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 ЗАЩИЩЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И КОМПЬЮТЕРНЫХ СЕТЕЙ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

27.03.04 УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

(код и наименование направления подготовки/специальности)

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

DATA ENGINEERING, ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ И КИБЕРБЕЗОПАСНОСТЬ

(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы разработки защищенного программного обеспечения и компьютерных сетей» входит в программу бакалавриата «Data Engineering, интеллектуальные системы и кибербезопасность» по направлению 27.03.04 «Управление в технических системах» 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 основных принципов, методов и технологий, используемых для создания безопасных компьютерных систем и защиты их от внешних и внутренних угроз. В рамках данного курса дается комплексное изучение аспектов разработки безопасной программной и аппаратной среды, методов криптографической защиты информации, сетевых протоколов и технологий, а также вопросов защиты персональных данных и безопасного хранения информации.

Целью освоения дисциплины является знакомство слушателей с современными методами и технологиями обеспечения защиты компьютерных систем от угроз, связанных с несанкционированным доступом, вредоносным ПО, кражей конфиденциальной информации и другими видами кибератак.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы разработки защищенного 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-10	Способен применять информационные технологии, соблюдать основные требования информационной безопасности	ПК-10.1 Знает основные подходы и методы сбора и анализа исходных данных для расчета и проектирования систем и средств автоматизации и управления; ПК-10.2 Владеет современными информационными технологиями для расчета и проектирования систем и средств автоматизации и управления; ПК-10.3 Умеет применять информационные технологии в профессиональной деятельности, соблюдать основные требования информационной безопасности;
ПК-7	Способен разрабатывать и анализировать проектные решения по обеспечению кибербезопасности автоматизированных систем	ПК-7.1 Знает основные подходы к разработке проектных решений по обеспечению кибербезопасности информационных систем; ПК-7.2 Умеет анализировать проектные решения на предмет обеспечения кибербезопасности; ПК-7.3 Владеет техниками реализации проектных решений, обеспечивающих кибербезопасность автоматизированных систем;
ПК-8	Способен организовать производственно-технологическую поддержку процессов создания, совершенствования и сопровождения информационных систем, автоматизирующих задачи организационного и производственного управления	ПК-8.1 Знает основные производственно-технологические этапы процесса создания, совершенствования и сопровождения информационных систем, предназначенных для автоматизации задач управления; ПК-8.2 Умеет организовывать основные производственные и технологические этапы создания информационных систем, автоматизирующих задачи организационного и производственного управления; ПК-8.3 Владеет методами и подходами для организации производственно-технологической поддержки процессов создания, совершенствования и сопровождения информационных систем;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы разработки защищенного программного обеспечения и компьютерных сетей» 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 разработки защищенного 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-10	Способен применять информационные технологии, соблюдать основные требования информационной безопасности	Основы информационной безопасности и киберустойчивости; Технологическая практика (учебная);	Проектная практика; Преддипломная практика;
ПК-7	Способен разрабатывать и анализировать проектные решения по обеспечению кибербезопасности автоматизированных систем	Основы информационной безопасности и киберустойчивости; Основы технологических угроз и кибербезопасности;	Проектная практика;
ПК-8	Способен организовать производственно-технологическую поддержку процессов создания, совершенствования и сопровождения информационных систем, автоматизирующих задачи организационного и производственного управления		

* - 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 защищенного программного обеспечения и компьютерных сетей» составляет «6» 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)**
			7
Контактная работа, ак.ч	*72*		*72*
Лекции (**ЛК**)	36		36
Лабораторные работы (**ЛР**)	36		36
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*117*		*117*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины ак.ч.	**ак.ч.**	**216**	**216**
	зач.ед.	**6**	**6**

Общая трудоемкость дисциплины «Основы разработки защищенного программного обеспечения и компьютерных сетей» составляет «6» зачетных единиц.

Таблица 4.2. Виды учебной работы по периодам освоения образовательной программы высшего образования для заочной формы обучения.

