

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 26.05.2026 17:36:21

Уникальный программный ключ:

ca953a0120d891083f939673076ef1a989aae18a

Федеральное государственное автономное образовательное учреждение высшего образования

«Российский университет дружбы народов имени Патриса Лумумбы»

Факультет физико-математических и естественных наук

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

02.03.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

(код и наименование направления подготовки/специальности)

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

ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы информационной безопасности» входит в программу бакалавриата «Фундаментальная информатика и информационные технологии» по направлению 02.03.02 «Фундаментальная информатика и информационные технологии» и изучается в 4 семестре 2 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 3 разделов и 8 тем и направлена на изучение основных уязвимостей операционных систем; защиты компьютерных сетей.

Целью освоения дисциплины является введение учащихся в предметную область защиты современных систем и сетей телекоммуникаций.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы информационной безопасности» 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)
ОПК-5	Способен устанавливать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	ОПК-5.1 Знает методику установки и администрирования информационных систем и баз данных. Знаком с содержанием Единого реестра российских программ; ОПК-5.2 Умеет реализовывать техническое сопровождение информационных систем и баз данных; ОПК-5.3 Имеет практические навыки установки и инсталляции программных комплексов, применения основ сетевых технологий;
ПК-3	Способен осуществлять администрирование прикладного программного обеспечения, сетевой подсистемы и систем управления базами данных инфокоммуникационной системы организации	ПК-3.1 Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем и сетевых подсистем инфокоммуникационной системы организации; методику установки и администрирования программных систем и сетевых подсистем инфокоммуникационной системы организации; ПК-3.2 Умеет настраивать и администрировать программные системы, сетевые подсистемы и базы данных инфокоммуникационной системы организации; ПК-3.3 Имеет практический опыт эксплуатации и администрирования программных систем, сетевых подсистем и баз данных инфокоммуникационной системы организации;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы информационной безопасности» 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 «Основы информационной безопасности».

