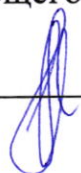


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

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.07 Основы информационной безопасности

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-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.
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.

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-2; ОПК-1	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-2; ОПК-1	Задания к практическим работам, контрольные вопросы, вопросы к зачету
3.	Методологические основы защиты информации	УК-2; ОПК-1	Задания к практическим работам, контрольные вопросы, вопросы к зачету

4.	Угрозы информационной безопасности	УК-2; ОПК-1	Задания к практическим работам, контрольные вопросы, вопросы к зачету
5.	Построение систем защиты информации	УК-2; ОПК-1	Задания к практическим работам, контрольные вопросы, вопросы к зачету
6.	Нормативно правовое регулирование защиты информации	УК-2; ОПК-1	Задания к практическим работам, контрольные вопросы, вопросы к зачету

Практическое занятие №1 (2 ч.)

Тема Информационная безопасность в системе национальной безопасности Российской Федерации

Вопросы для обсуждения:

1. Понятие информационной безопасности.
2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
3. Виды угроз информационной безопасности Российской Федерации.
4. Источники угроз информационной безопасности Российской Федерации.
5. Информационная безопасность и информационное противоборство.
6. Основные направления обеспечения информационной безопасности объектов информационной сферы государства
7. Общие методы обеспечения информационной безопасности Российской Федерации.

Практическое занятие №2 (2 ч.)

Тема Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации. Государственная тайна. Государственная система защиты информации.

Вопросы для обсуждения:

1. Как разделяется информация в зависимости от порядка ее предоставления или распространения в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации»?
2. Как разделяется информация в зависимости от категории доступа в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации»?
3. Какова цель Федерального закона «О персональных данных»? Дайте определение понятию «персональные данные».
4. Определите понятия «доступ к информации» и «конфиденциальность информации»; «предоставление информации» и «распространение информации».
5. Какие отношения регулируются в Федеральном законе «О коммерческой тайне»? Дайте определение понятию «коммерческая тайна».
6. Какие виды информации можно отнести к основным объектам служебной тайны?
7. Каким требованиям должна отвечать информация, чтобы считаться профессиональной тайной?
8. Какие отношения регулирует Закон РФ «О государственной тайне»?

Практическое занятие №3 (4 ч.)

Тема Методологические основы защиты информации

Вопросы для обсуждения:

1. Какие методы защиты информации относятся к организационным?
2. Перечислите известные Вам технологические методы защиты информации.
3. Перечислите уровни защиты ИС.
4. Типовые методы защиты информации для различных направлений защиты.
5. Компьютерные вирусы: основные типы, фазы существования.

6. Классификация компьютерных вирусов
7. Организационные меры антивирусной защиты.
8. Типы методов аутентификации
9. Криптографические методы защиты информации. Классификация криптографических алгоритмов.
10. Сетевые технологии защиты.

Практическое занятие №4 (2 ч.)

Тема Угрозы информационной безопасности

Вопросы для обсуждения:

1. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).
2. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
3. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
4. В каких системах на первом месте стоит обеспечение доступности информации?
5. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
6. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.

Практическое занятие №5 (4 ч.)

Тема Построение систем защиты информации

Вопросы для обсуждения:

1. В чем отличие терминов «Несанкционированный доступ» и «Нарушение конфиденциальности информации»?
2. Что понимается под утечкой информации?
3. Каким образом классифицируются каналы утечки информации?
4. Каким образом следует выбирать меры защиты конфиденциальности информации?
5. Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
6. Перечислите основные способы аутентификации. Какой, на Ваш взгляд, является наиболее эффективным?
7. Дайте определение шифра и сформулируйте основные требования к нему.
8. Поясните, что понимается под совершенным шифром.
9. Каким образом государство регулирует использование средств криптозащиты?
10. Каковы способы контроля целостности потока сообщений?
11. Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
12. Как организован обмен документами, заверенными цифровой подписью?
13. В чем отличие и сходство обычной и цифровой подписей?
14. Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
15. Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?
16. Что означает контроль целостности данных на уровне содержания? Приведите примеры.
17. Как обеспечить целостность данных при их хранении?
18. Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
19. Как изменяется надежность аппаратуры с течением времени?
20. Каковы способы повышения надежности аппаратуры и линий связи?

Практическое занятие №6 (4 ч.)

Тема **Нормативно правовое регулирование защиты информации**

Вопросы для обсуждения:

1. Нормативно-правовые документы в области информационной безопасности в РФ.
2. Акты федерального законодательства
3. Методические документы государственных органов России
4. Законе «Об информации, информационных технологиях и о защите информации»
5. Законодательные акты в области защиты информации.
6. Ответственность за нарушения в сфере информационной безопасности
7. Российские и международные стандарты, определяющие требования к защите информации.
8. Цели применения стандартов информационной безопасности.
9. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?
10. Для организаций какой сферы применимы стандарты серии ISO/IEC 27000?
11. Каковы отличительные черты стандартов серии ISO/IEC 27000?
12. Система сертификации РФ в области защиты информации.
13. Основные правила и документы системы сертификации РФ в области защиты информации.

