

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЛГПУ»)**

Структурное подразделение Институт физико-математического
образования, информационных и обслуживающих технологий
Кафедра информационных образовательных технологий и систем

УТВЕРЖДАЮ

Директор ИФМОИОТ

Е.Е. Горбенко

2023 г.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации

По направлению подготовки 44.03.01 Педагогическое образование

Профиль подготовки Компьютерные системы и образовательная
робототехника

Квалификация выпускника бакалавр

Форма обучения очная, заочная

Курс ОФО – 4 курс, ЗФО – 5 курс

Луганск, 2023

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы для подготовки бакалавров по направлению подготовки 44.03.01 Педагогическое образование очной и заочной форм обучения.

Рабочая программа учебной дисциплины разработана в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 44.03.01 «Педагогическое образование», утвержденным приказом Министерства образования и науки Российской Федерации от 22.02.2018 № 121 (с изменениями и дополнениями) и Профессиональным стандартом, утвержденным Приказом Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель)» от 08.10.2013 № 544н.

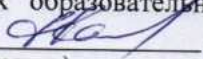
СОСТАВИТЕЛЬ:

доцент кафедры информационных образовательных технологий и систем, кандидат физико-математических наук, доцент Швыров Вячеслав Владимирович

Утверждена на заседании кафедры информационных образовательных технологий и систем

Протокол от «24» ноября 2023 г. №8

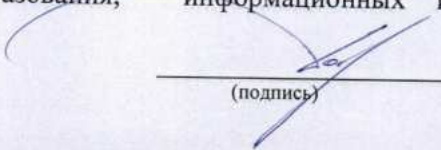
Заведующий кафедрой информационных образовательных технологий и систем


(подпись) Д.А. Капустин

Одобрена на заседании учебно-методической комиссии Института физико-математического образования, информационных и обслуживающих технологий


Протокол от «06» декабря 2023 г. №5

Председатель учебно-методической комиссии Института физико-математического образования, информационных и обслуживающих технологий


(подпись) О.В. Давыскиба

СОГЛАСОВАНО:

Заведующий учебно-методическим отделом


(подпись) В.В. Савенков

1. Цели и задачи дисциплины

Цели изучения дисциплины: изучение методов защиты информации, основных криптографических протоколов и схем, теоретических и прикладных вопросов обеспечения информационной безопасности.

Задачи:

- формирование профессиональных компетенций, позволяющих выполнять анализ и обеспечение безопасности информационных систем;
- изучение основных подходов для обеспечения целостности, доступности и конфиденциальности информации в компьютерных системах;
- формирование навыков безопасной работы в сети интернет;
- формирование базы знаний для самостоятельного решения задач в области защиты информации и решения прикладных задач.

–

2. Место дисциплины в структуре ОПОП

Учебная дисциплина «Защита информации» относится к базовой (обязательной) части учебного плана (Б1.О.07.06). Дисциплина реализуется кафедрой информационных образовательных технологий и систем (4) Институт физико-математического образования, информационных и обслуживающих технологий ФГБОУ ВО «ЛГПУ».

Необходимым условием для освоения учебной дисциплины являются знания принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности; умения решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности; навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности, а также навыками использования современных технологий разработки ПО.

Содержание дисциплины «Защита информации» является логическим продолжением содержания дисциплин «Алгоритмы и структуры данных», «Операционные системы» и основой для дальнейшего освоения дисциплин: написания разделов выпускной квалификационной работы.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Код по ФГОС ВО	Индикатор достижения	Результаты обучения по дисциплине
Универсальные		
Общепрофессиональные		
ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-9.2. Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности ОПК-9.3.	ОПК-9.1. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-9.2. Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности ОПК-9.3.
Профессиональные		
ПК-4. Способен разрабатывать требования и проектировать программное обеспечение, а также программно-аппаратные комплексы	ПК-4.1. Знать: методы и технологию анализа и проектирования требований к программному обеспечению процессов и систем с заданной структурой и функциональными свойствами ПК-4.2. Уметь: осуществлять разработку требований и проектирование технических заданий на разработку программного обеспечения программно-аппаратных комплексов ПК-4.3. Владеть: навыками разработки программного обеспечения технологических процессов обучающей организации	ПК-4.1. Знает: методы и технологию анализа и проектирования требований к программному обеспечению процессов и систем с заданной структурой и функциональными свойствами ПК-4.2. Умеет: осуществлять разработку требований и проектирование технических заданий на разработку программного обеспечения программно-аппаратных комплексов ПК-4.3. Владеет: навыками разработки программного обеспечения технологических процессов обучающей организации

