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

«ВВЕДЕНИЕ В ПРОФЕССИОНАЛЬНУЮ ДЕЯТЕЛЬНОСТЬ»

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: 22.06.2026	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 22.06.2026	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 22.06.2026

Год набора – 2026

Иркутск, 2026 г.

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

1.1 Дисциплина «Введение в профессиональную деятельность» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-8 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	ОПК ОС-8.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-8.1	Способен осуществлять подбор основных источников информации по регуляторам профессиональной деятельности, составлять обзор научно-технической литературы, по вопросам обеспечения информационной безопасности	**Знать** основы государства; основные положения отраслей современного российского права; правовые аспекты профессиональной деятельности **Уметь** использовать правовые знания в социальной и профессиональной деятельности; ориентироваться в системе нормативных правовых актов; принимать организационно-управленческие решения в соответствии с нормами действующего российского законодательства в сфере профессиональной деятельности **Владеть** навыками работы с нормативными правовыми документами; навыками выражения своих мыслей и мнения в межличностном и деловом общении с использованием правовых категорий

2 Место дисциплины в структуре ООП

Изучение дисциплины «Введение в профессиональную деятельность» базируется на результатах освоения следующих дисциплин/практик: «Основы информационной безопасности»

Дисциплина является предшествующей для дисциплин/практик: «Физические основы информационной безопасности», «Техническая защита информации», «Основы проектной деятельности», «Учебная практика: учебно-лабораторная практика»

3 Объем дисциплины

Объем дисциплины составляет – 2 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 1
Общая трудоемкость дисциплины	72	72
Аудиторные занятия, в том числе:	32	32
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	40	40
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

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	История защиты информации	1	4					1	5	Устный опрос
2	Сущность и значение профиля «Организация и технологии защиты информации (в сфере техники и технологии)»	2	2					1	5	Устный опрос
3	Квалификационная характеристика специалиста по защите информации	3	4					1	5	Устный опрос
4	Образовательная программа подготовки бакалавра	4	4					1	5	Устный опрос
5	Состав и назначение дисциплин образовательной программы	5	4					1	5	Устный опрос
6	Требования к	6	2					1	4	Устный

	уровню подготовки специалиста									опрос
7	Организация учебного процесса	7	4					1	4	Устный опрос
8	Научно-исследовательская работа	8	4					1	4	Устный опрос
9	Основополагающие принципы защиты информации	9	4					1	3	Устный опрос
	Промежуточная аттестация									Зачет
	Всего		32						40	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 1

№	Тема	Краткое содержание
1	История защиты информации	1.Защита информации с древних времен. 2.Основные особенности организации защиты информации в советский период. 3.Основные особенности организации защиты информации на современном этапе.4.Современное состояние системы защиты информации и перспективы ее совершенствования.
2	Сущность и значение профиля «Организация и технологии защиты информации (в сфере техники и технологии)»	1. Этапы становления специальности. 2. Специальности "Секретное делопроизводство и режим секретности проводимых работ", "Организация защиты государственных секретов", «Обработка защищаемых данных в информационных системах» как предшественники специальности «Комплексное обеспечение информационной безопасности автоматизированных систем». 3. Причины введения специальности «Комплексная защита информации». Сущность специальности, характеристика ее составляющих. 4. Место и значение специальности в подготовке специалистов по информационной безопасности. Связь специальности с другими специальностями в области информационной безопасности. 5. Назначение и структура Государственного образовательного стандарта по специальности.
3	Квалификационная характеристика специалиста по защите информации	1.Объекты профессиональной деятельности специалиста. Виды профессиональной деятельности. 2.Состав задач в области экспериментально-исследовательской, проектно-конструкторской, контрольно-аналитической, организационно-управленческой и эксплуатационной деятельности по защите

