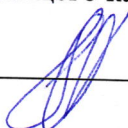


Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сахалинский государственный университет»

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.15 «Организационное и правовое обеспечение 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	<p>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.</p> <p>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.</p> <p>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.</p>
УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	<p>УК-10.1 Знать задачи и направления государственной политики в сфере противодействия коррупции.</p> <p>УК-10.2 Уметь определять содержание полномочий государственных органов в сфере противодействия коррупции, объяснять отрицательное влияние коррупции на общество и воспитывать нетерпимость к коррупции</p> <p>УК-10.3 Иметь необходимые навыки в сфере противодействия коррупции</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-8	Способен осуществлять подбор, изучение и обобщение научно-	ОПК-8.1 - Знает принципы поиска, обработки, обобщения и представления информации для решения задач профессиональной деятельности;

	технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.2 - Умеет работать с источниками информации, базами данных и нормативной документацией при решении профессиональных задач; ОПК-8.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности.
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.	Нормативно-правовая основа концепции ИБ	УК-2; УК-10; ОПК-5; ОПК-8; ОПК-4.1	Задания к практическим работам, контрольные вопросы, вопросы к зачету
2.	Правовое обеспечение информационной безопасности	УК-2; УК-10; ОПК-5; ОПК-8; ОПК-4.1	Задания к практическим работам, контрольные вопросы, вопросы к зачету
3.	Организационное обеспечение информационной безопасности	УК-2; УК-10; ОПК-5; ОПК-8; ОПК-4.1	Задания к практическим работам, контрольные вопросы, вопросы к зачету

### Практическое занятие №1 (10 ч.)

#### Тема Нормативно-правовая основа концепции ИБ

Вопросы для обсуждения:

1. Понятие и цель организационного и правового обеспечения защиты информации
2. Структура организационного и правового обеспечения защиты информации
3. Принципы и методы организационного и правового обеспечения защиты информации

### Практическое занятие №2 (14 ч.)

#### Тема Правовое обеспечение информационной безопасности

Вопросы для обсуждения:

1. Понятие информационной безопасности Российской Федерации
2. Методы обеспечения информационной безопасности Российской Федерации
3. Организация обеспечения информационной безопасности Российской Федерации
4. Классификация информации по возможности доступа
5. Классификация информации с точки зрения возможности распространения

6. Законодательство об электронной цифровой подписи
7. Стандарты и Технические регламенты

### Практическое занятие №3 (12 ч.)

#### Тема **Организационное обеспечение информационной безопасности**

*Вопросы для обсуждения:*

1. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти
2. Организационные структуры системы обеспечения информационной безопасности предприятия (организации)
3. Нормативные требования к составу и содержанию системы организационного обеспечения информационной безопасности
4. Корпоративное нормативное регулирование
5. Организация объектовых режимов безопасности
6. Управление персоналом на предприятиях и в организациях

#### Задания для текущего контроля

№ раздела дисципли ны	Наименование практических работ
1.	«Введение в правовые и организационные основы обеспечения информационной безопасности» «Правовые и организационные основы защиты охраняемой законом тайны» «Правовой режим коммерческой тайны» «Организационные и правовые основы обеспечения безопасности персональных данных» «Юридическая, административная, дисциплинарная, уголовная ответственность за правонарушения в сфере информационной безопасности»
2.	«Правовые основы информационной безопасности Российской Федерации» «Особенности организационно-правового обеспечения процессов создания автоматизированных систем» «Практика разработки и реализации политики информационной безопасности корпоративных информационных систем» «Правовое регулирование распространения информации и доступа к информации» «Особенности правового регулирования общественных отношений при использовании современных технических средств обработки информации и при разработке шифровальных средств» «Законодательство о техническом регулировании» «Правовые основы защиты компьютерной информации»
3.	«Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти» «Организационные структуры системы обеспечения информационной безопасности предприятия (организации)» «Нормативные требования к составу и содержанию системы организационного обеспечения информационной безопасности». «Корпоративное нормативное регулирование» «Организация объектовых режимов безопасности»

### **Примерные темы самостоятельной работы**

1. Понятие коммерческой тайны
2. Правовой режим коммерческой тайны
3. Понятие служебной тайны
4. Особенности защиты профессиональной тайны
5. Уголовная ответственность за разглашение государственной тайны
6. Уголовная ответственность за разглашение коммерческой, налоговой и банковской тайны
7. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
8. Гражданская и дисциплинарная ответственность за разглашение коммерческой тайны, банковской тайны, за нарушение правового режима ноу-хау
9. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
10. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи
11. Конституционные гарантии прав граждан на информацию
12. Структура государственной системы правового регулирования информационной безопасности в Российской Федерации
13. Корпоративная нормативная база по защите информации. Политика безопасности.
14. Организация пропускного режима.