Вид учебной работы	**ВСЕГО, ак.ч.**		**Семестр(-ы)**	**Семестр(-ы)**
			8	**9**
Контактная работа, ак.ч	*40*		*20*	*20*
Лекции (**ЛК**)	20		10	10
Лабораторные работы (**ЛР**)	20		10	10
Практические/семинарские занятия (**СЗ**)	0		0	0
Самостоятельная работа обучающихся, ак.ч.	*163*		*84*	*79*
Контроль (экзамен/зачет с оценкой), ак.ч.	*13*		*4*	*9*
Общая трудоемкость дисциплины ак.ч.	**ак.ч.**	**216**	**108**	**108**
	зач.ед.	**6**	**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	Защищенное программное обеспечение и компьютерные сети	1.1	Принципы разработки и проектирования защищенного программного обеспечения.	Основные принципы создания программного обеспечения с учётом требований безопасности: безопасность по умолчанию (наиболее строгие настройки изначально); минимизация привилегий (предоставление только необходимых прав); эшелонированная защита (несколько рубежей обороны); разделение обязанностей; защита отказоустойчивости; полное посредничество (проверка всех запросов). Этапы жизненного цикла защищённого программного обеспечения: анализ угроз, проектирование защиты, реализация с проверкой на уязвимости, тестирование безопасности, сопровождение и обновления.	ЛК
		1.2	Виды угроз безопасности в компьютерных сетях и защита от них	Классификация сетевых угроз: перехват трафика (прослушивание); модификация данных (атака «человек посередине»); отказ в обслуживании (DoS/DDoS-атаки); несанкционированный доступ к устройствам; распространение вредоносного программного обеспечения (черви, трояны); фишинговые атаки. Методы защиты: шифрование каналов связи; межсетевые экраны (фаерволы); системы обнаружения и предотвращения вторжений (IDS/IPS); сегментация сети; регулярное обновление программного обеспечения; обучение пользователей.	ЛК
		1.3	Методы шифрования информации и оценка безопасности системы	Симметричное шифрование: один ключ для шифрования и расшифрования (примеры: алгоритмы на основе блоков и потоковые шифры). Асимметричное шифрование: пара ключей – открытый (для шифрования) и закрытый (для расшифрования). Хеширование: получение фиксированной «свёртки» данных (контрольной суммы) для проверки целостности. Электронная подпись: комбинация хеширования и асимметричного шифрования для подтверждения подлинности и авторства. Оценка безопасности системы: анализ угроз, моделирование атак, тестирование на проникновение, анализ кода на наличие уязвимостей.	ЛК
Раздел 2	Протоколы защиты сетевых соединений и методологии защиты данных при работе с сетью.	2.1	Настройка и передача данных по протоколу FTP-FTPS	Протокол передачи файлов (FTP): назначение, принцип работы. Уязвимости стандартного FTP: передача логина, пароля и данных в открытом виде. Защищённый FTP (FTPS): добавление уровня шифрования с помощью протоколов TLS/SSL. Режимы работы FTPS: явный (явное согласование защиты) и неявный (защита с самого начала). Настройка сервера и клиента FTPS: установка сертификатов, выбор режимов, настройка портов.	ЛК, ЛР
		2.2	Настройка и передача данных по протоколу HTTP-HTTPS	Протокол передачи гипертекста (HTTP): основы работы. Угрозы для HTTP-трафика: перехват данных, подмена страниц, внедрение вредоносного кода. Безопасный HTTP (HTTPS): использование шифрования TLS/SSL поверх HTTP. Получение и установка сертификатов: центры сертификации (Certificate Authority), самоподписанные сертификаты. Принцип работы HTTPS: рукопожатие (handshake), обмен ключами, шифрование сеанса. Индикаторы защищённого соединения в браузере (замок, зелёная строка).	ЛР
		2.3	Основные принципы аутентификации и авторизации пользователей в системе	Аутентификация: проверка подлинности пользователя (кто заявляет, что он тот, за кого себя выдаёт). Факторы аутентификации: знание (пароль, PIN-код); владение (смарт-карта, токен, телефон); биометрия (отпечаток пальца, лицо, голос). Многофакторная аутентификация: использование двух и более факторов. Авторизация:	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				определение прав доступа после успешной аутентификации (что разрешено делать пользователю). Модели управления доступом: избирательная (матрица прав), мандатная (уровни допуска), ролевая (права на основе роли пользователя). Учётные записи, группы, политики паролей.	
Раздел 3	Правила организации информационной безопасности и защита от кибератак	3.1	Оценка уязвимости системы	Понятие уязвимости как недостатка (ошибки) в системе, который может быть использован злоумышленником. Типы уязвимостей: программные ошибки (переполнение буфера, неконтролируемый ввод); конфигурационные ошибки (стандартные пароли, открытые порты); архитектурные недостатки. Сканирование уязвимостей: использование автоматизированных средств (сканеров) для поиска известных уязвимостей. Оценка критичности уязвимостей по шкалам (например, CVSS – Common Vulnerability Scoring System). Приоритизация устранения уязвимостей.	ЛК
		3.2	Проведение тестирования на проникновение	Тестирование на проникновение как контролируемая имитация действий злоумышленника для оценки реальной защищённости системы. Этапы пентеста: сбор информации о цели (разведка); анализ и обнаружение уязвимостей; эксплуатация уязвимостей (попытка проникновения); закрепление в системе (имитация последствий); отчёт о результатах (описание найденных уязвимостей, уровень риска, рекомендации по устранению). Типы пентеста: «чёрный ящик» (без предварительной информации), «серый ящик» (с частичной информацией), «белый ящик» (с полной информацией об объекте). Правовые и этические аспекты пентеста: необходимость письменного разрешения.	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 14 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 защищенного программного обеспечения и компьютерных сетей».

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

РАЗРАБОТЧИКИ

Доцент	Варфоломеев А.А.
Должность	Фамилия И.О

РУКОВОДИТЕЛЬ БУП

Заведующий кафедрой	Разумный Ю.Н.
Должность	Фамилия И.О

РУКОВОДИТЕЛЬ ОП ВО

Профессор	Разумный Ю.Н.
Должность	Фамилия И.О