Задания для текущего контроля

№ раздела дисциплины	Наименование практических работ
1.	«Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Виды угроз информационной безопасности Российской Федерации».
2.	«Источники угроз информационной безопасности Российской Федерации. Анализ информационной инфраструктуры государства».
3.	«Методы защиты от компьютерных вирусов» «Криптографические методы защиты. Электронная подпись.»
4.	«Классификация угроз информационной безопасности»
5.	«Построение систем защиты от угрозы нарушения конфиденциальности»
6.	«Обзор международных стандартов информационной безопасности» «Обзор отечественных стандартов информационной безопасности»

Примерные темы самостоятельной работы

1. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
2. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности.
3. Интересы личности, общества и государства в информационной сфере.
4. Угрозы информационной безопасности Российской Федерации.
5. Внешние и внутренние источники угроз информационной безопасности государства.
6. Проблемы региональной информационной безопасности.
7. Информационное оружие, его классификация и возможности.
8. Методы нарушения конфиденциальности, целостности и доступности информации.
9. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
10. Компьютерная система как объект информационной безопасности.
11. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.

12. Анализ современных подходов к построению систем защиты информации.
13. Общая характеристика средств видеонаблюдения и обнаружения оптических приборов.

Примерные темы рефератов:

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Правовая база обеспечения информационной безопасности личности (общества, государства).
3. Виды защищаемой информации.
4. Интересы личности (общества, государства) в информационной сфере.
5. Угрозы информационной безопасности Российской Федерации.
6. Внешние (внутренние) источники угроз информационной безопасности государства.
7. Проблемы региональной информационной безопасности.
8. Информационное оружие, его классификация и возможности.
9. Методы нарушения конфиденциальности (целостности, доступности) информации.
10. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.
11. Компьютерная система как объект информационной безопасности.
12. Обеспечение информационной безопасности компьютерных систем.
13. Классификация и способы нейтрализации вредоносных программ;
14. Инфраструктура открытых ключей;
15. Криптографические способы защиты информации;
16. Защита информации в мобильных устройствах;
17. Источники угроз информационной безопасности РФ;
18. Доктрина информационной безопасности;
19. Виды угроз информационной безопасности Российской Федерации;
20. Понятие информационной безопасности;
21. Основы информационной безопасности;
22. Конфиденциальные документы;
23. Общие методы обеспечения информационной безопасности Российской Федерации;
24. Противодействие техническим каналам утечки информации;
25. Средства защиты информации. Генераторы акустического и электромагнитного шума.

Примерные вопросы к зачету.

1. Национальная безопасность.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.
3. Виды защищаемой информации.
4. Основные понятия и общеметодологические принципы теории информационной безопасности.
5. Роль информационной безопасности в обеспечении национальной безопасности государства.
6. Интересы личности в информационной сфере.
7. Интересы государства в информационной сфере.
8. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.
9. Угрозы информационному обеспечению государственной политики Российской Федерации.
10. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.
11. Угрозы безопасности информационных систем, как уже развернутых, так и создаваемых на территории России.

12. Внешние источники угроз.
13. Внутренние источники угроз.
14. Направления обеспечения информационной безопасности государства.
15. Проблемы региональной информационной безопасности.
16. Субъекты информационного противоборства.
17. Составные части и методы информационного противоборства.
18. Информационное оружие, его классификация и возможности.
19. Методы нарушения конфиденциальности, целостности и доступности информации.
Причины, виды, каналы утечки и искажения информации.
20. Классификация и способы нейтрализации вредоносных программ;
21. Инфраструктура открытых ключей;
22. Криптографические способы защиты информации;
23. Защита информации в мобильных устройствах;
24. Источники угроз информационной безопасности РФ;
25. Доктрина информационной безопасности;
26. Виды угроз информационной безопасности Российской Федерации;
27. Понятие информационной безопасности;
28. Основы информационной безопасности;
29. Конфиденциальные документы;
30. Общие методы обеспечения информационной безопасности Российской Федерации;
31. Противодействие техническим каналам утечки информации;
32. Средства защиты информации.
33. Охарактеризуйте угрозы доступности информации.
34. Основные угрозы целостности информации.
35. Компьютерные вирусы и ИБ.
36. Назовите классификационные признаки и характерные черты компьютерных вирусов.
37. Перечислите виды антивирусных программ.
38. Назовите факторы, которые определяют качество антивирусных программ.
39. Уровни ИБ. Основные задачи и положения, решаемые на каждом уровне.
40. Методы определения требований к защите информации
41. Классификация требований к средствам защиты информации

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.

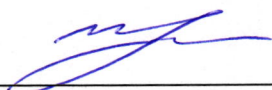
В случае выполнения данных условий, студент имеет возможность сдавать теоретический зачет по вопросам.

Оценка «зачтено» 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.
- 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.
- 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, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания

Составитель _____



Мазур И. К.

«19» марта 2024 г.