		информации, к решению которых должен быть подготовлен специалист.
4	Образовательная программа подготовки бакалавра	1. Состав образовательной программы. 2. Структура учебного плана. Назначение программ учебных дисциплин, учебных и учебно-производственных практик. 3. Классификация дисциплин образовательной программы по компонентам и циклам. 4. Сроки освоения образовательной программы.
5	Состав и назначение дисциплин образовательной программы	1. Общие гуманитарные и социально-экономические дисциплины, их краткая характеристика и назначение. 2. Состав и назначение общих математических и естественно-научных дисциплин. 3. Обще профессиональные дисциплины, их сущность и место в подготовке
6	Требования к уровню подготовки специалиста	1.Знания и умения, которые должен получить специалист в результате изучения общеобразовательной программы. 2.Методы, методики и технологии, которыми должен владеть специалист (дискуссия). 3.Требования к итоговой государственной аттестации специалиста.
7	Организация учебного процесса	1. Отличительные особенности вузовского учебного процесса. Виды учебных занятий. 2. Теоретическое обучение. Сущность и назначение лекционных и семинарских занятий. 3. Практическое обучение. Сущность и назначение практических, лабораторных занятий, учебных и учебно-производственных практик. 4. Сущность и назначение рефератов, докладов, контрольных и курсовых работ. 5. Контроль знаний студентов. Обеспечение контроля в процессе проведения учебных занятий. Промежуточная аттестация. Зачеты, экзамены. Рейтинговая система оценки знаний студентов. 6. Особенности организации образовательного процесса по дисциплинам специальности. Распределение занятий по семестрам. 7. Учебное расписание. Учебная нагрузка студентов. Общий бюджет времени, его планирование. Самоконтроль. 8. Требования к посещению занятий. Организация самостоятельной работы. Работа с литературой. Консультации преподавателей. Технические средства обучения. Электронно-вычислительная техника. 9. Основные принципы обучения. Комплексность. Системность. Фундаментальность.
8	Научно-исследовательская работа	1. Система организации студенческой научно-исследовательской работы. 2. Научные исследования в процессе теоретического и практического обучения. Подготовка научных докладов, рефератов, курсовых работ. 3. Научные исследования в процессе прохождения

		преддипломной практики и выполнения дипломной работы. 4. Студенческие научные кружки. Участие в научно-исследовательских работах, выполняемых вузом. Научные конференции и семинары. 5. Методические основы выполнения научно-исследовательской работы.
9	Основополагающие принципы защиты информации	1. Основные правовые принципы. 2.Организационные принципы защиты информации. 3. Основные принципы и характеристики

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Семестр № 1

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	40

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 самостоятельной работе:

Самостоятельные работы направлены на освоение арсенала методов (основ теории) для решения задач по дисциплине.
Ход работы (при выполнении заданий по практическим работам):
1) Ознакомиться по материалам курса лекций, по литературе или другим источникам информации с методами оценки экономических показателей;
2) Отыскать решение данных задач для конкретных случаев;
3) Сделать необходимые заготовки материалов (провести описание привлекаемых к решениям методов) для дальнейшего выполнения работ в приложении к своему проекту;
4) Теоретические основы и примеры решения задач могут представляться в качестве образцовых для заслушивания и обсуждения аудиторией.

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.

Осуществляется проверка соответствия выбираемой темы и наличие промежуточной аттестации по аналогичной дисциплине.
Пример задания:
1. Студент намеревается выбрать задание по теме: защита информации в системах управления базами данных;
2. Студент выбирает данную тему при наличии полученной аттестации по дисциплине «программно-аппаратные средства защиты информации» или по курсовой работе по данной дисциплине.

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-8.1	Демонстрирует способность осуществлять подбор основных источников информации по направлению профессиональной деятельности, составлять обзор научно-технической литературы, по вопросам обеспечения информационной безопасности, а также применять нормативные акты и	Устный опрос

	методические документы органов власти по направлению деятельности	

6.2.2 Типовые оценочные средства промежуточной аттестации

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

6.2.2.1.1 Описание процедуры

1) Зачет по дисциплине проводится согласно расписанию в назначенной аудитории, в которую приглашается к установленному началу зачета группа студентов.
2) К зачету допускаются студенты, которые выполнили все предусмотренные работы по освоению курса.
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.

