Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов имени Патриса Лумумбы»

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И КОМПЬЮТЕРНЫХ СЕТЕЙ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА
(код и наименование направления подготовки/специальности)

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

МАТЕМАТИЧЕСКИЕ МЕТОДЫ МЕХАНИКИ КОСМИЧЕСКОГО ПОЛЕТА И АНАЛИЗА ГЕОИНФОРМАЦИОННЫХ ДАННЫХ
(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы разработки безопасного программного обеспечения и компьютерных сетей» входит в программу бакалавриата «Математические методы механики космического полета и анализа геоинформационных данных» по направлению 01.03.02 «Прикладная математика и информатика» и изучается в 7 семестре 4 курса. Дисциплину реализует Кафедра механики и процессов управления. Дисциплина состоит из 3 разделов и 8 тем и направлена на изучение the basic principles, methods and technologies used to create secure computer systems and protect them from external and internal threats. This course provides a comprehensive study of the aspects of developing a secure software and hardware environment, methods of cryptographic information protection, network protocols and technologies, as well as issues of personal data protection and secure information storage.

Целью освоения дисциплины является to introduce students to modern methods and technologies for protecting computer systems from threats related to unauthorized access, malware, theft of confidential information and other types of cyber attacks.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы разработки безопасного программного обеспечения и компьютерных сетей» 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)
ПК-5	Способен разрабатывать, отлаживать, проверять работоспособность, модифицировать программное обеспечение; применять методы и средства проектирования программного обеспечения, разрабатывать и согласовывать программную документацию на программное обеспечение	ПК-5.1 Знает существующее системное и прикладное программное обеспечение, методы проектирования и разработки программного обеспечения, структур и баз данных, программных интерфейсов. Знает нормативно-техническую документацию для разработки программной документации на ПО; ПК-5.2 Умеет применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов. Умеет анализировать нормативно-техническую документацию для разработки программной документации на ПО; ПК-5.3 Владеет основными навыками технологиями разработки, отладки, проверки работоспособности и модификации системного прикладного программного обеспечения, модернизации технических решений по разработке ПО;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы разработки безопасного программного обеспечения и компьютерных сетей» относится к части, формируемой участниками образовательных отношений 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 разработки безопасного программного обеспечения и компьютерных сетей».

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

Шифр	**Наименование компетенции**	**Предшествующие дисциплины/модули, практики***	**Последующие дисциплины/модули, практики***
ПК-5	Способен разрабатывать, отлаживать, проверять работоспособность, модифицировать программное обеспечение; применять методы и средства проектирования программного обеспечения, разрабатывать и согласовывать программную документацию на программное обеспечение	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Технологическая практика; Анализ геоинформационных данных; Информатика и программирование; *Архитектура компьютерных сетей***; *Architecture of Computer Networks***;	Преддипломная практика; Технологическая практика;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Основы разработки безопасного программного обеспечения и компьютерных сетей» составляет «3» 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)**
			7
Контактная работа, ак.ч.	*54*		*54*
Лекции (**ЛК**)	36		36
Лабораторные работы (**ЛР**)	18		18
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*54*		*54*
Контроль (экзамен/зачет с оценкой), ак.ч.	*0*		*0*
Общая трудоемкость дисциплины	**ак.ч.**	***108***	*108*
	зач.ед.	***3***	*3*

