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

«ЗАЩИТА ИНФОРМАЦИИ»

Направление: 09.03.01 Информатика и вычислительная техника

Интеллектуальные системы обработки информации и управления

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Кононенко Роман Владимирович Дата подписания: 18.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 19.06.2025	Документ подписан простой электронной подписью Согласовал: Кононенко Роман Владимирович Дата подписания: 18.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Защита информации» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-10 Способность применять методы и средства защиты информации	ОПК ОС-10.2
ОПК ОС-3 Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК ОС-3.3
ОПК ОС-6 Способность разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием	ОПК ОС-6.4

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-10.2	Способность осваивать и использовать программное обеспечение для решения практических задач информационной безопасности и защиты информации	**Знать** существующие программные средства прикладного решения профессиональных задач; способы применения программных средств; системы, средства и технологии обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами федеральной службы безопасности рф, федеральной службой по техническому и экспортному контролю рф; криптографические методы в современных цифровых технологиях. **Уметь** организовывать работу по использованию средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами. **Владеть** навыками работы в программной системе прикладного назначения, способностями

		овладевать новыми интегрированными системами разработки
ОПК ОС-3.3	Способность использовать информационно-коммуникационные технологии, информационную и библиографическую культуру с учетом требований информационной безопасности для решения практических задач теории автоматов	**Знать** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Уметь** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Владеть** навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК ОС-6.4	Разработка планов и технического задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием с учетом информационной безопасности	**Знать** методику разработки организационно-распорядительных документов, бизнес-планов в сфере информационной безопасности, в том числе при проведении бенчмаркинга сэд; стандарты оформления организационно-распорядительных документов; сертифицированные продукты защиты информации **Уметь** разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности; использовать техническую и эксплуатационную документацию на системы и средства обеспечения информационной безопасности; использовать сертифицированные продукты защиты информации **Владеть** навыками разработки технической и эксплуатационной документации на системы и средства обеспечения

		информационной безопасности; навыками разработки проектов организационно-распорядительных документов, бизнес-планов сэд в сфере профессиональной деятельности; навыками проведения бенчмаркинга информационной безопасности; методиками построения защиты информации на предприятиях.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Защита информации» базируется на результатах освоения следующих дисциплин/практик: «Программирование», «Информатика», «Базы данных», «Методы программирования», «Правоведение»

Дисциплина является предшествующей для дисциплин/практик: «Системы искусственного интеллекта», «Авторское право», «Защита интеллектуальной собственности», «Коммерциализация результатов интеллектуальной деятельности»

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 № 6
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	64	64
лекции	32	32
лабораторные работы	32	32
практические/семинарские занятия	0	0
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 № 6

№ 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	Понятие и сущность	1	4	1	4					Тест

	информационной безопасности и защиты информации									
2	Основные угрозы информационной безопасности	2	4	2	4					Тест
3	Нормативно-правовая база информационной безопасности	3	4	3	2					Тест
4	Административный уровень обеспечения информационной безопасности	4	4	4	2					Тест
5	Процедурный уровень информационной безопасности	5	4	5, 6, 7	6					Тест
6	Система защиты информации	6	4	8	2					Тест
7	Обеспечение режима конфиденциальности при работе с защищаемой информацией	7	4	9, 10	6					Тест
8	Контроль за соблюдением требований информационной безопасности и защиты информации	8	2	11	2					Тест
9	Ответственность за правонарушения информационной безопасности и защиты информации	9	2	12	4			1	44	Тест
	Промежуточная аттестация								36	Экзамен
	Всего		32		32				80	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 6

№	Тема	Краткое содержание
1	Понятие и сущность информационной безопасности и защиты информации	Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности и защиты информации. Основные компоненты безопасности государства. Связь информационной безопасности с информатизацией общества. Базовые уровни обеспечения информационной безопасности и защиты информации.

2	Основные угрозы информационной безопасности	Классификация угроз безопасности информационной безопасности. Особенности угроз воздействия на объект атаки. Основные методы и каналы несанкционированного доступа к информации в информационной системе. Базовые принципы защиты от несанкционированного доступа к информации в соответствии с законодательством Российской Федерации. Задачи по защите информационной системы от реализации угроз. Риски угроз информационным ресурсам.
3	Нормативно-правовая база информационной безопасности	Российское и международное законодательство в сфере информационной безопасности и защите информации. Правовое регулирование защиты сведений, составляющих государственную и иные виды тайн. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Состав и назначение должностных инструкций организации. Порядок создания, утверждения и исполнения должностных инструкций организации.
4	Административный уровень обеспечения информационной безопасности	Концепция информационной безопасности, её цели и этапы построения. Политика информационной безопасности как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки политики информационной безопасности. Задачи, решаемые при анализе рисков. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки политики информационной безопасности и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации политики информационной безопасности.
5	Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.
6	Система защиты информации	Процесс развития средств и методов защиты информации. Этапы развития системы защиты информации в настоящее время. Комплексный подход к построению системы защиты информации. Цели и задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации.

