

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 27.08.2026 15:53:52

Уникальный программный ключ:

sa953a0120d891083f939673078ef1a989dae18a

Федеральное государственное автономное образовательное учреждение высшего образования

«Российский университет дружбы народов имени Патриса Лумумбы»

Факультет искусственного интеллекта

(наименование основного учебного подразделения (ОУП) – разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/специальности)

Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(наименование (профиль/специализация) ОП ВО)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Физические основы защиты информации» входит в программу бакалавриата «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» по направлению 10.03.01 «Информационная безопасность» и изучается в 5 семестре 3 курса. Дисциплину реализует Кафедра информационной безопасности. Дисциплина состоит из 4 разделов и 7 тем и направлена на изучение основных физических принципов образования технических каналов утечки информации, а также закономерностей проявления физических эффектов в технических системах и их взаимодействия с окружающей средой.

Целью освоения дисциплины является формирование у обучающихся понимания основных методов и базовых умений выявления, классификации и противодействия утечке информации по различным техническим каналам на основе знаний физических явлений, лежащих в основе их возникновения, и закономерностей технической реализации средств защиты.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Физические основы защиты информации» направлено на формирование у обучающихся следующих компетенций (части компетенций):

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
пОПК-2.1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	пОПК-2.1.1 Знает возможные функциональные процессы объекта защиты и его информационных составляющих для выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба; пОПК-2.1.2 Проводит анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Применяет средства технической защиты информации для решения задач профессиональной деятельности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Физические основы защиты информации» относится к обязательной части блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Физические основы защиты информации».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Аппаратные средства вычислительной техники;	Эксплуатационная практика; Технологическая практика; Методы и средства криптографической защиты информации; Комплексное обеспечение защиты информации объекта информатизации;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
			Защита информации от утечки по техническим каналам;
пОПК-2.1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Аппаратные средства вычислительной техники;	Эксплуатационная практика; Технологическая практика; Защита информации от утечки по техническим каналам; Анализ и управление рисками информационной безопасности; Программно-аппаратные средства защиты информации; Комплексное обеспечение защиты информации объекта информатизации;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Физические основы защиты информации» составляет «4» зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	ВСЕГО, ак.ч.		Семестр(-ы)
			5
Контактная работа, ак.ч	60		60
Лекции (ЛК)	30		30
Лабораторные работы (ЛР)	30		30
Практические/семинарские занятия (СЗ)	0		0
Самостоятельная работа обучающихся, ак.ч.	66		66
Контроль (экзамен/зачет с оценкой), ак.ч.	18		18
Общая трудоемкость дисциплины ак.ч.	ак.ч.	144	144
	зач.ед.	4	4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы*

Номер раздела	Наименование раздела дисциплины	Наименование темы		Вид учебной работы*
Раздел 1	Физические основы образования каналов утечки информации.	1.1	Системный подход как основа создания эффективной инженерно-технической защиты информации.	ЛК, ЛР
Раздел 2	Физические основы технических систем.	2.1	Закономерности проявления физических эффектов.	ЛК, ЛР
		2.2	Закономерности технической реализации физических эффектов.	ЛК, ЛР
Раздел 3	Технические каналы утечки информации.	3.1	Классификация технических каналов утечки информации.	ЛК, ЛР
Раздел 4	Электромагнитные явления и эффекты в создании каналов утечки информации.	4.1	Источники электромагнитных излучений и наводок	ЛК, ЛР
		4.2	Методы защиты информации от утечки через ПЭМИН	ЛК, ЛР
		4.3	Структурные схемы образования комплексных каналов утечки информации	ЛК, ЛР

* - заполняется только по ОЧНОЙ форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – практические/семинарские занятия.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Лекционная	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска.
Лаборатория	Аудитория для проведения лабораторных работ, индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и оборудованием.	Персональные компьютеры или моноблоки с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. Программное обеспечение: среда виртуализации Oracle VM VirtualBox (свободно-распространяемое ПО), операционная система Debian Linux (свободно-распространяемое ПО), интерпретатор Python (свободно-распространяемое ПО), свободно-распространяемые программные пакеты симуляции физических атак (например, SeseLab и GRFICSv3 (свободно-распространяемое ПО)).
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 25 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	Персональные компьютеры или моноблоки с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. Программное обеспечение: среда виртуализации Oracle VM VirtualBox (свободно-распространяемое ПО), операционная система Debian Linux (свободно-распространяемое ПО), интерпретатор Python (свободно-распространяемое ПО), свободно-распространяемые программные пакеты симуляции физических атак (например, SeseLab и GRFICSv3 (свободно-распространяемое ПО)).
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет).

* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО!**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : [16+] / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет им. А. А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=694670> (дата обращения: 25.03.2026). – Библиогр.: с. 117-118. – ISBN 978-5-4499-3327-0. – DOI 10.23681/694670. – Текст : электронный.

2. Шейдаков, Н. Е. Физические основы защиты информации : учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. — Москва : РИОР : ИНФРА-М, 2026. — 204 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/21158>. - ISBN 978-5-369-01603-9. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2084198> (дата обращения: 25.03.2026). – Режим доступа: по подписке.

Дополнительная литература:

1. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. - Саратов : РФЯЦ-ВНИИЭФ, 2019. - 267 с. - ISBN 978-5-9515-0426-5. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1230831> (дата обращения: 25.03.2026). – Режим доступа: по подписке.

2. Техническая защита информации : практикум / сост. А. С. Кравченко, В. А. Мельник, С. Л. Сахаров ; ФКОУ ВО Воронежский институт ФСИН России. - Иваново : Издательско-полиграфический комплекс «ПресСто», 2023. - 80 с. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2158325> (дата обращения: 25.03.2026). – Режим доступа: по подписке.

3. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/584050> (дата обращения: 25.03.2026).

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров

- Электронно-библиотечная система РУДН – ЭБС РУДН <https://mega.rudn.ru/MegaPro/Web>
- ЭБС «Университетская библиотека онлайн» <http://www.biblioclub.ru>
- ЭБС Юрайт <http://www.biblio-online.ru>
- ЭБС «Консультант студента» www.studentlibrary.ru
- ЭБС «Знаниум» <https://znanium.ru/>

2. Базы данных и поисковые системы

- Sage <https://journals.sagepub.com/>
- Springer Nature Link <https://link.springer.com/>
- Wiley Journal Database <https://onlinelibrary.wiley.com/>
- Наукометрическая база данных Lens.org <https://www.lens.org>

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1. Курс лекций по дисциплине «Физические основы защиты информации».

* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС!**

РАЗРАБОТЧИКИ:

Заведующий кафедрой
информационной безопасности

Должность

Подпись

Царегородцев А.В.

Фамилия И.О

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой
информационной безопасности

Должность

Подпись

Царегородцев А.В.

Фамилия И.О

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой
информационной безопасности

Должность

Подпись

Царегородцев А.В.

Фамилия И.О