Пример задания:

Зачет проводится в форме устного опроса по экзаменационным билетам.
1. Специализация специалистов по ИБ.
2. Какими компетенциями Soft-Skill должен обладать специалист по ИБ.
3. Какими компетенциями Hard-Skill должен обладать специалист по ИБ.
4. Понятие «Защита информации». Задачи защиты информации.
5. Понятия “Субъект”, “Объект”, “Доступ”. Примеры.
6. Что такое информация. Основные свойства информации.
7. Виды носителей информации.
8. Жизненный цикл информации.
9. Информационная система.
10. Что понимается под конфиденциальной информацией?
11. Виды тайн.
12. Основные регуляторы.
13. Структура правовой системы.
14. Угроза информационной безопасности. Классификация.
15. Основные направления реализации угроз.
16. Основные методы реализации угроз.
17. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
18. Модель нарушителя.
19. Несанкционированный доступ.
20. Классификация методов защиты от НСД.
21. Организационные методы защиты от НСД.
22. Инженерно-технические методы защиты от НСД.
23. Резервное копирование.
24. Что понимается под утечкой информации?
25. Идентификация. Аутентификация. Авторизация.
26. Криптографические методы защиты информации.
27. Симметричная криптосистема.
28. Асимметричная криптосистема.
29. Методы защиты конфиденциальности информации на уровне содержания.
30. Стеганография.

31. Защита целостности информации при хранении.
32. Защита целостности информации при обработке.
33. Защита целостности информации при транспортировке.
34. Дезинформация. Основные приемы, методы борьбы.
35. Политика безопасности. Модель безопасности.
36. Аксиомы политики безопасности.
37. Субъектно-объектные модели разграничения доступа.
38. Понятия Потока, Доступа.
39. Матрица доступа.
40. Мандатный доступ.
41. Социальная инженерия.
42. Инфомационная война. Основные виды.
43. Вредоносное ПО.
44. Антивирусное ПО.
45. Что понимается под словом « инцидент».
46. Цели, функции и задачи защиты информации в сетях передачи данных.
47. Архитектура механизмов защиты информации в сетях передачи данных.
48. Безопасность беспроводных сетей.
49. Виды персональной ответственности – Гражданская, Административная, Уголовная.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Посещал лекции. Полно и связно ответил более чем на 50% теоретических вопросов, дал правильное определение основным понятиям. Может обосновать свои суждения, привести необходимые примеры.	Пропустил более половины занятий без уважительной причины. Обнаруживает незнание большей части вопроса, допускает ошибки в формулировке определений и правил, беспорядочно и неуверенно излагает материал.

7 Основная учебная литература

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

[Сайт] – URL: https://e.lanbook.com/book/293009

2. Введение в информационную безопасность : учебное пособие для вузов по направлениям подготовки (специальностям), не входящим в направление подготовки "Информационная безопасность" / А. А. Малюк [и др.]; под ред. В. С. Горбатова, 2014. - 288.

8 Дополнительная учебная литература и справочная

1. Осавелюк Е. А. Информационная безопасность государства и общества в контексте деятельности СМИ : монография / Е. А. Осавелюк, 2023. - 92.

[Сайт] – URL: https://e.lanbook.com/book/330518

2. Прохорова О. В. Информационная безопасность и защита информации : учебное пособие / О. В. Прохорова, 2020. - 124 с

[Сайт] – URL: https://e.lanbook.com/book/133924

3. Нестеров С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров, 2016. - 321.

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

3. Microsoft® Office Professional Plus 2010 Russian OpenLicensePack NoLevel AcademicEdition

4. Microsoft Office 2007 VLK (поставки 2007 и 2008)

12 Материально-техническое обеспечение дисциплины

1. Экран ScreenMedia GoldView 274*206 настенный

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

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. 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

16. 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

17. 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

18. 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

19. 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

20. 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

21. 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