Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных»

УТВЕРЖДЕНА:
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

Рабочая программа дисциплины

«АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление: 10.03.01 Информационная безопасность

Организация и технологии защиты информации (в сфере техники и технологии)

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Мамедов Эльшан Фахраддинович Дата подписания: 17.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 17.06.2025	Документ подписан простой электронной подписью Согласовал: Сибиряк Юрий Владимирович Дата подписания: 10.06.2025

Год набора – 2025

Иркутск, 2025 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Аудит информационной безопасности» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК ОС-2.2.1
ОПК ОС-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК ОС-2.4.2
ОПК ОС-7 Способен проводить аудит безопасности информационных систем, а также защищенность объекта информатизации в соответствии с нормативными документами регулятора	ОПК ОС-7.3

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-7.3	Знает комплекс организационно-технических мероприятий, проводимых независимыми экспертами, имеющих целью оценку состояния ИБ объекта аудита и степени его соответствия критериям аудита ИБ	**Знать** теоретические основы построения и функционирования информационных систем аудита; основные стандарты, регламентирующие управление качеством информационной безопасности; организационно-правовую документацию предприятий (устав, положение о предприятии), работающих в сфере защиты информации; основные методы и технологию управления службой защиты информации; организацию аудита информационной безопасности информационной системы; методологию оценки информационных рисков объектов информатизации. **Уметь** применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; применять отечественные и зарубежные стандарты для проектирования,

		разработки и оценки защищенности объектов; реализовывать системы защиты информации в соответствии со стандартами по оценке защищенных систем. **Владеть** навыками работы с нормативными правовыми актами; методами обработки результатов анализа данных аудита и содержащие оценку уровней защищенности объекта информатизации или соответствие ее требованиям стандартов; навыками определения наиболее вероятных угроз безопасности в отношении ресурсов ис и уязвимостей защиты, делающих возможным осуществление этих угроз; методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации; методами и средствами выявления угроз безопасности объекту информатизации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
ОПК ОС-2.2.1	Использует актуальные профессиональные знания и ключевые инструменты, которые позволяют оценить реальную защищенность активов (в том числе ИТ-активов) функциональных процессов объекта защиты. Результаты аудита позволяют создать/улучшить существующую систему ИБ с целью повышения устойчивости к деструктивным воздействиям	**Знать** организационные меры по защите информации, основные методы управления защитой информации **Уметь** разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации **Владеть** навыками выработки рекомендаций для решения о модернизации системы защиты информации
ОПК ОС-2.4.2	Способен проводить аудит защищенности объекта информатизации; знает способы защиты технических средств обработки информации от	**Знать** критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы

	утечки по техническим каналам, методы и средства нормативного контроля, а также соответствия критериям аудита с учетом заданных требований	измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации **Уметь** осуществлять контроль обеспечения уровня защищенности объектов информатизации; применять методы и средства нормативного контроля **Владеть** навыками оценки защищенности объектов информатизации с помощью типовых программных средств; навыками работы с нормативными и руководящими документами в сфере аудита защищенности объекта информатизации

2 Место дисциплины в структуре ООП

Изучение дисциплины «Аудит информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Информационные технологии», «Основы информационной безопасности»

Дисциплина является предшествующей для дисциплин/практик: «Информационно-психологическая безопасность в современном обществе», «Организационное и правовое обеспечение информационной безопасности», «Персональные данные», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Нормативная база, российские и международные стандарты по информационной безопасности», «Основы управления информационной безопасностью»

3 Объем дисциплины

Объем дисциплины составляет – 4 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 3
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	64	64
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	32	32
Самостоятельная работа (в т.ч. курсовое проектирование)	44	44
Трудоемкость промежуточной аттестации	36	36

Вид промежуточной аттестации (итогового контроля по дисциплине)	Экзамен	Экзамен

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 3

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Общие положения теории информационной безопасности	1	4			1	2	1	4	Устный опрос
2	Понятие аудита информационной безопасности	2	4			2	4	1	4	Устный опрос
3	Анализ и управление рисками информационной безопасности	3	4			3	2	1	8	Устный опрос
4	Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	4	8			4	8	1	12	Устный опрос
5	Методика проведения аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	5	4			5	8	1	10	Устный опрос
6	Лицензирование и сертификация деятельности в области защиты	6	8			6	8	1	6	Устный опрос

	информации									
	Промежуточная аттестация								36	Экзамен
	Всего		32				32		80	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 3

№	Тема	Краткое содержание
1	Общие положения теории информационной безопасности	Основные положения, понятия и определения теории информационной безопасности.
2	Понятие аудита информационной безопасности	Понятие аудита безопасности. Методы анализа данных при аудите информационной безопасности.
3	Анализ и управление рисками информационной безопасности	Анализ информационных рисков предприятия. Методы оценивания информационных рисков предприятия. Управление информационными рисками.
4	Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	Действующая в Российской Федерации система нормативно-правовых документов в области информационной безопасности. Основные федеральные законы и постановления Правительства Российской Федерации, регулирующие вопросы информационной безопасности. Руководящие и нормативно-методические документы в сфере информационной безопасности. Государственные стандарты Российской Федерации в сфере обеспечения информационной безопасности.
5	Методика проведения аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	Планирование и организация работ по аудиту информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации.
6	Лицензирование и сертификация деятельности в области защиты информации	Правовая основа системы лицензирования, сертификации и аттестации объектов информатизации в Российской Федерации. Лицензирование деятельности по защите информации. Сертификация средств защиты информации.