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	Secure Software and Computer Networks	1.1	Principles of Secure Software Development and Design	Basic principles of software development with security requirements: security by default (most strict settings initially); least privilege (granting only necessary rights); defense in depth (multiple lines of defense); separation of duties; fail secure; complete mediation (checking every request). Lifecycle stages of secure software: threat analysis, security design, implementation with vulnerability checking, security testing, maintenance and updates.	ЛК
		1.2	Types of Security Threats in Computer Networks and Protection Against Them.	Classification of network threats: traffic interception (eavesdropping); data modification (man-in-the-middle attack); denial of service (DoS/DDoS attacks); unauthorized access to devices; malware distribution (worms, Trojans); phishing attacks. Protection methods: communication channel encryption; firewalls; intrusion detection and prevention systems (IDS/IPS); network segmentation; regular software updates; user training.	ЛК
		1.3	Information Encryption Methods and System Security Assessment.	Symmetric encryption: one key for encryption and decryption (e.g., block ciphers and stream ciphers). Asymmetric encryption: a key pair – public key (for encryption) and private key (for decryption). Hashing: producing a fixed-length “digest” of data (checksum) to verify integrity. Digital signature: a combination of hashing and asymmetric encryption to authenticate identity and authorship. System security assessment: threat analysis, attack modeling, penetration testing, source code vulnerability analysis.	ЛК
Раздел 2	Network Connection Security Protocols and Data Protection Methodologies When Working with Networks	2.1	Configuring and Transferring Data Using FTP – FTPS.	File Transfer Protocol (FTP): purpose and working principle. Vulnerabilities of standard FTP: transmission of login, password, and data in plaintext. Secure FTP (FTPS): adding an encryption layer using TLS/SSL protocols. FTPS operation modes: explicit (explicit security negotiation) and implicit (security from the start). Configuring an FTPS server and client: installing certificates, selecting modes, configuring ports.	ЛР
		2.2	Configuring and Transferring Data Using HTTP – HTTPS.	Hypertext Transfer Protocol (HTTP): basic operation. Threats to HTTP traffic: data interception, page spoofing, malicious code injection. Secure HTTP (HTTPS): using TLS/SSL encryption over	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				HTTP. Obtaining and installing certificates: certificate authorities (CA), self-signed certificates. How HTTPS works: handshake, key exchange, session encryption. Indicators of a secure connection in browsers (padlock, green address bar).	
		2.3	Basic Principles of User Authentication and Authorization in a System.	Authentication: verifying a user's identity (who claims to be whom). Authentication factors: knowledge (password, PIN); possession (smart card, token, phone); biometrics (fingerprint, face, voice). Multi-factor authentication: using two or more factors. Authorization: determining access rights after successful authentication (what the user is allowed to do). Access control models: discretionary (access matrix), mandatory (clearance levels), role-based (permissions based on user role). User accounts, groups, password policies.	ЛК
Раздел 3	Information Security Organization Rules and Protection Against Cyberattacks	3.1	System Vulnerability Assessment.	Concept of a vulnerability as a flaw (error) in a system that can be exploited by an attacker. Types of vulnerabilities: software errors (buffer overflow, uncontrolled input); configuration errors (default passwords, open ports); architectural flaws. Vulnerability scanning: using automated tools (scanners) to find known vulnerabilities. Criticality assessment using scales (e.g., CVSS – Common Vulnerability Scoring System). Prioritizing vulnerability remediation.	ЛК
		3.2	Conducting Penetration Testing (Pentesting).	Penetration testing as a controlled simulation of an attacker's actions to assess the real security of a system. Stages of a penetration test: information gathering about the target (reconnaissance); vulnerability analysis and discovery; vulnerability exploitation (attempting to breach); system persistence (simulating consequences); results report (description of found vulnerabilities, risk level, remediation recommendations). Types of pentesting: black box (no prior information), gray box (partial information), white box (full knowledge of the target). Legal and ethical aspects of pentesting: requirement for written authorization.	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.	
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве ____ шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	
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.	

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. "Computer Networking: A Top-Down Approach" by James Kurose and Keith Ross.
2. "Cryptography Engineering: Design Principles and Practical Applications" by Bruce Schneier, Niels Ferguson, and Tadayoshi Kohno.
3. "Securing the Clicks Network Security in the Age of Social Media" by Gary Bahadur, Jason Inasi, and Alex de Carvalho.
4. "Threat Modeling: Designing for Security" by Adam Shostack

Дополнительная литература:

1. "Building Secure Software: How to Avoid Security Problems the Right Way" by John Viega and Gary McGraw.
2. Network Security Essentials: Applications and Standards" by William Stallings.
3. "Intelligent Networked Teleoperation Control" by Xiaodong Liu and Muhammad Ilyas.

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 http://lib.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 «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/
- поисковая система Яндекс https://www.yandex.ru/
- поисковая система Google https://www.google.ru/
- реферативная база данных SCOPUS http://www.elsevierscience.ru/products/scopus/

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

1. Курс лекций по дисциплине «Основы разработки безопасного программного обеспечения и компьютерных сетей».

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

РАЗРАБОТЧИК:

Доцент		Варфоломеев Александр Алексеевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой		Разумный Юрий Николаевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Профессор		Разумный Юрий Николаевич
Должность, БУП	*Подпись*	*Фамилия И.О.*