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

«ОСНОВЫ 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: Маринов Александр Андреевич Дата подписания: 17.06.2026	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 18.06.2026	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 18.06.2026

Год набора – 2026

Иркутск, 2026 г.

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

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

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-6 Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ОПК ОС-6.1
ОПК ОС-7 Способен проводить аудит безопасности информационных систем, а также защищенность объекта информатизации в соответствии с нормативными документами регулятора	ОПК ОС-7.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-6.1	Знает основной перечень требований защиты информации при этапах проведения аудита, и краткое изложение процесса аудита ИБ	**Знать** основные составляющие информационной безопасности; объекты защиты; категории и носители информации **Уметь** определять средства защиты информации **Владеть** способами передачи конфиденциальной информации на расстоянии
ОПК ОС-7.1	Знает основы защиты информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений	**Знать** основные составляющие информационной безопасности; объекты защиты; категории и носители информации **Уметь** определять средства защиты информации **Владеть** способами передачи конфиденциальной информации на расстоянии

2 Место дисциплины в структуре ООП

Изучение дисциплины «Основы информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: Нет

Дисциплина является предшествующей для дисциплин/практик: «Аудит информационной безопасности», «Методы и средства криптографической защиты информации», «Техническая защита информации»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	Трудоемкость в академических часах (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 1
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	32	32
лекции	16	16
лабораторные работы	0	0
практические/семинарские занятия	16	16
Самостоятельная работа (в т.ч. курсовое проектирование)	40	40
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 № 1

№ 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	Теория информационной безопасности	1	2			1, 2, 3, 4	8	1	6	Устный опрос
2	Методология защиты информации	2	3			5	2	1	7	Устный опрос
3	Организационные основы и методологические принципы защиты информации	3	3			6, 8	4	1	7	Устный опрос
4	Классификация конфиденциальной информации	4	3					1	7	Устный опрос
5	Объекты защиты информации	5	3			7	2	1	7	Устный опрос
6	Классификация видов, методов и средств защиты информации	6	2					1	6	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		16				16		76	

4.2 Краткое содержание разделов и тем занятий

Семестр № 1

№	Тема	Краткое содержание
1	Теория информационной безопасности	Сущность и понятие информационной безопасности. Значение информационной безопасности и ее место в системе национальной безопасности. Современная Доктрина информационной безопасности Российской Федерации.
2	Методология защиты информации	Сущность и понятие защиты информации. Цели и значение защиты информации. Теоретические и концептуальные основы защиты информации.
3	Организационные основы и методологические принципы защиты информации	Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация носителей защищаемой информации.
4	Классификация конфиденциальной информации	Виды тайны и степени конфиденциальности. Классификация защищаемой информации по собственникам и владельцам.
5	Объекты защиты информации	Понятие и структура угроз защищаемой информации. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию. Каналы и методы несанкционированного доступа к конфиденциальной информации.
6	Классификация видов, методов и средств защиты информации	Виды обеспечения защиты информации. Назначение и структура систем защиты информации

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 1

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Сущность и понятие информационной безопасности	2
2	Цели и значение защиты информации	2
3	Значение информационной безопасности и ее место в системе национальной безопасности	2
4	Современная Доктрина информационной безопасности Российской Федерации	2
5	Теоретические и концептуальные основы защиты информации	2
6	Организационные основы и методологические принципы защиты информации	2
7	Современные факторы, влияющие на защиту информации	2

8	Критерии, условия и принципы отнесения информации к защищаемой	2

4.5 Самостоятельная работа

Семестр № 1

№	Вид СРС	Кол-во академических часов
1	Проработка разделов теоретического материала	40

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: работа в группе

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/view.php?id=10423

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/mod/quiz/view.php?id=385056

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 1 | Устный опрос

Описание процедуры.

Устный опрос проводится по окончанию лекционных занятий путем опроса студентов по списочному составу (при наличии бюджета времени после обсуждения установленных вопросов).

Критерии оценивания.

опрашиваемым студентом должны быть даны верные (по смыслу) ответы на поставленные вопросы; допускается помощь в ответах со стороны аудитории (давшие правильный ответ освобождаются от персональной очереди отвечающих по списку).

