

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

«ФИЗИЧЕСКИЕ 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:
Дмитриев Алексей
Александрович
Дата подписания: 13.06.2026

Документ подписан простой
электронной подписью
Утвердил: Говорков Алексей
Сергеевич
Дата подписания: 14.06.2026

Документ подписан простой
электронной подписью
Согласовал: Маринов
Александр Андреевич
Дата подписания: 17.06.2026

Год набора – 2026

Иркутск, 2026 г.

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

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

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-1 Способность анализировать физические явления и процессы для решения профессиональных задач	ОПК ОС-1.4

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-1.4	Способен осуществлять настройку и конфигурирование программно-аппаратных средств защиты информации, включая подсистемы объекта защиты информационной безопасности, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать Основные принципы построения и функционирования программно-аппаратных средств защиты информации. Методы и средства настройки и конфигурирования подсистем защиты информации (межсетевые экраны, IDS/IPS, SIEM-системы). Принципы работы компьютерных сетей и уязвимости, связанные с их конфигурацией. Уметь Настраивать и конфигурировать аппаратные и программные средства защиты информации (брандмауэры, VPN, системы аутентификации). Анализировать и устранять уязвимости в конфигурации компьютерных сетей. Развертывать и настраивать системы антивирусной защиты. Применять средства криптографической защиты. Проводить аудит защищенности информационных систем и сетей. Интерпретировать логи и события безопасности для выявления инцидентов. Владеть Навыками администрирования средств защиты информации (настройка политик безопасности, управление доступом). Практическими навыками работы с криптографическими алгоритмами и протоколами (AES, RSA, SSL/TLS).

		Современными инструментами мониторинга и управления информационной безопасностью
--	--	--

2 Место дисциплины в структуре ООП

Изучение дисциплины «Физические основы информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Информационные технологии», «Основы информационной безопасности», «Аудит информационной безопасности»

Дисциплина является предшествующей для дисциплин/практик: «Основы управления информационной безопасностью», «Программно-аппаратные средства защиты информации», «Безопасность сетей и баз данных», «Безопасность операционных систем»

3 Объем дисциплины

Объем дисциплины составляет – 6 ЗЕТ

Вид учебной работы	Трудоемкость в академических часах (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 4
Общая трудоемкость дисциплины	216	216
Аудиторные занятия, в том числе:	96	96
лекции	32	32
лабораторные работы	32	32
практические/семинарские занятия	32	32
Самостоятельная работа (в т.ч. курсовое проектирование)	84	84
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 № 4

№ 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	Введение в технические разведки	1	4	1	4	1	4	1	12	Устный опрос
2	Видовая разведка (IMINT)	2	4	2	4	2	4	1	12	Устный опрос
3	Радиоэлектронная разведка (SIGINT)	3	4	3	4	3	4	1	10	Устный опрос
4	Параметрическая	4	4	4	4	4	4	1	10	Устный

	разведка (MASINT)									опрос
5	Космическая разведка	5	4	5	4	5	4	1	10	Устный опрос
6	Воздушная разведка	6	4	6	4	6	4	1	10	Устный опрос
7	Морская разведка	7	4	7	4	7	4	1	10	Устный опрос
8	Защита информации от технических разведок	8	4	8	4	8	4	1	10	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		32		32		32		120	

4.2 Краткое содержание разделов и тем занятий

Семестр № 4

№	Тема	Краткое содержание
1	Введение в технические разведки	История развития технических разведок. Цели, задачи и организация технической разведки.
2	Видовая разведка (IMINT)	Принципы получения изображений в различных диапазонах (оптический, ИК, радио). Аппаратура видовой разведки: фотографическая, телевизионная, лазерная.
3	Радиоэлектронная разведка (SIGINT)	Основы радиоразведки и радиотехнической разведки. Разведка побочных излучений (ПЭМИН).
4	Параметрическая разведка (MASINT)	Разведка физических параметров объектов (акустическая, магнитная, радиационная). Применение в военной и гражданской сферах.
5	Космическая разведка	Системы космической разведки (оптические, радиолокационные, радиоэлектронные). Современные космические аппараты и их возможности.
6	Воздушная разведка	Самолеты и БПЛА в разведке. Аппаратура воздушной разведки: РЛС, оптико-электронные системы.
7	Морская разведка	Гидроакустические и радиолокационные методы. Корабли и подводные аппараты в разведке.
8	Защита информации от технических разведок	Методы защиты от утечки информации по техническим каналам. Организационные и технические меры защиты.

