Государственное образовательное учреждение
«Приднестровский государственный университет
имени Т.Г. Шевченко»

Рыбницкий филиал
Кафедра информатики и программной инженерии

УТВЕРЖДАЮ
Директор Рыбницкого филиала
ПГУ им. Т.Г. Шевченко,
профессор _____ И.А. Павлинов
«26» 09 2023 г.

РАБОЧАЯ ПРОГРАММА

на 2023/2024 учебный год
Учебной ДИСЦИПЛИНЫ
«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки:
2.09.03.04 «Программная инженерия»

Профиль подготовки:
«Разработка программно-информационных систем»

квалификация (степень) выпускника
Бакалавр

Форма обучения:
очная

Год набора:
2020

Рыбница 2023

Рабочая программа дисциплины «Защита информации» разработана в соответствии с требованиями Государственного образовательного стандарта ВО по направлению подготовки 2.09.03.04 – «Программная инженерия», утвержденного приказом Министерства образования и науки Российской Федерации № 920 от 19 сентября 2017 года и основной профессиональной образовательной программы по профилю подготовки « Разработка программно-информационных систем».

Составитель рабочей программы:

Доцент, канд. техн. наук _____ (подпись) *Л.Я. Козак*

Рабочая программа утверждена на заседании кафедры *информатики и программной инженерии*

«21» сентября 2023 г. протокол № 2

Зав. выпускающей кафедрой

«21» 09 2023 г. _____ (подпись) *Л.А. Тягульская*

1. Цели и задачи освоения дисциплины

Цель освоения учебной дисциплины «Защита информации» – ознакомить студентов с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами; изучить методы идентификации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

Задачами освоения учебной дисциплины являются:

– иметь представление об использовании основных положений теории информационной безопасности в различных областях АСОИУ и иметь представление о направлении развития и перспективах защиты информации;

– знать правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в АСОИУ, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов;

– уметь применять методы защиты компьютерной информации при проектировании АСОИУ в различных предметных областях.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита информации» (Б1.В.12) относится к блоку 1 «Дисциплины», к части, формируемой участниками образовательных отношений Федерального государственного образовательного стандарта высшего образования по направлению подготовки 2.09.03.04 «Программная инженерия» (уровень бакалавриата).

Общая трудоемкость дисциплины составляет 3 зачетных единицы (108 часов).

Для освоения дисциплины «Защита информации» обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин: «Исследование операций», «Основы программирования» «Операционные системы», «Архитектура ЭВМ», «Введение в алгоритмы».

Компетенции, сформированные в процессе освоения дисциплины, необходимы при освоении последующих дисциплин, непосредственно связанных с современными информационными технологиями, при прохождении производственной и преддипломной практик, выполнении ВКРБ.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

Категория (группа) компетенций	**Код и наименование**	**Код и наименование индикатора достижения компетенции**
Общепрофессиональные компетенции и индикаторы их достижения		
Разработка и проектирование	**ОПК-3.** Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	ИД-1$_{ОПК-3.1.}$ Знать принципы, методы и средства анализа и структурирования профессиональной информации; ИД-2$_{ОПК-3.2.}$ Уметь анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров; ИД-3$_{ОПК-3.3.}$ Иметь навыки подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами.

4. *Структура и содержание дисциплины*

4.1. Распределение* трудоемкости в з.е./часах *по видам аудиторной и самостоятельной работы студентов по семестрам

Семестр	Количество часов						Форма итогового контроля
	Трудоемкость, з.е./часы	В том числе					
		Аудиторных				Самост. работа	
		Всего	Лекций	Лаб. раб.	Практич. занятия		
7	3/108	54	36	18	–	54	Зачет
Итого:	**3/108**	**54**	**36**	**18**	–	**54**	**Зачет**

4.2. Распределение видов учебной работы и их трудоемкости по модулям дисциплины

№ раз-дела	Наименование модулей	Количество часов				
		Всего	Аудиторная работа			Внеауд работа (СР)
			Л	ПЗ	ЛР	
1	Основы информационной безопасности. Основные понятия и определения. Политика государства в области информационной безопасности. Угрозы и нарушители безопасности информации	6	6	-	-	-
2	Исторический обзор криптографических методов защиты информации. Меры обеспечения защиты информации	12	4	-	-	8
3	Криптографические методы защиты информации. Стеганграфическая защита информации	28	8	-	8	12
4	Модель угроз безопасности информации. Методы контроля разграничения доступа. Организационные меры защиты информации	28	10	-	6	12
5	Техническая защита информации. Программно-технические методы защиты информации	22	4	-	-	18
6	Политика безопасности. Системы обнаружения и предотвращения компьютерных атак	12	4	-	4	4
	Итого:	**108**	**36**	**-**	**18**	**54**

