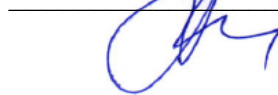


**Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»
Кафедра информатики**

УТВЕРЖДЕН
на заседании кафедры
«26» мая 2026 г., протокол № 9
Директор ИЕНиТБ



Фёдоров О.А.

**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, 2026 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	УК-3.1. Знать основные приемы и нормы социального взаимодействия; основные понятия и методы конфликтологии, технологии межличностной и групповой коммуникации в деловом взаимодействии. 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. УК-3.3. Владеть простейшими методами и приемами социального взаимодействия и работы в команде.
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 - Знает сущность и понятие информационной безопасности, характеристику ее составляющих, а также основные средства и способы обеспечения информационной безопасности; ОПК-1.2 - Умеет проводить анализ и выбор средств и способов обеспечения информационной безопасности; ОПК-1.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1 - Знает основные виды и порядок применения нормативных и методических документов, а также порядок соблюдения законодательных ограничений в сфере профессиональной деятельности; ОПК-5.2 - Умеет использовать основные методы правовой оценки различных подходов решения задач в сфере профессиональной деятельности; ОПК-5.3 - Владеет навыками разработки текстовой документации в области профессиональной деятельности в соответствии с нормативными требованиями, регламентирующими деятельность по защите информации.
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение	ОПК-10.1 - Знает принципы формирования политики информационной безопасности автоматизированных систем; ОПК-10.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по

	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

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

Вопросы с выбором одного правильного ответа

1. **Что является основной целью управления информационной безопасностью?**

- а) Полное исключение любых инцидентов ИБ.
- б) Обеспечение приемлемого уровня рисков при использовании информационных активов.
- в) Максимальная закрытость всех данных организации.
- г) Использование только сертифицированных средств защиты.

Правильный ответ: б.

2. **Какой из перечисленных документов задаёт базовый подход к управлению ИБ на международном уровне?**

- а) ГОСТ Р ИСО/МЭК 27001.
- б) ФЗ «О персональных данных».
- в) Приказ ФСТЭК № 21.
- г) Доктрина информационной безопасности РФ.

Правильный ответ: а.

3. **Триада CIA в информационной безопасности включает:**

- а) Конфиденциальность, целостность, доступность.
- б) Контроль, идентификация, аутентификация.
- в) Конфиденциальность, изоляция, авторизация.
- г) Целостность, контроль, аудит.

Правильный ответ: а.

4. **Что понимается под «риском информационной безопасности»?**

- а) Факт уже произошедшего инцидента.
- б) Потенциальный ущерб от реализации угрозы при наличии уязвимости.
- в) Наличие уязвимости в системе.
- г) Отсутствие средств защиты.

Правильный ответ: б.

5. **Какой этап следует первым в цикле управления рисками ИБ?**

- а) Оценка последствий.
- б) Идентификация активов и их ценности.
- в) Выбор мер защиты.
- г) Мониторинг и пересмотр.

Правильный ответ: б.

6. **В модели PDCA применительно к СУИБ (системе управления ИБ) этап «Check» означает:**

- а) Планирование мер защиты.
- б) Внедрение средств защиты.
- в) Контроль и измерение эффективности.

г) Корректирующие действия.

Правильный ответ: в.

7. Кто в организации несёт основную ответственность за обеспечение ИБ?

а) Служба информационной безопасности.

б) IT-отдел.

в) Руководство организации (топ-менеджмент).

г) Отдел кадров.

Правильный ответ: в.

8. Политика информационной безопасности — это:

а) Технический документ с настройками межсетевых экранов.

б) Высокоуровневый документ, отражающий намерения и обязательства руководства по ИБ.

в) Инструкция для пользователей по работе с почтой.

г) Перечень штрафов за нарушения ИБ.

Правильный ответ: б.

9. Что такое «владелец информационного актива»?

а) Лицо, которое физически хранит носитель с данными.

б) Лицо, отвечающее за классификацию, защиту и использование актива.

в) Системный администратор, обслуживающий сервер.

г) Сотрудник службы безопасности.

Правильный ответ: б.

10. Какой метод оценки рисков ИБ опирается на экспертные суждения и качественные шкалы (например, «низкий/средний/высокий»)?