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов (4 зач. ед.)
--------------------	--------------------------

	Очная форма	Заочная форма
Общая учебная нагрузка (всего)	144	144
Обязательная аудиторная учебная нагрузка (всего часов), в том числе:		
Лекции	24	6
Семинарские занятия		
Практические занятия		
Лабораторные работы	40	10
Курсовая работа / курсовой проект		
Другие формы организации учебного процесса (контрольные работы, индивидуальные занятия, консультации и др.)	27	9
Самостоятельная работа студента (всего)	53	119
Форма аттестация	Экзамен, зачет	Экзамен, зачет

4.2. Содержание дисциплины

Тема 1. Основы информационной безопасности

Основные понятия информационной безопасности. Конфиденциальность. Ценность информации. Целостность информации. Классификация информационных угроз. Методологии оценки угроз. Методики STRIDE и DREAD. Стандарты информационной безопасности.

Тема 2. Методы резервного копирования данных

Методы сжатия данных. Сжатие с потерями. Сжатие без потерь. Алгоритм Хаффмана. Защита информации в архивах. Технологии и уровни RAID. Зеркалирование. Технология чередования. Составные уровни RAID. Методы восстановления информации.

Тема 3. Методы аутентификации и авторизации

Понятие аутентификации и авторизации. Базовая аутентификация. Основные требования к паролям. Биометрическая аутентификация. Протоколы аутентификации. Форматы токенов аутентификации. Аутентификация в корпоративных сетях. Методы разграничения доступа.

Тема 4. Анализ и настройка безопасности в операционных системах семейства MS Windows

Использование командной строки. Основные системные утилиты. Брандмауэр Windows. Входящие и исходящие правила. Локальные политики безопасности. Групповые политики безопасности. Анализ безопасности. Шаблоны безопасности. Контроль над использованием сменных носителей. Черные и белые списки устройств.

Тема 5. Основы криптографической защиты информации

Основные понятия и определения. Криптография и криптоанализ. Классические криптосистемы. Шифр Сцигала. Магические квадраты. Шифр Трисемуса. Шифр Плейфера. Обзор современных криптосистем. Блочные шифры. Сеть Фейстеля. Применение сети Фейстеля в DES. Криптосистема RSA. Криптосистема AES. Современные хеш-функции.

Тема 6. Компьютерные вирусы

Понятие вируса. Классификация вирусов. Макровирусы. Загрузочные вирусы. Файловые вирусы. Троянские программы. Основные источники заражения вирусами. Методы внедрения руткитов. Методы профилактики. Современные клавиатурные шпионы. Общая модель аппаратного ввода. Методы внедрения шпионов. Методы обнаружения клавиатурных шпионов.

Тема 7. Основы сетевой безопасности

Понятие спама. Методы защиты от спама. Капча виды капчи. Графическая капча. Особенности защиты веб-ресурсов. Анализ уязвимостей с помощью утилиты Burp Suite. Защита от SQL-инъекций.

Тема 8. Основы захвата и анализа трафика

Понятие трафика. Захват трафика. Установка драйверов и системы захвата. Настройка параметров брандмауэра. Основные сетевые протоколы для захвата. Установка и настройка утилиты WireShark. Параметры захвата. Анализ протокола ICMP и команды ping.

Тема 9. Перехват трафика

Методы перехвата трафика. Утилита WireShark. Параметры фильтрации при захвате. Типы протоколов. Фильтрация по источнику. Фильтрация по назначению.

Тема 10. Анализ сетевых атак

Фильтрация по протоколу. Дейтаграмма. Структура кадра. Поля и атрибуты. Методы поиска в дампе трафика. Признаки сетевой атаки. Виды и анализ сетевых атак.

