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

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА 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)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Программно-аппаратные средства 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 6, 7 семестрах 3, 4 курсов. Дисциплину реализует Кафедра информационной безопасности . Дисциплина состоит из 2 разделов и 4 тем и направлена на изучение программных и аппаратных средств, используемых для обеспечения защиты информации от несанкционированного доступа, утечек данных, вирусов и других видов атак. Студенты получают знания о принципах работы антивирусных программ, межсетевых экранов, систем обнаружения вторжений, криптографических средств и других инструментов, используемых для обеспечения информационной безопасности, а также получают умения работы с ними.

Целью освоения дисциплины является формирование у обучающихся понимания принципов функционирования современных программно-аппаратных средств защиты информации, а также развитие навыков их настройки и эксплуатации для обеспечения информационной безопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Программно-аппаратные средства 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-2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.2 Применяет программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.2 При решении профессиональных задач организует защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Программно-аппаратные средства 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 «Программно-аппаратные средства 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-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Организационное и правовое обеспечение информационной безопасности; Защищенный документооборот;	Технологическая практика; Комплексное обеспечение защиты информации объекта информатизации;
ОПК-2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	Ознакомительная практика; Исследовательская практика; Информационные технологии; Операционные системы; Базы данных, системы управления базами данных; Сети и системы передачи информации; Технологии искусственного интеллекта в задачах кибербезопасности; Аппаратные средства вычислительной техники; Языки программирования; Технологии и методы программирования;	Технологическая практика;
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; Физические основы защиты информации;	Технологическая практика; 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 «Программно-аппаратные средства защиты информации» составляет «10» зачетных единиц.

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)**	**Семестр(-ы)**
			6	**7**
Контактная работа, ак.ч	*146*		*78*	*68*
Лекции (**ЛК**)	73		39	34
Лабораторные работы (**ЛР**)	73		39	34
Практические/семинарские занятия (**СЗ**)	0		0	0
Самостоятельная работа обучающихся, ак.ч.	*151*		*66*	*85*
Контроль (экзамен/зачет с оценкой), ак.ч.	*63*		*36*	*27*
Общая трудоемкость дисциплины ак.ч.	**ак.ч.**	**360**	**180**	**180**
	зач.ед.	**10**	**5**	**5**

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	Основы программно-аппаратных средств защиты информации	1.1	**Назначение, задачи и базовые механизмы программно-аппаратной защиты информации.** Цели и задачи программно-аппаратной защиты информации. Критерии оценки информационной безопасности объектов автоматизации. Идентификация, аутентификация, авторизация, разграничение и контроль доступа. Защита сетевых файловых ресурсов и управление доступом средствами ОС.	ЛК, ЛР
		1.2	**Криптографические и специализированные аппаратные средства защиты.** Симметричные и асимметричные криптосистемы, хэш-функции, электронная подпись. Криптографические сопроцессоры, специализированные компьютерные системы безопасности, электронные ключи, RFID, смарт-карты, APDU, защищенная передача данных и аппаратные компоненты криптозащиты.	ЛК, ЛР
Раздел 2	Программно-аппаратные средства защиты информации	2.1	**Сетевые программно-аппаратные средства защиты информации.** Безопасность открытых сетей и межсетевого взаимодействия. Межсетевые экраны, маршрутизаторы, шлюзы, VPN, IPsec, инфраструктура открытых ключей, цифровые сертификаты. Системы обнаружения и предупреждения вторжений, методы их обхода и тестирования.	ЛК, ЛР
		2.2	**Защита программного обеспечения, встроенных систем и развитие ПАСЗИ.** Защита ПО от несанкционированной загрузки, копирования, отладки и дизассемблирования. Защита встроенных систем, мобильных и беспроводных сетей. Управление рисками, аудит информационной безопасности, современные системы и перспективы развития программно-аппаратных средств защиты 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), операционные системы Debian Linux (свободно-распространяемое ПО), pfSense Community Edition (свободно-распространяемое ПО), Kali Linux (свободно-распространяемое ПО), межсетевой экран Netfilter (свободно-распространяемое ПО), системы обнаружения/предотвращения вторжений Suricata, Snort (свободно распространяемое ПО), SIEM-система Security Onion (свободно-распространяемое ПО), средства для работы с электронной подписью GnuPG, DSS, Surguch, openCryptoki (свободно-распространяемое ПО), пакет шифрования VeraCrypt (свободно-распространяемое ПО), эмулятор системы пожарной сигнализации Prometheus Fire Alarm System (свободно-распространяемое ПО), киберполигон Ampire.

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), операционные системы Debian Linux (свободно-распространяемое ПО), pfSense Community Edition (свободно-распространяемое ПО), Kali Linux (свободно-распространяемое ПО), межсетевой экран Netfilter (свободно-распространяемое ПО), системы обнаружения/предотвращения вторжений Suricata, Snort (свободно распространяемое ПО), SIEM-система Security Onion (свободно-распространяемое ПО), средства для работы с электронной подписью GnuPG, DSS, Surguch, openCryptoki (свободно-распространяемое ПО), пакет шифрования VeraCrypt (свободно-распространяемое ПО), эмулятор системы пожарной сигнализации Prometheus Fire Alarm System (свободно-распространяемое ПО), киберполигон Ampire.
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. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584673 (дата обращения: 26.03.2026).

2. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1865598 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

Дополнительная литература:

1. Программно-аппаратные средства защиты информации : учебное пособие : в 3 частях / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2024. – Часть 3. – 82 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=723472 (дата обращения: 26.03.2026). – Библиогр. в кн. – ISBN 978-5-8265-2795-5 (ч. 3). – ISBN 978-5-8265-2464-0. – Текст : электронный.

2. Программно-аппаратные средства защиты информации : учебное пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. - Новосибирск : Изд-во НГТУ, 2023. - 80 с. - ISBN 978-5-7782-4905-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2246196 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

3. Шевцов, В. Ю. Программно-аппаратная защита локальных АРМ с использованием ПО Secret Net : учебно-методическое пособие / В. Ю. Шевцов, Е. В. Булгакова. - Москва ; Вологда : Инфра-Инженерия, 2024. - 80 с. - ISBN 978-5-9729-1918-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169714 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

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 «Программно-аппаратные средства защиты информации».

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

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой информационной безопасности		Царегородцев А.В.
Должность	*Подпись*	*Фамилия И.О*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой информационной безопасности		Царегородцев А.В.
Должность	*Подпись*	*Фамилия И.О*

РАЗРАБОТЧИКИ:

Заведующий кафедрой информационной безопасности		Царегородцев А.В.
Должность	*Подпись*	*Фамилия И.О*