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-5	Способен устанавливать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	Архитектура компьютеров и операционные системы;	Реляционные базы данных; Системы управления базами данных; Кибербезопасность предприятия;
ПК-3	Способен осуществлять администрирование прикладного программного обеспечения, сетевой подсистемы и систем управления базами данных инфокоммуникационной системы организации	Архитектура компьютеров и операционные системы;	Преддипломная практика; Сетевые технологии; Администрирование сетевых подсистем; Администрирование локальных сетей; Моделирование сетей передачи данных; Машинное обучение в телекоммуникациях; Основы теории систем; Реляционные базы данных; Системы управления базами данных; Кибербезопасность предприятия;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Основы информационной безопасности» 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)
			4
<i>Контактная работа, ак.ч.</i>	54		54
Лекции (ЛК)	18		18
Лабораторные работы (ЛР)	36		36
Практические/семинарские занятия (СЗ)	0		0
<i>Самостоятельная работа обучающихся, ак.ч.</i>	63		63
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	27		27
Общая трудоемкость дисциплины	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		Содержание темы	Вид учебной работы*
Раздел 1	Основы безопасности сетевых информационных технологий	1.1	Общая проблематика информационной безопасности	Базовые понятия: информация, информационная безопасность (ИБ), основные свойства (конфиденциальность, целостность, доступность --- триада CIA). Рассматриваются виды угроз (естественные, техногенные, преднамеренные), уязвимости, риски и методы их оценки. Обсуждаются субъекты (владельцы информации, пользователи, нарушители) и объекты защиты (аппаратные, программные, данные, каналы связи). Анализируются нормативно-правовые аспекты (законы, стандарты, политики безопасности). Вводится понятие системы защиты информации (СЗИ) и принципы её построения (эшелонированность, минимизация привилегий, непрерывность).	ЛК, ЛР
		1.2	Хакерские атаки	Классификация атаки по цели, источнику, воздействию. Рассматриваются этапы жизненного цикла атаки: разведка (сбор информации, сканирование портов, OSINT), проникновение (эксплуатация уязвимостей), закрепление (бэкдоры, руткиты), развитие (повышение привилегий, латеральное перемещение), маскировка (чистка логов, шифрование), достижение цели (кража, порча, шифрование данных). Изучаются социальная инженерия (фишинг, претекстинг, кви про кво), атаки «отказ в обслуживании» (DoS/DDoS), атаки типа «человек посередине» (MitM), ARP-spoofing, DNS-spoofing, сниффинг, спуфинг.	ЛК, ЛР
		1.3	Угрозы сетевой безопасности	Уязвимости сетевых протоколов и технологиям защиты. Рассматриваются угрозы на канальном уровне (MAC-флудинг, CAM-атаки, VLAN hopping), сетевом уровне (IP-спуфинг, ICMP-атаки (smurf, ping flood), маршрутизационные атаки (RIP, OSPF, BGP hijacking)), транспортном уровне (TCP SYN flood, TCP RST, сессионный хайджек, UDP flood), прикладном уровне (DNS-амплификация, HTTP-атаки, SMTP-спам). Обсуждаются средства противодействия: сегментация сетей (VLAN, DMZ), системы обнаружения вторжений (IDS/IPS), фильтрация трафика, применение защищённых протоколов (SSH, TLS,	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				IPsec), технологии DNSSEC, BGPsec.	
		1.4	Административная защита сетей	Организационно-административные меры обеспечения сетевой безопасности. Рассматриваются политики безопасности (Acceptable Use Policy, политика паролей, удалённого доступа), управление доступом на основе ролей (RBAC), управление учётными записями и привилегиями. Изучаются методы защиты периметра: межсетевые экраны (firewall), прокси-серверы, шлюзы безопасности, DMZ. Обсуждаются системы централизованного мониторинга (SIEM), управления событиями и реагирования на инциденты (SOC). Вводятся процедуры аудита, резервного копирования, восстановления после сбоя, а также требования к физической защите сетевого оборудования.	ЛК, ЛР
Раздел 2	Защита информации в современных операционных системах	2.1	Критерии безопасности информационных систем	Стандарты и методологии оценки безопасности ИС. Рассматриваются «Оранжевая книга» (TCSEC): классы А, В, С, D, требования к дискреционному и мандатному контролю. Изучаются международные стандарты ISO/IEC 15408 (Common Criteria) --- функциональные и гарантийные требования (EAL1-EAL7). Вводятся российские руководящие документы Гостехкомиссии (классы защищённости СВТ, АС). Обсуждаются стандарты управления ИБ: ISO/IEC 27001 (система менеджмента ИБ), ГОСТ Р ИСО/МЭК 27001. Анализируются профили защиты, задания по безопасности, методики аттестации и сертификации.	ЛК, ЛР
		2.2	Формальные модели безопасности ОС	Математические модели управления доступом. Рассматривается дискреционная модель (HRU, Take-Grant) --- доступ субъекта к объекту на основе матрицы прав. Изучается мандатная модель Белла --- Лападулы (многоуровневая защита, свойство простой и звёздной безопасности, невозможность понижения уровня). Вводится модель Кларка --- Уилсона (целостность, разделение обязанностей, транзакции). Обсуждается модель Китайская стена (китайская стена) для предотвращения конфликта интересов. Анализируются ролевая модель (RBAC) и модель Биба (целостность, правила «не писать вверх», «не читать вниз»). Приводятся примеры реализации в SELinux, AppArmor, FreeBSD.	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 3	Программная защита	3.1	Основы криптографии	Базовые понятия криптографии: шифрование, дешифрование, ключ, криптостойкость. Рассматриваются симметричные алгоритмы (блочные --- AES, DES, ГОСТ 28147-89; поточные -- - RC4, Salsa20), режимы шифрования (ECB, CBC, CTR, GCM). Изучаются асимметричные алгоритмы (RSA, ECC, Диффи --- Хеллмана) --- открытый и закрытый ключи, электронная подпись. Вводятся хеш-функции (MD5, SHA-1, SHA-256, ГОСТ Р 34.11-2012), их свойства (однаправленность, устойчивость к коллизиям). Обсуждаются протоколы распределения ключей, инфраструктура открытых ключей (PKI), сертификаты X.509, протокол TLS/SSL.	ЛК, ЛР
		3.2	Программные уязвимости	Классификация типичных уязвимостей программного обеспечения. Рассматриваются переполнение буфера (стековое и кучевое), переполнение целочисленного типа, гонка состояний (race condition), небезопасная работа с памятью (use-after-free, double free), форматные строки (format string attack), SQL-инъекции, межсайтовый скриптинг (XSS), CSRF, инъекции команд ОС (command injection). Изучаются методы эксплуатации: шеллкод, ROP (Return-Oriented Programming), возврат в libc, bypass ASLR, DEP, Stack Canary. Обсуждаются средства выявления уязвимостей: статический и динамический анализ, фаззинг, тестирование на проникновение (pentest).	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.	Компьютер/ноутбук с доступом к сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, Яндекс Телемост или аналог.
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенный персональными компьютерами (в количестве 20 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	ОС Linux/ Windows, Python, Julia. Дополнительное ПО: офисный пакет MS Office или LibreOffice, OBS Studio.
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.	ОС Linux/ Windows, Python, Julia. Дополнительное ПО: офисный пакет MS Office или LibreOffice, OBS Studio.

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2016. — 452 с.

2. Мэйволд Э. Безопасность сетей. Эком, 2016 г., 528 с. — <http://www.intuit.ru/department/security/netsec/>

Дополнительная литература:

1. Шумский А. А. Системный анализ в защите информации. — Учебное пособие для вузов. — М.: Гелиос АРВ, 2005. — 224 с.

2. Полянская О.Ю., Горбатов В.С. Инфраструктуры открытых ключей. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий — ИНТУ-ИТ.ру, 2007. — <http://www.intuit.ru/department/security/pki/>

3. Галатенко В. А. Основы информационной безопасности. Интернет-университет информационных технологий — ИНТУИТ.ру, 2008 г., 208 с. — <http://www.intuit.ru/department/security/secbasics/>

4. Галатенко В.А. Стандарты информационной безопасности. Интернет-

университет информационных технологий — ИНТУИТ.ру, 2005. —

<http://www.intuit.ru/department/security/secst/>

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/>

- Научометрическая база данных Lens.org <https://www.lens.org>

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

1. Курс лекций по дисциплине «Основы информационной безопасности».

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

РАЗРАБОТЧИК:

Профессор кафедры теории
вероятностей и
кибербезопасности

Должность, БУП

Подпись

Кулябов Дмитрий
Сергеевич

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории
вероятностей и
кибербезопасности

Должность БУП

Подпись

Самуйлов Константин
Евгеньевич

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории
вероятностей и
кибербезопасности

Должность, БУП

Подпись

Самуйлов Константин
Евгеньевич

Фамилия И.О.