### **Примерные темы рефератов:**

1. Понятие служебной тайны в российском законодательстве.
2. Виды различных тайн в российском законодательстве (адвокатская, медицинская, личная, следствия, переговоров, переписки и т. д.).
3. Коммерческая тайна как разновидность способов защиты информации.
4. Ноу-хау - вид защищаемой информации в российском праве.
5. Конституция РФ как правовая основа защиты информации.
6. Гражданский кодекс РФ как правовая основа защиты информации.
7. Федеральный закон «О персональных данных» как правовая основа защиты информации.
8. Правовые основы защиты личной тайны в России.
9. Конституция РФ как основа закрепления прав на личную тайну.
10. Защита персональных данных: право или обязанность?
11. Виды защищаемых персональных данных.
12. Процесс восстановления нарушенных прав на различные виды тайн и персональные данные.
13. Уголовно-правовая политика России в области защиты информации на современном этапе.
14. Виды гражданско-правовых и дисциплинарных норм, применяемых при наступлении ответственности за разглашение защищаемой информации
15. Административная ответственность за разглашение защищаемой информации.
16. Виды административных норм в российском административном праве, устанавливающих ответственность за разглашение защищаемой информации.
17. Правовое регулирование отношений, связанных с доступом к персональным данным и их обработкой
18. Основные положения концепции и программы правовой информатизации как инструмента правового регулирования информационной безопасности личности, общества, государства
19. Организация внутри объектового режима.
20. Порядок проведения служебных расследований

## 21. Управление персоналом на предприятиях и в организациях

### Примерные вопросы к зачету.

1. Государственная система защиты информации в РФ от иностранных технических разведок и от ее утечки по техническим каналам.
2. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа.
3. Оценка соответствия объектов информатизации требованиям безопасности информации.
4. Классификация автоматизированных систем и требования по защите информации.
5. Организационные средства защиты информации. Место организационных средств в систем комплексной защиты информации объектов информатизации.
6. Классификация и основное содержание направлений организационной деятельности по обеспечению информационной безопасностью
7. Архитектура систем защиты информации. Классификация требований к СЗИ. Принципы построения систем защиты.
8. Служба защиты информации. Нормативная база создания служб защиты информации.
9. Принципы организации службы. Основные задачи службы.
10. Функции службы защиты информации. Порядок взаимодействия службы защиты информации с другими структурными подразделениями объекта.
11. Общее содержание организации и обеспечения работ по защите информации.
12. Основные мероприятия по подготовке лиц, ответственных за обеспечение информационной безопасности.
13. Управление процессами функционирования систем защиты информации.
14. Организационное и документальное обеспечение работ по защите информации.
15. Основное назначение документационного обеспечения информационной безопасности. Структура и состав системы документационного обеспечения защиты информации.
16. Организация пропускного и внутриобъектового режима. Понятие "пропускной режим".
17. Основные мероприятия по обеспечению пропускного режима на объекте.
18. Средства технического контроля и управления доступом.
19. Понятия государственной, профессиональной, служебной тайны.
20. Конфиденциальная информация. Признаки информации, составляющей коммерческую тайну.
21. Понятие политики информационной безопасности, принципы разработки и внедрения эффективных политик.
22. Организация и поддержание конфиденциального документооборота.
23. Программные, аппаратные и организационные средства его обеспечения.
24. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации.
25. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта.
26. Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне.
27. Требования к помещениям и хранилищам, в которых ведутся закрытые работы.
28. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей.
29. Защита информации в экстремальных ситуациях. Дайте определение понятию «информация».
30. Перечислите виды охраноспособной информации.
31. Опишите методы охраны информации.
32. Обоснуйте необходимость защиты информации.
33. Объясните, в чём разница между охраной и защитой информации.
34. Каковы существенные особенности информации?
35. Чем вызвана необходимость правового регулирования в информационной сфере?
36. Приведите пример правовой охраны информации.
37. Составьте перечень известных вам нормативных актов, посвящённых охране информации.

38. Каково назначение коммерческой тайны?
39. Чем вызвана необходимость защиты служебной тайны?
40. Оцените надёжность защиты при помощи права различных видов тайн.
41. Перечислите виды защищаемых персональных данных
42. В чём заключается сущность правовой защиты различных видов тайн?
43. Оцените надёжность правовой защиты различных видов тайн.
44. Укажите принципиальные различия между различными видами тайн и персональными данными.
45. Сравните различные виды персональных данных с точки зрения правовой защиты.
46. Дайте характеристику уголовно-правовым способам борьбы с разглашением защищаемой информации.
47. От чего зависит применение уголовно-правовых норм в борьбе с разглашением защищаемой информации?
48. Дайте характеристику гражданско-правовому способу защиты охраняемой информации.
49. Перечислите виды гражданско-правовых норм, направленных на защиту охраняемой информации.
50. Дайте определение понятию «разглашение защищаемой информации».
51. Перечислите виды разглашаемой информации.
52. Обоснуйте значение административно-правовых способов борьбы с разглашением защищаемой информации.
53. Какие положения, связанные с вопросами обработки информации, закреплены в Конституции Российской Федерации?
54. Какие виды информации обязательно требуется защищать в соответствии с законодательством Российской Федерации?
55. К какой информации не может быть ограничен доступ?
56. Какую ответственность может повлечь нарушение требований Федеральных законов?

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
<b>Итого за семестр</b>			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.