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
7 семестр / 13-14 триместр			
1	Тема 1. Основы информационной безопасности	4	2
2	Тема 2. Методы резервного копирования данных	4	2
3	Тема 3. Методы аутентификации и авторизации	2	2
4	Тема 4. Анализ и настройка безопасности в операционных системах семейства MS Windows	2	
5	Тема 5. Основы криптографической защиты информации	2	
6	Тема 6. Компьютерные вирусы	2	
7	Тема 7. Основы сетевой безопасности	2	
8	Тема 8. Основы захвата и анализа трафика	2	
9	Тема 9. Перехват трафика	2	
10	Тема 10. Анализ сетевых атак	2	
Итого:		24	6

4.4. Практические занятия

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
7 семестр / 13-14 триместр			
Итого:			

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
7 семестр / 13-14 триместр			
1	Защита информации в архивах	4	2
2	Настройка брандмауэра	4	2
3	Команды для администрирования системы	4	2
4	Локальные политики безопасности	4	2
5	Групповые политики	4	2
6	Анализ и настройка безопасности	4	
7	Шаблоны безопасности	4	
8	Классические криптосистемы	4	
9	Алгоритмы создания цифровых подписей	4	
10	Алгоритм RSA	2	
11	Основы сетевой безопасности	2	
Итого:		40	10

4.6. Самостоятельная работа студентов

№ п/п	Название раздела / темы	Вид самостоятельной работы	Объем часов	
			Очная форма	Заочная форма
7 семестр / 13-14 триместр				
1	Введение в информационной безопасности. Основные виды и источники атак на информацию. Основные понятия информационной безопасности.	Конспект лекций	10	24
2	Основные проблемы при разработке программного обеспечения. Средства защиты программ, основные мотивы и средства взлома программ.	Конспект лекций	10	24
3	Методы резервного дублирования информации. Существующие средства резервного дублирования информации.	Конспект лекций	10	24

4	RAID-технологии построения дисковых массивов различных уровней.	Конспект лекций	10	24
5	Контроль целостности информации. Основные алгоритмы контроля целостности.	Конспект лекций	13	23
Итого:			53	119

4.7. Курсовые работы / проекты

5. Методическое обеспечение, образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий.

Наряду с методикой традиционной лекционно-практической работы предусмотрено использование активных форм и методов учебной деятельности, в том числе: учебные дискуссии, беседы, мозговой штурм.

Методика проблемно-диалогического обучения применяется в процессе лекционной работы над учебным материалом в каждой из тем учебной дисциплины.

Методика обучения в сотрудничестве с применением командных, групповых видов работы используется в процессе организации лабораторных работ.

Методика исследовательской деятельности используется как основа для организации самостоятельной работы студентов в объеме учебных тем. Применяются средства мультимедиа: презентации, видео, базы ЭОР.

Информационные технологии: использование электронных образовательных ресурсов (электронный конспект, размещенный во внутренней сети или т.п.) при подготовке к лекциям, лабораторным работам и самостоятельной работе.

Работа в команде, проектная деятельность: совместная работа студентов в группе при выполнении лабораторных работ.

6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы в следующих формах: выполнение лабораторных работ; защита лабораторных работ.

Промежуточный контроль по результатам освоения дисциплины проходит в форме зачета (включает в себя ответ на теоретические вопросы и выполнение тестового задания).

Система оценивания учебных достижений студентов, оценочные средства представлены в фонде оценочных средств к рабочей программе учебной дисциплины (в приложении).

7. Учебно-методическое и программно-информационное обеспечение дисциплины

А) основная литература:

1. Барычев С.Г. Основы современной криптографии / С.Г. Барычев, Р.Е. Серов. – М. : Горячая линия – Телеком, 2002. – 152 с.
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М. : МЦНМО, 2003. – 326 с.
3. Глухих В.И. Информационная безопасность и защита данных: учебное пособие / В.И. Глухих. – Иркутск : Изд-во Иркутского государственного технического университета, 2011. – 250 с.
4. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. – М. : ТВП, 2001. – 254 с.
5. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии / А.В. Черемушкин – М. : МЦНМО, 2002. – 104~с.

Б) дополнительная литература:

1. Климов А.П. Реестр Windows 7 / А.П. Климов. – С-П. : Питер, 2010. – 325 с.
2. Романец Ю.В. Защита информации в компьютерных системах и сетях. / Ю.В. Романец, И.А. Тимофеев, В.Ф. Шаньгин. – М. : Радио и связь, 1999. – 328 с.
3. Складов Д.В. Искусство защиты и взлома информации / Д.В. Складов. – СПб.:БХВ-Петербург, 2004. – 288с.

В) Интернет-ресурсы:

8. Материально-техническое обеспечение дисциплины

Лекционные занятия: комплект электронных презентаций/слайдов, аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и т.п.

Лабораторные работы: компьютерный класс, оснащенный мультимедийным проектором, интерактивной доской, сетевой инфраструктурой и организованным доступом в Интернет, пакеты ПО MS Word, MS Excel , среда Visual Studio 2022.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет, рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде и т.п.

9. Лист дополнений и изменений

[illegible]