а) Количественный.

б) Качественный.

в) Статистический.

г) Вероятностный.

Правильный ответ: б.

11. Сопоставьте термин и определение:

Термин	Определение
1. Угроза	А. Слабое место, которое может быть использовано для реализации угрозы
2. Уязвимость	Б. Потенциальное событие, способное нанести ущерб
3. Воздействие (impact)	В. Степень ущерба, который может быть нанесён при реализации угрозы

Правильный ответ: 1–Б, 2–А, 3–В.

12. Сопоставьте стандарт/документ и его основное назначение:

Документ	Назначение
1. ISO/IEC 27001	А. Требования к системе менеджмента ИБ (сертификация)
2. ISO/IEC 27002	Б. Практические рекомендации и меры контроля ИБ
3. ГОСТ Р ИСО/МЭК 15408	В. Критерии оценки безопасности ИТ (Common Criteria)

Правильный ответ: 1–А, 2–Б, 3–В.

13. Сопоставьте тип контроля и пример:

Тип контроля	Пример
1. Административный	А. Политика паролей и обучение сотрудников
2. Технический	Б. Межсетевой экран, шифрование
3. Физический	В. Контроль доступа в серверную, видеонаблюдение

Правильный ответ: 1–А, 2–Б, 3–В.

14. Сопоставьте категорию риска и способ обработки:

Категория риска	Способ обработки
1. Высокий риск, критичный для бизнеса	А. Принять меры по снижению (mitigation)
2. Низкий риск с малой вероятностью	Б. Принять риск (acceptance)
3. Риск, который можно передать (например, страхование)	В. Передача риска (transfer)

Правильный ответ: 1–А, 2–Б, 3–В.

15. Сопоставьте роль и основную задачу в управлении ИБ:

Роль	Задача
1. Владелец актива	А. Отвечает за классификацию и ценность данных
2. Администратор ИБ	Б. Настраивает и поддерживает средства защиты
3. Аудитор ИБ	В. Проверяет соответствие требованиям и эффективность мер

Правильный ответ: 1–А, 2–Б, 3–В.

вставьте пропущенное слово

16. Пропущенное слово: «Управление информационной безопасностью — это _____ подход к идентификации, оценке и обработке рисков ИБ в организации».

Варианты: системный, случайный, эпизодический, интуитивный.

Правильный ответ: системный.

17. Пропущенное слово: «В рамках ISO/IEC 27001 ключевым результатом является создание и поддержание _____ информационной безопасности».

Варианты: системы менеджмента, набора антивирусов, реестра инцидентов, плана резервного копирования.

Правильный ответ: системы менеджмента.

18. Пропущенное слово: «Классификация информации позволяет определить необходимый уровень _____ для каждого типа данных».

Варианты: защиты, доступности, скорости передачи, архивации.

Правильный ответ: защиты.

19. Пропущенное слово: «Инцидент ИБ — это любое событие, которое негативно влияет на _____ информационных активов».

Варианты: конфиденциальность, целостность или доступность, стоимость, срок хранения.

Правильный ответ: конфиденциальность, целостность или доступность.

20. **Пропущенное слово:** «Принцип наименьших привилегий означает, что пользователю предоставляются только те _____, которые необходимы для выполнения его обязанностей».

Варианты: права доступа, устройства, пароли, отчёты.

Правильный ответ: права доступа.

Вопросы с обоснованием выбора (выберите ответ и кратко объясните, почему он верный)

21. **Какой подход к управлению ИБ наиболее соответствует современным требованиям?**

- а) Защита только периметра сети.
- б) Комплексный риск-ориентированный подход.
- в) Использование максимально дорогих средств защиты.
- г) Полный запрет на внешние коммуникации.

Правильный ответ: б.

Обоснование: Риск-ориентированный подход позволяет целенаправленно распределять ресурсы на наиболее значимые угрозы и активы, а не тратить их на избыточные или неактуальные меры.

22. **Что важнее при выборе мер защиты?**

- а) Стоимость решения.
- б) Соответствие выявленным рискам и бизнес-целям.
- в) Популярность продукта на рынке.
- г) Рекомендации одного вендора.