		Методы (виды) обеспечения защиты информации
7	Обеспечение режима конфиденциальности при работе с защищаемой информацией	Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных. Допуск должностных лиц, работников к конфиденциальной информации. Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных. Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну. Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям.
8	Контроль за соблюдением требований информационной безопасности и защиты информации	Основные положения по осуществлению контроля, назначение, цель и задачи контроля. Основные мероприятия по осуществлению контроля. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа. Проведение служебного расследования по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений режима конфиденциальности.
9	Ответственность за правонарушения информационной безопасности и защиты информации	Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области защиты государственной тайны. Уголовная ответственность за правонарушения в области конфиденциальной информации.

4.3 Перечень лабораторных работ

Семестр № 6

№	Наименование лабораторной работы	Кол-во академических часов
1	Понятие и сущность информационной безопасности и защиты информации	4
2	Основные угрозы информационной безопасности	4
3	Российское и международное законодательство в сфере информационной безопасности и защите информации	2
4	Стандарты и нормативно-методические документы в области обеспечения	2

	информационной безопасности	
5	Государственная система обеспечения информационной безопасности	2
6	Административный уровень обеспечения информационной безопасности	2
7	Процедурный уровень информационной безопасности	2
8	Система защиты информации	2
9	Этапы и порядок проведения работ по созданию системы защиты информации	4
10	Обеспечение режима конфиденциальности при работе с защищаемой информацией	2
11	Допуск должностных лиц, работников к конфиденциальной информации	2
12	Контроль за соблюдением требований информационной безопасности и защиты информации	4

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Семестр № 6

№	Вид СРС	Кол-во академических часов
1	Тест (СРС)	44

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Онлайн квиз по темам, вебинар

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по лабораторным работам:

Находятся на электронном образовательном ресурсе el.istu.edu

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Находятся на электронном образовательном ресурсе el.istu.edu

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 6 | Тест

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

Критерии оценивания.

Демонстрирует способность осваивать и использовать программное обеспечение для решения практических задач информационной безопасности и защиты информации

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-10.2	Демонстрирует высокий уровень знаний в сфере использования программного обеспечения для решения практических задач информационной безопасности и защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности РФ, Федеральной службой по техническому и экспортному контролю РФ.	выполнение индивидуального задания и практических работ
ОПК ОС-3.3	Демонстрирует базовый уровень знаний в сфере использования информационно-коммуникационных технологий, информационной и библиографической культуры с учетом требований информационной безопасности.	выполнение индивидуального задания и практических работ
ОПК ОС-6.4	Демонстрирует высокий уровень знаний в сфере разработки планов и технического задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием с учетом информационной безопасности	выполнение индивидуального задания и практических работ

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 6, 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

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	76 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Обучающийся в целом правильно интерпретирует полученный результат.	75-61 – ответ в основном правильный, логически выстроен, использована профессиональная терминология.	менее 60 – ответы на теоретическую часть неправильные или неполные.

7 Основная учебная литература

1. Петренко В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица, 2021. - 108.

2. Петренко В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие / В. И. Петренко, И. В. Мандрица, 2022. - 108.

8 Дополнительная учебная литература и справочная

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

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. Свободно распространяемое программное обеспечение Microsoft Windows (Подписка DreamSpark Premium Electronic Software Delivery (3 years). Сублицензионный договор №14527/MOC2957 от 18.08.16г.)

12 Материально-техническое обеспечение дисциплины

1. Компьютер "Intel Core i3/DDR 4Gb/HDD 1Tb/GF 1Gb/LCD23' /ИБП"

2. Компьютер "Intel Core i3/DDR 4Gb/HDD 1Tb/GF 1Gb/LCD23' /ИБП"

3. Компьютер "Intel Core i3/DDR 4Gb/HDD 1Tb/GF 1Gb/LCD23' /ИБП"

4. Компьютер "Intel Core i3/DDR 4Gb/HDD 1Tb/GF 1Gb/LCD23' /ИБП"