4.3. Тематический план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно-наглядные пособия
Основы информационной безопасности. Основные понятия и определения. Политика государства в области информационной безопасности. Угрозы и нарушители безопасности информации				
1	1	2	Базовые направления криптографии: шифрование, кодирование и стеганография. Основные различия.	–
2		2	Стеганография. Подготовка и использование симпатических чернил, цифровая стеганография.	–

			Методы определения «присутствия» информации.	
3		2	Кодирование. Архивация - кодирование сжатием (методы Huffman, Lempel-Ziv, арифметические). Использование кодирования при передаче информации (методы Radix/Base64, UUE).	–
Итого по разделу часов:		*6*		
Исторический обзор криптографических методов защиты информации. Меры обеспечения защиты информации				
4	2	2	Древние методы шифрования. Шифры перестановок.	–
5		2	Древние методы шифрования. Шифры алфавитной замены. Статистические свойства языка. Вскрытие шифров алфавитной замены.	–
Итого по разделу часов:		*4*		
Криптографические методы защиты информации. Стеганграфическая защита информации				
6	3	2	Симметричные криптосистемы (алгоритмы DES, 3-DES, AES, ГОСТ-28147-89). Принципы работы, назначение.	раздаточный материал
7		2	Асимметричные криптосистемы (алгоритм RSA). Цифровая подпись. Пространство ключей.	раздаточный материал
8		2	Требования к современным криптографическим системам и алгоритмам.	–
9		2	Другие криптографические алгоритмы. Вычисление контрольных сумм (CRC) и хеширование (MD4/5, SHA).	–
Итого по разделу часов:		*8*		
Модель угроз безопасности информации. Методы контроля разграничения доступа. Организационные меры защиты информации				
10	4	2	Защита носителей информации (Floppy/HDD/CD/ DVD/Flash).	раздаточный материал
11		2	Защита программного обеспечения с помощью электронных ключей (LPT/COM/USB), HID-устройства, iButton.	–
12		2	Альтернативные методы защиты. Аутентификация по биометрическим данным (отпечаток пальца, геометрия руки, радужная оболочка глаза, сетчатка глаза, голосовая идентификация, геометрия лица, клавиатурный почерк).	–
13		2	Защита исходного кода программ – обфускация кода.	–
14		2	Вредоносное программное обеспечение как средство преодоления защиты информации.	–
Итого по разделу часов:		*10*		
Техническая защита информации. Программно-технические методы защиты информации				
15	5	2	Комплекс мер по защите информации. Разработка стратегии.	раздаточный материал
16		2	Организационные меры. Физическая, электромагнитная, активная и пассивная защита. Человеческий фактор.	–
Итого по разделу часов:		*4*		
Политика безопасности. Системы обнаружения и предотвращения компьютерных атак				

17	6	2	Основные моменты гражданского и уголовного кодексов ПМР в отношении защиты информации. Основные моменты Конституции ПМР в отношении защиты личной информации.	–
18		2	Способы подделки документов и методы выявления подделок.	–
Итого по разделу часов:		*4*		
Итого:		**36 часов**		

Лабораторные работы

№ п/п	№ раздела дисципли-ны	Объем часов	Тема практического занятия	Наимено-вание лаборатор.	Учебно-наглядные пособия
Криптографические методы защиты информации. Стеганграфическая защита информации					
1	3	2	Стеганография. Изготовление и использование симпатических чернил на основе молока, $NaHCO_3$, $FeCl_3$, $K_4[Fe(CN)_6]$ и др.	аудитория № 30	методич. пособие
2		2	Кодирование. Сравнение различных методов.	аудитория № 30	методич. пособие
3		2	Шифрование. Применение алгоритмов DES, 3DES, RSA для шифрования файлов.	аудитория № 30	методич. пособие
4		2	Контрольные суммы файлов. Реализация алгоритма подсчета CRC.	аудитория № 30	методич. пособие
Итого по разделу часов:		*8*			
Модель угроз безопасности информации. Методы контроля разграничения доступа. Организационные меры защиты информации					
8	4	2	Использование специализированного программного обеспечения для защиты пространства данных (создание виртуальных дисков).	аудитория № 30	методич. пособие
9		2	Использование электронных ключей для защиты программного обеспечения. Изучение продуктов фирмы KEYLOK.	аудитория № 30	методич. пособие
10		2	Защита программного обеспечения с помощью биометрических параметров (использование клавиатурного почерка).	аудитория № 30	методич. пособие
Итого по разделу часов:		*6*			
Политика безопасности. Системы обнаружения и предотвращения компьютерных атак					
16	6	2	Разработка динамической библиотеки с базовым набором криптографических средств. Методы шифрования и расшифрования сообщений.	аудитория № 30	методич. пособие
17		2	Разработка динамической библиотеки с базовым набором криптографических средств. Функции подсчета контрольных сумм, хеш-функции.	аудитория № 30	методич. пособие
Итого по разделу часов:		*4*			
Итого:		**18 часов**			

Самостоятельная работа обучающегося

Раздел дисциплины	№ п/п	Тема и вид самостоятельной работы обучающегося	Трудоемкость (в часах)
Исторический обзор криптографических методов защиты информации. Меры обеспечения защиты информации			
2	1	Криптографические протоколы: основные, промежуточные. *Работа с литературой*	4
	2	Криптографические протоколы: развитые, эзотерические. *Конспектирование*	4
		Итого по разделу часов:	*8*
Криптографические методы защиты информации. Стеганграфическая защита информации			
3	3	Информационная безопасность автоматизированных систем. *Подготовка сообщения*	4
	4	Самотестирующиеся и самокорректирующиеся программы. *Конспектирование*	4
	5	Конфиденциальные вычисления. *Работа с литературой*	4
		Итого по разделу часов:	*12*
Модель угроз безопасности информации. Методы контроля разграничения доступа. Организационные меры защиты информации			
4	6	Системы защиты информации. *Работа с литературой*	4
	7	Развитие теории и практики защиты информации. *Подготовка сообщения*	4
	8	Сетевая защита. *Работа с литературой*	4
		Итого по разделу часов:	*12*
Техническая защита информации. Программно-технические методы защиты информации			
5	9	Симметричные криптосистемы. *Работа с литературой*	2
	10	Шифр простой перестановки, магический квадрат. *Подготовка сообщения*	4
	11	Перестановка «Магический квадрат». *Конспектирование*	4
	12	Асимметричные криптосистемы. *Работа с литературой*	4
	13	Хакерские атаки, способы борьбы с ними. *Работа с литературой*	4
		Итого по разделу часов:	*18*
Политика безопасности. Системы обнаружения и предотвращения компьютерных атак			
6	14	Доктрина информационной безопасности ПМР. *Конспектирование*	4
		Итого по разделу часов:	*4*
Итого:			**54 часа**

5. *Перечень тем курсовых работ*

не предусмотрены

6. *Учебно-методическое и информационное обеспечение дисциплины*

6.1. Обеспеченность обучающихся учебниками, учебными пособиями

№ п\п	Наименование учебника, учебного пособия	Автор	Год изд-ия	Кол-во экземпляров	Эл. версия	Место размещения электронной версии
Основная литература						
1	Криптография, ее истоки и место в современном обществе	Винокуров А.	2021	3	+	http://www.library.ugatu.ac.ru/pdf

2	Криптография от папируса до компьютера	Жельников В.	2021	1	+	https://portal.tpu.ru/SHARED/k/KRETS/Trud/Tab3/Spisok.pdf
3	Введение в защиту информации в автоматизированных системах	Малюк А.А., Пазизин С.В., Погожин Н.С.	2023	1	+	http://window.edu.ru/resource/041/24041
4	Основы информационной безопасности: учебн. пособие для вузов	Белов Е.Б.	2021	1	+	http://window.edu.ru/resource/013/41013
Дополнительная литература						
5	Информационная безопасность	Мещеряков Р.В	2022	-	+	http://old.osp.ru/text/print/302/157830.html.
6	Защита информации в автоматизированных системах обработки данных	Герасименко В.А.	2020	2	+	https://portal.tpu.ru/SHARED/k/KRETS/Trud/Tab3/Spisok.pdf
7	Метод защиты арифметических вычислений в компьютерных системах	Насыпный В.В.	2021	1	+	https://www.twirpx.com/file/171197/
8	Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.	-	2022	1	+	http://www.gostehcom.ru
9	Безопасность информационных технологий	Периодич. Журнал	2020	1	+	http://www.aup.ru/books/m157
10	ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования		2019	3	+	https://www.libex.ru/detail/book337330.html
14	ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.		2021	1	+	https://cyberleninka.ru/article/n/standarty-metody-i-tehnologii-sistemnoy-inzhenerii
Итого по дисциплине: % печатных изданий 85; % электронных 55						

6.2. Программное обеспечение и Интернет-ресурсы

Программное обеспечение:

Windows 7, средства просмотра Opera/Google Chrome, MS Office 2010.

Интернет-ресурсы:

1. Национальный открытый университет «Интуит» https://www.intuit.ru/ studies/courses/691/547/info.

2. Ресурсный центр помощи студентам (методические указания) – материалы сайта: http://vstuhelp.narod.ru/met/zi.html.

3. Алефиренко В.М. Основы защиты информации (методические указания) – материалы сайта: http://www.twirpx.com/files/informatics/security/technical/ft.guideline/.

4. Электронный портал факультета электроники и вычислительной техники – материалы сайта: http://fevt.ru/load/78.

6.3. Методические указания и материалы по видам занятий

Методические указания предоставляются студентам в виде теоретических предпосылок (в электронном виде) к лабораторным работам.

Отчеты по лабораторным работам следует оформлять в соответствии с общими требованиями и правилами оформления.

7. Материально-техническое обеспечение дисциплины

Для осуществления образовательного процесса по дисциплине «Защита информации» требуется наличие компьютерной техники с установленным соответствующим программным обеспечением и другого оборудования, поддерживающего проведение презентаций, построение проектной документации, ведение групповой обработки, выход в сеть Интернет. Также требуется обеспечение литературой, которую в достаточном объеме может предложить электронная библиотека, читальный зал филиала ПГУ им. Т.Г. Шевченко в г. Рыбница и БД по дисциплине в виртуальной обучающей среде Moodle.

Карта обеспечения дисциплины учебными материалами:

№ п/п	Наименование	Вид	Форма доступа
1	Учебно-методическая литература по дисциплине «Защита информации»	Электронный	Электронная библиотека, кафедра ИиПИ
2	Описание лаб. работ	Электронный	Электронная библиотека, кафедра ИиПИ
3	Мультимедийные материалы	Сетевой	Медиатека кафедры ИиПИ
4	Электронная библиотека	Сетевой	Портал филиала ПГУ им. Т.Г. Шевченко в г. Рыбница/ Moodle

Карта обеспечения дисциплины оборудованием:

№ п/п	Номер аудитории	Кол-во	Наименование	Форма использования
1	Аудитория № 30	7	Персональные компьютеры, объединенные локальной сетью. ОС Windows 10. Расширенный пакет Office. Глобальная сеть Internet.	Организация лабораторных работ, доступ к образовательным ресурсам во время самостоятельной работы студентов, работа с мультимедийными материалами на лабораторных занятиях

8. Методические рекомендации по организации изучения дисциплины

Рабочая учебная программа по дисциплине «Защита информации» составлена в соответствии с требованиями Федерального Государственного образовательного стандарта ВО по направлению 2.09.03.04 «Программная инженерия» и учебного плана по профилю подготовки «Разработка программно-информационных систем».

Методические рекомендации для студентов

Методические рекомендации для студентов содержат:

- тематику лабораторных работ;
- планы лабораторных работ с указанием примерного списка аудиторных и домашних заданий.

Изучение дисциплины «Защита информации» включает лекционные и лабораторные занятия. Лекции разбиты на основные разделы, каждый раздел может содержать несколько тем.

Курс сопровождают лабораторные работы. При подготовке к лабораторным работам студентам необходимо самостоятельно изучить рекомендуемую литературу, ответить на контрольные вопросы. В течение семестра каждый студент должен подготовить хотя бы один доклад на темы, предложенные преподавателем.

При подготовке к занятиям необходимо использовать литературу, имеющуюся в достаточном количестве в библиотеке вуза. В список рекомендуемой литературы входит основная и дополнительная литература. Список литературы приведен в карте обеспечения дисциплины учебно-методической литературой.

Текущий контроль усвоения знаний по дисциплине предполагает использование разных форм контроля, в том числе тестирование. Итоговый контроль может осуществляться в форме теста и экзамена. Вопросы к экзамену и образцы тестовых заданий приведены.

Методические указания по организации самостоятельной работы студентов

Рабочая учебная программа по дисциплине «Защита информации» составлена в соответствии с требованиями Федерального Государственного образовательного стандарта ВО с учетом рекомендаций ОПОП по направлению подготовки 2.09.03.04 «Программная инженерия» и учебного плана по профилю подготовки «Разработка программно-информационных систем». Программа по курсу «Защита информации» рассчитана на 36 лекционных часов, 18 лабораторных и 54 часа самостоятельной работы. Изучение курса «Защита информации» рассчитано на один семестр, в конце которого проводится зачет.

В 2023–2024 учебном году работа со студентами реализуется в комбинированном формате. Комбинированный формат проведения учебных занятий включает контактную работу обучающихся с преподавателями в аудитории и работу обучающихся и работу обучающихся с преподавателями дистанционно в режимах онлайн (online) и офлайн (ofline) с использованием образовательного портала «Электронный университет ПГУ» (Moodle); платформ видеоконференций – Zoom и др.; возможности мессенджеров – Viber, Skype, Telegram и др., а так же проведение работы посредством групповой электронной почты обучающихся и электронной почты преподавателей.