Правильный ответ: б.

Обоснование: Меры защиты должны быть обоснованы оценкой рисков и поддерживать бизнес-процессы, а не выбираться по второстепенным критериям.

23. **Почему важно документировать политику ИБ и процедуры?**

- а) Чтобы усложнить работу сотрудников.
- б) Для обеспечения единообразия, обучения, аудита и юридической защиты.
- в) Только для прохождения сертификации.
- г) Чтобы увеличить объём внутренних документов.

Правильный ответ: б.

Обоснование: Документация фиксирует требования и процессы, делает их понятными для сотрудников, служит основой для контроля и аудита, а также может использоваться как доказательство должной осмотрительности.

24. **Зачем нужен регулярный пересмотр рисков ИБ?**

- а) Потому что так написано в стандарте.
- б) Потому что угрозы, активы и бизнес-процессы со временем меняются.
- в) Чтобы оправдать бюджет службы ИБ.
- г) Чтобы чаще проводить аудиты.

Правильный ответ: б.

Обоснование: Среда угроз и внутренние условия организации динамичны: появляются новые технологии, меняются процессы и требования, поэтому оценка рисков должна быть актуальной.

25. **Почему обучение сотрудников — важная мера ИБ?**

- а) Это формальность для отчётов.
- б) Человеческий фактор — один из главных источников инцидентов (фишинг, ошибки).
- в) Обучение повышает ИТ-грамотность ради общего развития.
- г) Так требуют все стандарты без исключений.

Правильный ответ: б.

Обоснование: Большинство инцидентов связано с действиями или ошибками пользователей; обучение снижает вероятность успешных атак, основанных на социальной инженерии.

Ситуационные и дополнительные вопросы

26. **Организация хранит персональные данные клиентов. Какой из факторов в первую очередь определяет требования к защите этих данных?**

- а) Количество сотрудников в IT-отделе.
- б) Требования законодательства и регуляторов (например, ФЗ-152, требования ФСТЭК/РКН).
- в) Стоимость средств защиты.
- г) Предпочтения директора по безопасности.

Правильный ответ: б.

Обоснование: Юридические требования задают обязательный минимум мер защиты; их невыполнение влечёт административную и иную ответственность.

27. **При оценке риска ИБ вы определили высокую вероятность и высокий ущерб. Какой способ обработки риска предпочтителен?**

- а) Игнорировать.
- б) Принять без изменений.
- в) Снизить риск за счёт внедрения мер защиты.
- г) Переложить на другую организацию без анализа.

Правильный ответ: в.

Обоснование: Высокий риск требует активных действий по его снижению до приемлемого уровня; принятие или перекладывание без обоснования недопустимо.

28. **Что должно быть в плане реагирования на инциденты ИБ?**

- а) Только список телефонов экстренных служб.
- б) Роли и обязанности, процедуры обнаружения, уведомления, сдерживания, восстановления и анализа.
- в) Описание всех возможных угроз.
- г) Бюджет на закупку новых средств защиты.

Правильный ответ: б.

Обоснование: План должен быть практическим руководством к действию, а не справочником угроз или финансовым документом.

29. **Какой из следующих показателей лучше всего отражает эффективность управления ИБ?**

- а) Количество установленных антивирусов.
- б) Количество проведённых тренингов.
- в) Снижение числа критических инцидентов и ущерба от них.
- г) Количество страниц в документации по ИБ.

Правильный ответ: в.

Обоснование: Конечная цель управления ИБ — снижение реального ущерба и рисков; количественные показатели «на входе» не гарантируют результата.

30. **Почему сертификация по ISO/IEC 27001 важна для организации?**

- а) Это единственный способ защитить данные.
- б) Она подтверждает наличие и результативность системы управления ИБ для клиентов, партнёров и регуляторов.
- в) Она автоматически защищает от всех кибератак.
- г) Она освобождает от любых проверок.

Правильный ответ: б.

Обоснование: Сертификация — это независимая оценка зрелости процессов ИБ; она повышает доверие заинтересованных сторон, но не гарантирует полную безопасность.

Критерии оценки знаний при проведении тестирования

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

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

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

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

Результаты текущего контроля используются при проведении промежуточной аттестации