4**.3 Перечень лабораторных работ**

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 3

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Основные положения, понятия и определения теории информационной безопасности	2
2	Аудит безопасности и методы его проведения	4
3	Анализ рисков в области защиты информации	2
4	Обзор стандартов информационной безопасности, применяемых в органах власти	8
5	Использование правовых и методологических основ аудита информационной безопасности	8
6	Органы, уполномоченные на ведение лицензионной деятельности в сфере информационной безопасности	8

4.5 Самостоятельная работа

Семестр № 3

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям (лабораторным работам)	44

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия, Кейс-технология

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/course/index.php?categoryid=1107

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/course/index.php?categoryid=1107

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 3 | Устный опрос

Описание процедуры.

Описание процедуры:
Проведение устного опроса в форме «вопрос-ответ».

Вопросы для контроля:
Раздел № 4 Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации.
1. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения».
2. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
3. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Критерии оценивания.

Полнота ответа: Раскрытие всех аспектов вопроса, использование ключевых понятий, терминов.
Точность и достоверность: Правильность определений, формул, фактов, дат, имен, ссылок на источники.
Глубина понимания: Демонстрация понимания сути явлений, причинно-следственных связей, умение анализировать, синтезировать, обобщать, а не просто воспроизводить заученное.
Логичность и структурированность: Последовательность изложения, наличие введения, основной части, вывода.
Культура речи: Грамотность, ясность, использование профессиональной терминологии.
Умение аргументировать: Подтверждение своих тезисов примерами, доказательствами, ссылками на теории.
Ответы на дополнительные/уточняющие вопросы: Способность развить тему, применить знания в нестандартной ситуации.

ответ раскрыт полностью – 5 баллов
ответ раскрыт частично – 2-4 баллов
имеет только общее представление о проблеме – 1 балл
не ответил – 0 баллов

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	**Критерии оценивания**	**Средства (методы) оценивания промежуточной аттестации**
ОПК ОС-7.3	Демонстрирует высокий уровень знаний о сущности процесса аудита в области информационной безопасности.	Устное собеседование по теоретическим вопросам и/или выполнение

		практических заданий.
ОПК ОС-2.2.1	Демонстрирует высокий уровень знаний, позволяющих оценить реальную защищенность активов (в том числе ИТ-активов) функциональных процессов объекта защиты.	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий.
ОПК ОС-2.4.2	Демонстрирует высокий уровень знаний в сфере проведения аудита защищенности объекта информатизации	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 3, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

Перечень теоретических вопросов, практических заданий и ситуаций, выносимых на экзамен, доводятся преподавателем до студентов в начале изучения программы. Формулировки вопросов, заданий должны быть четкими, краткими, понятными, исключающими двойное толкование. Могут быть применены тестовые задания или задания комбинированного характера. Количество вариантов для устных заданий должно быть больше чем число студентов, сдающих экзамен не менее, чем на 3. Количество вариантов для письменных заданий должно быть не менее двух.

Теоретические вопросы к экзамену

1. Сущность конституционного права на информацию.
2. Гарантия права на информацию.
3. Понятие защиты информации.
4. Законодательство Российской Федерации о защите информации.
5. Понятие информации. Её виды.
6. Понятие правового режима информации, его виды.
7. Правовой режим свободного доступа к информации.
8. Понятие и общая характеристика информации ограниченного доступа.
9. Режим конфиденциальной информации.
10. Правовое регулирование и защита государственной тайны.
11. Понятие государственной тайны и принципы засекречивания информации.
12. Перечень сведений, составляющих государственную тайну.
13. Порядок засекречивания сведений и их носителей. Степени секретности сведений, грифы секретности и формы допуска граждан к государственной тайне.
14. Что такое комплексная система защиты информации?
15. Что относится к конфиденциальной информации и государственной тайне?
16. Какие виды защиты информации реализованы с помощью отдельных взаимосвязанных элементов, представленных в виде структурно-типовой системы защиты