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-6.1	Способен продемонстрировать специализированные знания в области защиты информации	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий
ОПК ОС-7.1	Способен продемонстрировать специализированные знания в области защиты информации	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 1, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

1) Экзамен по дисциплине проводится согласно расписанию в назначенной аудитории, в которую приглашается к установленному началу экзамена группа студентов.
2) К экзамену допускаются студенты, которые выполнили все предусмотренные работы по освоению курса: сданы практические работы по выбранной теме.
3) Каждый студент из числа допущенных выбирает один билет и готовится к ответу в течение не менее 30 - 45 минут письменно на поставленные два вопроса в билете.
1. Понятие национальной безопасности. Информационная безопасность в системе национальной безопасности.
2. Структура государственной системы защиты информации.
3. Категории информационной безопасности
4. Основные методы нарушения конфиденциальности, целостности и доступности информации.
5. Уровни информационной безопасности
6. Общая модель защиты информации.
7. Раскрыть основные понятия и принципы теории информационной безопасности.
8. Угрозы безопасности информации.
9. Причины и виды утечки и искажения информации.
10. Анализ методов обеспечения информационной безопасности.
11. Методы защиты информации от НСД в АС.
12. Правовое обеспечение информационной безопасности.
13. Организационное обеспечение информационной безопасности.
14. Инженерно-техническое обеспечение информационной безопасности.
15. Организационно-режимные меры по защите носителей информации.
16. Политики безопасности в АС.
17. Концепция информационной безопасности.
18. Перечислить технические каналы утечки информации.
19. Прямой перехват сигналов. Организационно-технические меры защиты.
20. Излучения радиопередающих устройств систем связи и передачи информации.

Организационно-технические меры защиты.
21. Излучения технических средств обработки информации (ПЭМИН). Организационно - технические меры защиты.
22. Нежелательные электромагнитные связи (наводки). Организационно-технические меры защиты.
23. Излучатели электромагнитных полей. Организационно-технические меры защиты.
24. Высокочастотное навязывание. Организационно-технические меры защиты.
25. Утечка информации по акустическим каналам. Организационно-технические меры защиты.
26. Утечка информации по виброакустическим каналам. Организационно-технические меры защиты.
27. Утечка информации по оптико-акустическим каналам. Организационно-технические меры защиты.
28. Утечка информации по электро-акустическим каналам. Организационнотехнические меры защиты.
29. Виды защиты информации в компьютерных сетях.
30. Криптографическая защита информации.
31. Вредоносные компьютерные программы. Организационно-технические меры защиты.
32. Информация как объект права.

Пример задания:

1.Структура государственной системы защиты информации.
2. Излучения технических средств обработки информации (ПЭМИН). Организационно - технические меры защиты.

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
уверенно и без ошибок отвечает на все вопросы билета	допускает незначительные ошибки в ответе на один из вопросов, включая дополнительные по результатам собеседования.	знает ответы на два вопроса или допускает ошибки в ответах на вопросы	не отвечает на два и более вопросов

7 Основная учебная литература

1. Игнатьева Е. П. Основы информационной безопасности : учебное пособие / Е. П. Игнатьева, 2023. - 96.

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files3/er-32855.pdf

2. Нестеров С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров, 2023. - 324.

[Сайт] – URL: https://e.lanbook.com/book/341267

8 Дополнительная учебная литература и справочная

1. Основы информационной безопасности : учеб. пособие для вузов по специальностям в обл. информ. безопасности / Е. Б. Белов [и др.], 2006. - 544.

2. Расторгуев С. П. Основы информационной безопасности : учеб. пособие для вузов по специальностям "Компьютер. безопасность"... / С. П. Расторгуев, 2007. - 186.

3. Новиков В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения : учебное пособие для вузов по дополнительным профессиональным программам в области информационной безопасности / В. К. Новиков, 2015. - 175.

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 Seven Professional (Microsoft Windows Seven Starter) - Seven, Vista, XP_prof_64, XP_prof_32 - поставка 2010

2. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional [1x100] RUS (проведен апгрейд с Microsoft Windows Seven Starter [1x100]) - поставка 2010

3. Свободно распространяемое программное обеспечение Microsoft Windows Server Standard 2008 R2 Russian Academic OPEN 1 License No Level

12 Материально-техническое обеспечение дисциплины

1. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

2. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

3. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

4. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

5. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

6. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

7. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

8. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

9. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

10. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

11. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

12. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

13. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

14. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

15. МФУ FS-1128 MFP

16. Проектор Epson EB-W04LCD.WXGA 1280*800.3000:1.2800 ANSI Lumens

17. Сервер CPU Intel Core i7-960/GA-X58A-UD3R/DDR-IIIDimm 2Gb/HDD 1 Tb/DVD-RW/512MB PCI-E/блок пит.+ПО