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

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление: 09.03.02 Информационные системы и технологии

Информационные системы и технологии в административном управлении

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Мамедов Эльшан Фахраддинович Дата подписания: 09.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 11.06.2025	Документ подписан простой электронной подписью Согласовал: Аршинский Вадим Леонидович Дата подписания: 09.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

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

Код, наименование компетенции	Код индикатора компетенции
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-3.4
ОПК ОС-4 Способность участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил	ОПК ОС-4.3

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-3.4	Имеет представление об основных компонентах информационной безопасности и способен применять инструменты обеспечения информационной безопасности в рамках решения задач профессиональной деятельности	**Знать** основы российской правовой системы и законодательства, правового статуса личности, организации деятельности органов государственной власти Российской Федерации по защите информации; характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ; виды и степень ответственности за правонарушения и преступления в информационной сфере; порядок работы с персоналом по вопросам обеспечения защиты информации ограниченного доступа, проведения мероприятий по физической и технической защите конфиденциальной информации, организации службы безопасности предприятия **Уметь** определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности

		Владеть навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности; навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии
ОПК ОС-4.3	Способен составлять рабочую документацию в соответствии с требованиями стандартов по обеспечению информационной безопасности	**Знать** основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации **Уметь** анализировать правовые акты и осуществлять правовую оценку информации; предпринимать необходимые меры по восстановлению нарушенных прав; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации **Владеть** навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности навыками работы с нормативными правовыми актами

2 Место дисциплины в структуре ООП

Изучение дисциплины «Основы информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Технологии программирования», «Методы анализа данных», «Архитектура информационных систем», «Анализ бизнес-процессов», «Операционные системы», «Базы данных»

Дисциплина является предшествующей для дисциплин/практик: «Нейросетевые технологии», «Правоведение», «Проектная деятельность», «Интеллектуальные системы и технологии», «Проектирование информационных систем», «Мониторинг безопасности информационных систем»

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 № 5
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	48	48
лекции	16	16
лабораторные работы	32	32
практические/семинарские занятия	0	0
Контактная работа, в том числе	0	0
в форме работы в электронной информационной образовательной среде	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	60	60
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет с оценкой	Зачет с оценкой

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 5

№ 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	Информационные отношения и режим защиты информации ограниченного доступа	1	4	1	2			1	12	Устный опрос
2	Защита конфиденциальной информации	2	4	2	4			1	12	Устный опрос
3	Защита персональных данных	3	4	3	4			1	12	Устный опрос
4	Организационное обеспечение информационной безопасности	4	2	6, 8, 9, 10	14			1	12	Устный опрос
5	Государственное регулирование деятельности по защите информации	5	2	4, 5, 7	8			1	12	Устный опрос
	Промежуточная									Зачет с

	аттестация									оценкой
	Всего		16		32				60	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 5

№	Тема	Краткое содержание
1	Информационные отношения и режим защиты информации ограниченного доступа	Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности. Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующие обеспечение информационной безопасности в Российской Федерации Понятие и виды информации ограниченного доступа по законодательству РФ. Правовой режим защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Правовой режим защиты информации конфиденциального характера. Понятие информации конфиденциального характера по российскому законодательству. Основные виды конфиденциальной информации. Основные требования, предъявляемые к организации защиты конфиденциальной информации
2	Защита конфиденциальной информации	Институт правовой защиты служебной тайны. Правовые основы защиты служебной тайны. Нормативно-правовые акты, регулирующие правовую защиту служебной тайны. Защита в режиме служебной тайны сведений, доступ к которым ограничивается в соответствии с законодательством, при обращении и хранении таких сведений (информации) в органах государственной власти и органах местного самоуправления. Институт правовой защиты коммерческой тайны. Правовые основы защиты

		коммерческой тайны. Объекты и субъекты права на коммерческую тайну. Права и обязанности обладателя коммерческой тайны. Ответственность за нарушение прав на коммерческую тайну. Институт правовой защиты банковской тайны. Институт правовой защиты профессиональной тайны
3	Защита персональных данных	Институт правовой защиты персональных данных. Правовые основы защиты информации персонального характера. ФЗ «О персональных данных», подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных. Государственный надзор и контроль обработки персональных данных
4	Организационное обеспечение информационной безопасности	Понятие организационной защиты информации. Сущность организационных методов защиты информации. Соотношение организационных мер защиты информации с мерами правового и технического характера. Основные термины, связанные с организацией защиты информации. Организация режима секретности. Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Особенности системы организационной защиты государственной тайны. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны. Организация деятельности режимно-секретных органов. Установление и изменение степени секретности сведений, отнесенных к государственной тайне. Понятие «рассекречивание сведений». Основания для рассекречивания сведений. Допуск к государственной тайне. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности. Организация доступа к сведениям, составляющим государственную тайну
5	Государственное регулирование деятельности по защите информации	Государственное регулирование деятельности в области защиты информации. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной

		деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Правовые основы сертификации в области защиты информации. Правонарушения в информационной сфере и особенности защиты от них. Особенности правонарушений в информационной сфере. Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Правовая защита информационных систем. Правовая защита результатов интеллектуальной деятельности

4.3 Перечень лабораторных работ

Семестр № 5

№	Наименование лабораторной работы	Кол-во академических часов
1	Информационные отношения и режим защиты информации ограниченного доступа	2
2	Правовой режим защиты информации конфиденциального характера	4
3	Институт правовой защиты персональных данных	4
4	Государственное регулирование деятельности в области защиты информации	4
5	Преступления в сфере компьютерной информации	2
6	Понятие и сущность организационной защиты информации	4
7	Организация режима секретности	2
8	Организация служебного расследования по фактам утраты информации	4
9	Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам	4
10	Организационно-правовое взаимодействие с регуляторами в сфере информационной безопасности	2

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Семестр № 5

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям (лабораторным работам)	60

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 лабораторным работам:

Лабораторные работы предназначены для теоретического осмысления и обобщения разделов курса. Вводная лекция служит для создания общего впечатления о дисциплине. На занятии до сведения обучающегося доводятся основные вопросы дисциплины, показывается ее роль и место в соответствующей области знаний, определяется значение дисциплины для формирования компетенций. Для закрепления материала обучающимся на занятии предлагается выполнить небольшие контрольные работы по темам:

Информационные отношения и правовой режим защиты информации ограниченного доступа;

Правовая защита различных видов конфиденциальной информации;

Защита персональных данных и государственное регулирование деятельности по защите информации;

Организационное обеспечение информационной безопасности;

Организация охраны, режима и работы с персоналом;

Организация защиты информации в различных направлениях деятельности предприятия (организации);

Организация взаимодействия с федеральными органами исполнительной власти в сфере обеспечения информационной безопасности.

Неотъемлемой частью изучения дисциплины «Основы информационной безопасности» является выполнение лабораторных работ, основной целью которых является выработка умений работы с литературой, изучения специальных разделов (работа регуляторов), этапы и порядок проведения работ по созданию системы защиты информации.

В лабораторных работах обучающийся должен выполнить проектирование политики информационной безопасности организации (предприятия).

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на лабораторных занятиях, входит в накопленную оценку.

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 5 | Устный опрос

Описание процедуры.

Выполнение письменной проверочной работы.
Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности. Основной целью политики информационной безопасности является общее описание правил работы с информацией компании. Наличие сформулированных и закрепленных на бумаге правил обеспечения информационной безопасности позволит достичь:
1. Стабильность защиты.
2. Независимость защиты от личных и профессиональных качеств исполняющего персонала.
3. Возможность контроля как защиты, так и процедур обработки информации.
Перед разработкой политики информационной безопасности должен быть проведен анализ активов, включающий их учет и оценку.
Готовая политика должна иметь в своем составе отдельный раздел для каждого обнаруженного актива, группы взаимосвязанных активов или обособленной части актива компании в зависимости от ранее проведенного анализа их структуры и взаимосвязи.
В дополнение и исходя из политики информационной безопасности могут быть разработаны другие документы, такие как руководства или стандарты. В отличие от политик они более конкретны, что выражается в привязке к определенному оборудованию, версиям программ или в точном указании необходимой последовательности действий для достижения заданного результата.
Политика информационной безопасности разрабатывается специалистами информационной безопасности компании для использования остальными сотрудниками компании. Поэтому, она должна быть изложена максимально просто, на обычном языке с использованием минимума специальной лексики только там, где это необходимо.

Критерии оценивания.

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-3.4	Демонстрирует высокий уровень знаний нормативных правовых актов РФ и стандартов в сфере информационной безопасности	Проверочная работа

	киберфизических систем, руководящих и методических документов ФСТЭК России и ФСБ России при применении экспертных систем комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем	
ОПК ОС-4.3	Демонстрирует высокий уровень знаний нормативных правовых актов РФ и стандартов в сфере информационной безопасности киберфизических систем, руководящих и методических документов ФСТЭК России и ФСБ России при применении экспертных систем комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем	Проверочная работа

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 5, Типовые оценочные средства для проведения дифференцированного зачета по дисциплине

6.2.2.1.1 Описание процедуры

Перечень теоретических вопросов, практических заданий и ситуаций, выносимых на дифференцированный зачет, 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.

Вопросы к дифференцированному зачету

1. Основные нормативно-правовые акты в области защиты персональных данных.
2. Характеристика Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Обеспечение конфиденциальности персональных данных.
4. Специальные категории персональных данных.
5. Права субъекта персональных данных, обязанности оператора.
6. Принципы обработки и хранения персональных данных.
7. Условия обработки персональных данных.
8. Особенности обработки персональных данных в государственных информационных системах персональных данных.
9. Понятие, виды и полномочия федеральных органов в области обеспечения безопасности персональных данных.
10. Система государственного контроля и надзора за обеспечением безопасности и

защиты персональных данных.
11. Методические документы регуляторов.
12. Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных.
13. Технические меры защиты от НСД в информационных системах персональных данных различного класса.
14. Понятие информационной системы персональных данных.
15. Структура информационной системы персональных данных.
16. Состав мероприятий по приведению информационных систем и процессов обработки персональных данных в соответствие с требованиями законодательства о персональных данных.
17. Информационные отношения как объект правового регулирования.
18. Законодательство Российской Федерации в области информационной безопасности.
19. Категории информации по условиям доступа к ней и распространения.
20. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
21. Субъекты и объекты правоотношений в области информационной безопасности.
22. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
23. Правовой режим защиты информации конфиденциального характера.
24. Правовые основы защиты служебной тайны.
25. Организационно-правовое взаимодействие служб ИБ организаций (предприятий) с ФСБ России, ФСТЭК России и Роскомнадзором.
26. Правовое регулирование деятельности Федеральной службы безопасности РФ.
27. Правовое регулирование деятельности Федеральной службы по техническому и экспортному контролю РФ.
28. Правовое регулирование деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ (Роскомнадзора).
29. Современные проблемы информационной безопасности и пути их решения.
30. Системный подход к управлению информационной безопасностью.
31. Система государственного управления информационной безопасностью.
32. Локальные нормативные акты предприятия по информационной безопасности.
33. Формы правовой защиты информации на предприятии.
34. Юридическая ответственность за нарушение законодательства в сфере информационной безопасности.
35. Особенности организационной защиты компьютерных информационных систем и сетей.
36. Обязанности руководства по обеспечению информационной безопасности.
37. Назначение, цели и виды аудита информационной безопасности.

Пример задания:

1 Организация контроля соблюдения персоналом требований режима защиты информации.
2 Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
3 Характеристика ФЗ «О безопасности критической информационной инфраструктуры».

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. Краковский Ю. М. Информационная безопасность и защита информации : учебное пособие для вузов по направлению подготовки 09.03.01 "Информатика и вычислительная техника" (протокол № 528 от 10 августа 2015 года) / Ю. М. Краковский, 2016. - 223.

8 Дополнительная учебная литература и справочная

1. Игнатьев Е. Б. Защита информации: криптоалгоритмы хеширования : учебное пособие для вузов / Е. Б. Игнатьев, 2024. - 264.

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

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