информации?
17. Что такое информационная безопасность?
18. Какие компоненты входят в систему информационной безопасности?
19. Какие виды угроз информационной безопасности встречаются наиболее часто?
20. Приведите примеры источников угроз информации.
21. Что из себя представляет концептуальная модель информационной безопасности?
22. Каковы возможные пути утраты информации? Приведите конкретные примеры.
23. Перечислите основные направления защиты информации и дайте характеристику каждого из них.
24. Назовите основные цели проведения аудита информационной безопасности.
25. Перечислите основные виды аудита информационной безопасности.
26. Какова последовательность действий при проведении аудита информационной безопасности?
27. Опишите концептуальную модель аудита информационной безопасности.
28. Чем определяются масштабы аудита информационной безопасности?
29. С какой целью проводится анализ рисков?
30. Назовите задачи, решаемые при анализе рисков.
31. Как может быть оценена величина риска?
32. В чем заключается задача управления рисками?
33. Какова структура нормативно-правовой базы Российской Федерации в сфере информационной безопасности?
34. Опишите основные типы документов, входящие в нормативно-правовую базу Российской Федерации в сфере информационной безопасности.
35. Назовите основные федеральные законы и постановления Правительства Российской Федерации, регулирующие вопросы информационной безопасности. Охарактеризуйте их содержание.
36. К каким видам информации, согласно законодательству Российской Федерации, не может быть ограничен доступ?
37. На выполнение каких требований направлена защита информации?
38. Что относится к персональным данным?
39. Что такое электронная цифровая подпись? Для чего она нужна и при соблюдении каких условий она действительна?
40. Что относится и что не относится к служебной информации ограниченного распространения?
41. Назовите основные руководящие и нормативно-методические документы в сфере информационной безопасности. Охарактеризуйте их содержание.
42. Что понимается под аттестацией объектов информатизации?
43. Что понимается под сертификацией средств защиты информации по требованиям безопасности информации?
44. Какие существуют направления в проблеме защиты информации от несанкционированного доступа? В чем их сходство и различие?
45. Сколько установлено классов защищенности средств вычислительной техники от несанкционированного доступа к информации?
46. Сколько установлено классов защищенности автоматизированных систем от несанкционированного доступа к информации? На какие группы делятся эти классы?
47. Каковы основные вопросы защиты информации?
48. Назовите основные государственные стандарты Российской Федерации в сфере информационной безопасности. Охарактеризуйте их содержание.
49. Что является целями работ по аудиту состояния информационной безопасности автоматизированных систем исполнительных органов государственной власти и органов местного самоуправления субъектов России?

50. Что относится к внешнему и внутреннему аудиту информационной безопасности?
51. Каковы основные этапы планирования аудита информационной безопасности?
52. Какие существуют практические подходы к анализу и оценке текущего состояния информационной безопасности организации?
53. Каким требованиям по информационной безопасности должна отвечать система защиты информации?
54. Какие функции, согласно ФЗ «О государственной тайне», выполняют органы исполнительной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий?
55. Каковы основные понятия и определения в сфере лицензирования, сертификации и аттестации объектов информатизации в Российской Федерации?
56. Что является законодательной и нормативной базой лицензирования и сертификации в области защиты государственной тайны?
57. Какие виды деятельности подлежат лицензированию?
58. Что понимается под аттестацией объектов информатизации?
59. Какие объекты информатизации подлежат обязательной аттестации?

Пример задания:

Сущность права на информацию.
Перечислите основные направления защиты информации и дайте характеристику каждого из них.
Характеристика внешнего и внутреннего аудита информационной безопасности.

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
ответ правильный, логически выстроен, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	ответ в целом правильный, логически выстроен, использована профессиональная терминология. Обучающийся в целом правильно интерпретирует полученный результат.	ответ в основном правильный, логически выстроен, использована профессиональная терминология.	ответы на теоретическую часть неправильные или неполные.

7 **Основная учебная литература**

1. Прохорова О. В. Информационная безопасность и защита информации / О. В. Прохорова, 2023. - 124.

2. Организационное и правовое обеспечение информационной безопасности : учебник для бакалавриата и магистратуры / Т. А. Полякова [и др.]; ред.: Т. А. Полякова, А. А. Стрельцов, 2024. - 357.

3. Петренко В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / / В. И. Петренко, И. В. Мандрица, 2024. - 108.

8 Дополнительная учебная литература и справочная

1. Усов Е. Г. Защита информации : электронный курс / Е. Г. Усов, 2023

2. Вавилин Я. А. Информационные технологии в управлении качеством и защита информации : учебное пособие для вузов / Я. А. Вавилин, В. Г. Солдатов, И. Г. Манкевич, 2025. - 196.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Microsoft DreamSpark Premium Electronic Software Delivery_2018

2. Microsoft Office 2007 Standard - 2003 Suites и 2007 Suites - поставка 2010

12 Материально-техническое обеспечение дисциплины

1. Проектор мультимедиа BenQ MW621ST(с экраном 3*3 м)

2. Экран ScreenMedia GoldView 274*206 настенный