4.3 Перечень лабораторных работ

Семестр № 4

№	Наименование лабораторной работы	Кол-во академических часов
1	Разработка схемы организации технической разведки на примере современных систем.	4
2	Обработка и анализ многоспектральных изображений.	4
3	Имитация перехвата радиосигналов и анализ их параметров.	4
4	Анализ данных сейсмических датчиков.	4
5	Моделирование работы спутниковой системы разведки.	4
6	Обработка данных, полученных с воздушных носителей.	4
7	Анализ данных гидролокаторов.	4
8	Разработка плана защиты объекта от видовой и радиоэлектронной разведки.	4

4.4 Перечень практических занятий

Семестр № 4

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Схема разведки	4
2	Определение объектов	4
3	Поиск радиосигналов	4
4	Анализ вибраций	4
5	Сравнение разрешения	4
6	Радиолокация	4
7	Анализ корабельных сигналов	4
8	Экранирование сигналов	4

4.5 Самостоятельная работа

Семестр № 4

№	Вид СРС	Кол-во академических часов
1	Проработка разделов теоретического материала	84

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Деловая игра

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

Бабурин А. В. Физические основы защиты информации: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (5,34 Мб) / А. В. Бабурин, А. С. Пахомова. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015

5.1.2 Методические указания для обучающихся по лабораторным работам:

Бабурин А. В. Физические основы защиты информации: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (5,34 Мб) / А. В. Бабурин, А. С. Пахомова. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015

5.1.3 Методические указания для обучающихся по самостоятельной работе:

Бабурин А. В. Физические основы защиты информации: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (5,34 Мб) / А. В. Бабурин, А. С. Пахомова. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015

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 4 | Устный опрос

Описание процедуры.

1. Выдача 2 вопросов каждому студенту индивидуально
2. Подготовка студентами письменного ответа
3. Объяснения ответов на вопросы

Критерии оценивания.

Глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует в ответе материал научной литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

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-1.4	Понимание принципов работы программно-аппаратных средств защиты информации. Знание методов настройки и конфигурирования подсистем защиты (межсетевые экраны, IDS/IPS, SIEM). Понимание основ криптографии и	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий

	принципов работы СКЗИ. Знание нормативных требований (ФЗ-152, ГОСТ Р 57580, требования ФСТЭК и ФСБ). Умение проводить аудит защищенности компьютерных сетей. Способность выявлять уязвимости в конфигурации систем. Навыки интерпретации логов и событий безопасности.	
--	--	--

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 4, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

Успешному проведению экзамена способствует систематическое посещение лекционных, практических и семинарских занятий, лабораторных работ, тщательная проработка вопросов, выносимых на обсуждения на групповых занятиях и самостоятельная подготовка обучающихся. При подготовке к экзамену необходимо ознакомиться с вопросами, составить структурно-логическую схему ответа на каждый вопрос, используя при этом материалы лекционных практических и семинарских занятий, рекомендуемую преподавателем литературу. При возникновении сложностей в процессе подготовки к экзамену необходимо обратиться за консультацией к преподавателю.

Экзамены являются заключительным этапом изучения учебной дисциплины и имеют целью проверить теоретические знания обучающихся, их навыки и умение применять полученные знания при решении практических задач. Экзамен проводится в объеме рабочей программы учебной дисциплины. В экзаменационный билет включены четыре теоретических вопроса из разных разделов программы.

Пример задания:

1. Введение в технические разведки

Дайте определение технической разведки.

Назовите основные цели технической разведки.

Какие виды технической разведки существуют?

Как развивалась техническая разведка в XX веке?

Какие страны являются лидерами в области технической разведки?

В чем разница между агентурной и технической разведкой?

Какие физические принципы лежат в основе технической разведки?

