ключ).

Вопрос 11 (Одиночный выбор)

Какой стандарт является основополагающим в серии ISO/IEC 27000?

1. ISO/IEC 27001
2. ISO/IEC 27002
3. ISO/IEC 27000
4. ISO/IEC 27005

Ответ: 1. ISO/IEC 27001

Вопрос 12 (Верно / Неверно)

Компьютерный вирус — это программное обеспечение, которое самовоспроизводится и внедряется в другие программы.

1. Верно
2. Неверно

Ответ: 1. Верно

Вопрос 13 (Открытый вопрос)

Перечислите любые два типа компьютерных вирусов по среде обитания.

Ответ: Файловые, загрузочные, макровирусы, скриптовые (любые два)

Вопрос 14 (Одиночный выбор)

Какой метод криптографии использует один ключ для шифрования и расшифрования?

1. Симметричный
2. Асимметричный
3. Хэширование
4. Электронная подпись

Ответ: 1. Симметричный

Вопрос 15 (Сопоставление)

Сопоставьте понятие и определение:

Понятие	Определение
1. Шифр	А. Процесс восстановления открытого текста
2. Ключ	Б. Алгоритм криптографического преобразования
3. Дешифрование	В. Параметр, управляющий преобразованием
4. Шифрование	Г. Процесс преобразования открытого текста в зашифрованный

Ответ: 1–Б, 2–В, 3–А, 4–Г

Вопрос 16 (Верно / Неверно)

Электронная подпись обеспечивает конфиденциальность документа.

1. Верно
2. Неверно

Ответ: 2. Неверно (она обеспечивает целостность и авторство)

Вопрос 17 (Одиночный выбор)

Что понимается под «утечкой информации»?

1. Уничтожение данных
2. Неконтролируемое распространение защищаемой информации
3. Блокировка доступа
4. Копирование данных с разрешения

Ответ: 2. Неконтролируемое распространение защищаемой информации

Вопрос 18 (Множественный выбор)

Какие из перечисленных мер относятся к антивирусной защите?

(Выберите **два** варианта)

1. Использование межсетевого экрана
2. Регулярное обновление антивирусных баз
3. Ограничение физического доступа
4. Запрет на запуск непроверенных программ

Ответ: 2, 4

Вопрос 19 (Открытый вопрос)

Что такое «информационное оружие»?

Ответ: Средства и методы информационного воздействия, направленные на нарушение безопасности информации, дезорганизацию систем управления, уничтожение, искажение или хищение информационных ресурсов.

Вопрос 20 (Одиночный выбор)

Какой из перечисленных методов относится к техническим каналам утечки информации?

1. Изучение документов
2. Акустический канал
3. Опрос персонала
4. Анализ открытых источников

Ответ: 2. Акустический канал

Критерии оценки знаний при проведении тестирования

Отметка «**отлично**» выставляется при условии правильного ответа не менее чем 85% тестовых заданий;

Отметка «**хорошо**» выставляется при условии правильного ответа не менее чем 70 % тестовых заданий;

Отметка «**удовлетворительно**» выставляется при условии правильного ответа не менее 50 %;

Отметка «**неудовлетворительно**» выставляется при условии правильного ответа менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации