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 (121)»

УТВЕРЖДЕНА:
на заседании совета института ИТиАД им. Е.И. Попова
Протокол №8 от 16 февраля 2026 г.

Рабочая программа дисциплины

«ЗАЩИТА ИНФОРМАЦИИ»

Направление: 09.03.01 Информатика и вычислительная техника

Автоматизированные системы обработки информации и управления

Квалификация: Бакалавр

Форма обучения: заочная

Документ подписан простой электронной подписью Составитель программы: Кононенко Роман Владимирович Дата подписания: 31.05.2026	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 10.06.2026	Документ подписан простой электронной подписью Согласовал: Кононенко Роман Владимирович Дата подписания: 05.06.2026

Год набора – 2026

Иркутск, 2026 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	Способен осваивать и использовать программное обеспечение для решения практических задач информационной безопасности и защиты информации	**Знать** Основы информационной безопасности и защиты информации **Уметь** Обеспечить сохранность данных на персональной компьютере от стороннего доступа **Владеть** Инструментами настройки безопасности доступа к данный в операционной системе
ОПК ОС-3.3	Способность использовать нормативные правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; умеет оценить информационные риски в автоматизированных системах и определять меры, правила, процедуры, методы и средства для защиты информации	**Знать** **Уметь** **Владеть**
ОПК ОС-6.4	Разрабатывает планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием с учетом информационной безопасности	**Знать** **Уметь** **Владеть**

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», «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	Учебный год № 3
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	16	16
лекции	8	8
лабораторные работы	8	8
практические/семинарские занятия	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	119	119
Трудоемкость промежуточной аттестации	9	9
Вид промежуточной аттестации (итогового контроля по дисциплине)	Экзамен	Экзамен

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Учебный год № 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
2	Основные угрозы информационной безопасности. Нормативно-правовая база информационной безопасности	2	4	1	4			1	119	Тест
2	Административный уровень обеспечения информационной безопасности	3	4	1	4					Тест
	Промежуточная								9	Экзамен

	аттестация									
	Всего		8		8				128	

4.2 **Краткое содержание разделов и тем занятий**

Учебный год № 3

№	Тема	Краткое содержание
2	Основные угрозы информационной безопасности. Нормативно- правовая база 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. 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.
2	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.

4**.3 Перечень лабораторных работ**

Учебный год № 3

№	Наименование лабораторной работы	Кол-во академических

		часов
1	Основные угрозы информационной безопасности	4
1	Административный уровень обеспечения информационной безопасности	4

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Учебный год № 3

№	Вид СРС	Кол-во академических часов
1	Подготовка к зачёту	119

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: онлайн квиз по каждой теме, 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 учебный год 3 | Тест

Описание процедуры.

онлайн тест

Критерии оценивания.

Более 50% верных ответов

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	Настраивать права доступа на ОС	Практическое задание
ОПК ОС-3.3		
ОПК ОС-6.4		

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Учебный год 3, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

Экзамен превосходит в форме устного ответа на билеты

Пример задания:

1. Методы кодирования дискретной информации
2. Методы кодирования непрерывной информации
3. Понятие и сущность информационной безопасности
4. Обобщенный канал передачи-хранения информации
5. Подстановочное криптирование
6. Перестановочное криптирование
7. Криптирование гаммированием
8. Код Фано
9. Код Хаффмена
10. Избыточные коды
11. Код Хемминга
12. Расширенный код Хемминга
13. Основные угрозы информационной безопасности
14. Порождающая матрица кода
15. Проверочная матрица кода
16. Основные принципы защиты информации
17. Циклические коды
18. Циклическое умножение многочленов
19. Циклическое деление многочленов
20. Циклические кодеры
21. Циклические декодеры
22. Случайные и псевдослучайные последовательности
23. Генерирование длинных псевдослучайных последовательностей
24. Квитирование пакетов данных
25. CRC-8
26. CRC-16
27. Блочное шифрование
28. Требования к алгоритмам шифрования
29. Алгоритм шифрования DES
30. Структура DES в режиме CBC
31. Структура DES в режиме CFB
32. Цифровая подпись
33. Алгоритм генерирования ключевых последовательностей для DES

34. Организация защиты коммерческой информации
35. Российское и международное законодательство в сфере информационной безопасности и защите информации
36. Методы защиты информации
37. Средства защиты информации
38. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности
39. Методы хеширования данных
40. Администрирование ключей
41. Методы идентификации пользователей
42. Методы аутентификации
43. Государственная система обеспечения информационной безопасности
44. Административный уровень обеспечения информационной безопасности
45. Процедурный уровень информационной безопасности
46. Система защиты информации
47. Этапы и порядок проведения работ по созданию системы защиты информации
48. Обеспечение режима конфиденциальности при работе с защищаемой информацией
49. Допуск должностных лиц, работников к конфиденциальной информации
50. Контроль за соблюдением требований информационной безопасности и защиты информации
51. Чиповые пластиковые карты
52. Сенсорные пластиковые карты
53. Бесконтактные пластиковые карты
54. Организация защиты информации в информационных сетях
55. Классификация вирусов

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.

[Сайт] – URL: https://e.lanbook.com/book/149364

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

[Сайт] – URL: https://e.lanbook.com/book/264242

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.

[Сайт] – URL: https://e.lanbook.com/book/392402

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"