Какова роль космических технологий в современной разведке?

2. Видовая разведка (IMINT)

Что такое видовая разведка?

Какие диапазоны электромагнитного спектра используются в видовой разведке?

Как работает тепловизор?

В чем преимущества многоспектральной съемки?

Какие типы камер используются в воздушной разведке?

Как определяется разрешение спутниковых снимков?

Какие факторы влияют на качество изображения в ИК-диапазоне?

Как работает лазерный сканер в видовой разведке?

3. Радиоэлектронная разведка (SIGINT)

Что включает в себя радиоэлектронная разведка?

Какие задачи решает радиотехническая разведка?

Как работает перехват радиосигналов?

Что такое ПЭМИН и как его используют в разведке?

Какие методы защиты от радиоэлектронной разведки существуют?

Как определяют местоположение источника радиосигнала?

Какие частотные диапазоны наиболее уязвимы для перехвата?

Как работают станции радиоперехвата?

4. Параметрическая разведка (MASINT)

Что изучает параметрическая разведка?

Какие физические параметры объектов могут быть использованы в разведке?

Как работает магнитометрическая разведка?

Какие методы используются в акустической разведке?

Как обнаруживают ядерные испытания с помощью сейсмических датчиков?

Какие приборы применяются в радиационной разведке?

Как химическая разведка определяет состав веществ?

В чем особенность гиперспектральной разведки?

5. Космическая разведка

Какие виды космической разведки существуют?

Как работают спутники оптической разведки?

Какие преимущества у радиолокационных спутников?

Как определяют координаты объектов с помощью спутников?

Какие страны обладают собственными системами космической разведки?

Как спутники обнаруживают пуски ракет?

Какие технологии используются для передачи данных со спутников?

Какова роль GPS в современной разведке?

6. Воздушная разведка

Какие летательные аппараты используются в воздушной разведке?

В чем преимущества БПЛА перед пилотируемыми самолетами?

Как работает РЛС на самолетах ДРЛО?

Какие датчики устанавливают на разведывательные БПЛА?

Как обеспечивается скрытность воздушной разведки?

Какие задачи решает авиационная радиоэлектронная разведка?

Как используются вертолеты в разведке?

Какие методы защиты от воздушной разведки существуют?

7. Морская разведка

Какие задачи решает морская разведка?

Как работают гидроакустические станции?

Какие корабли используются для радиоэлектронной разведки?

Как обнаруживают подводные лодки?

Какие технологии применяются в разведке морских акваторий?

Как работают буи радиогидроакустической разведки?

Какие методы используются для слежения за надводными кораблями?

Как защищают морские объекты от технической разведки?

8. Защита информации от технических разведок

Какие каналы утечки информации существуют?

Как защищают информацию от перехвата радиосигналов?

Какие методы маскировки применяются против видовой разведки?

Как экранируют технику от ПЭМИН?

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует в ответе материал научной литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.	Твердо знает материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	Имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ	Не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

7 Основная учебная литература

1. Бабурин А. В. Физические основы защиты информации: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (5,34 Мб) / А. В. Бабурин, А. С. Пахомова. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015

[Сайт] – URL: УДК 004.056

8 Дополнительная учебная литература и справочная

1. Романов О. А. Организационное обеспечение информационной безопасности : учебник для вузов по специальностям "Организация и технология защиты информации" / О. А. Романов, С. А. Бабин, С. Г. Жданов, 2008. - 2008.

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

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. Лицензионное программное обеспечение Системное программное обеспечение
2. Лицензионное программное обеспечение Пакет прикладных офисных программ
3. Лицензионное программное обеспечение Интернет-браузер

12 Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: комплект учебной мебели, рабочее место преподавателя, доска. Мультимедийное оборудование (в том числе переносное): мультимедийный проектор, экран, акустическая система, компьютер с выходом в интернет.

2. Учебная аудитория для проведения лабораторных/практических (семинарских) занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: комплект учебной мебели, рабочее место преподавателя, доска. Мультимедийное оборудование (в том числе переносное): мультимедийный проектор, экран, акустическая система, компьютер с выходом в интернет.