ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«Приднестровский государственный университет им. Т.Г. Шевченко»
Бендерский Политехнический филиал

Кафедра «Промышленность и информационные технологии»

УТВЕРЖДАЮ
Директор БПФ ГОУ
«ПГУ им. Т. Г. Шевченко»
_____С. С. Иванова
«30» 09 2024 г

РАБОЧАЯ ПРОГРАММА

Б1.В.ДВ.03.01 «Информационная безопасность»

на 2024/2025 учебный год

Направление подготовки:
38.03.01 Экономика
Профиль подготовки
Экономика предприятий и организаций (строительство)

Квалификация
бакалавр

Форма обучения:
очная

ГОД НАБОРА 2024 г.

Бендеры, 2024

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с требованиями Государственного образовательного стандарта ВО по направлению подготовки 38.03.01 "Экономика" и основной профессиональной образовательной программы (учебного плана) по профилю подготовки «Экономика предприятий и организаций (строительство)»

Составитель рабочей программы
доц. каф. ПиИТ, к.п.н _____ В. А. Богданова

Рабочая программа утверждена на заседании кафедры «Промышленность и информационные технологии»
11 сентября 2024 г. протокол №2

Зав. кафедрой, отвечающей за реализацию дисциплины
11 сентября 2024 г._____ Н. А. Маруних
подпись

Зав. выпускающей кафедры «Экономика строительства и теории коммуникаций»,

« 11 » 09 2024 г. _____ Е.В. Корниевская
подпись

Зам. директора по УМР _____ Н. А. Колесниченко
подпись

« 12 » 09 2024 г

1. Цель и задачи освоения дисциплины

Цель освоения дисциплины «Информационная безопасность» является формирование у студентов устойчивых навыков работы в сложной сетевой информационной среде современного предприятия, офиса.

Задачами *освоения дисциплины «Информационная безопасность» являются*: получение сведений о современном состоянии проблем обеспечения информационной безопасности компьютерных систем, существующих угрозах, видах обеспечения ИБ, методах и средствах защиты информации, основах построения комплексных систем защиты, основ правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизмов их реализации, понятий и видов защищаемой информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» относится к дисциплине по выбору вариативной части Б1.В.ДВ.03.01 ОПОП ВО по направлению 38.03.01 Экономика, профиль «Экономика предприятий и организаций (строительство)». Читается во 2 семестре на очном обучении.

3. Требования к результатам освоения дисциплины:

Изучение дисциплины направлено на формирование компетенций приведенных в таблице ниже:

Категория (группа) компетенций	**Код и наименование**	**Код и наименование индикатора достижения универсальной компетенции**
Универсальные компетенции и индикаторы их достижения		
Системное и критическое мышление	ОПК-5. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	$ИД_{ОПК-5.1.}$ Способен применять общие или специализированные пакеты прикладных программ, предназначенные для выполнения профессиональных задач $ИД_{ОПК-5.2.}$ Способен выбирать инструментарий обработки и анализа данных, современные информационные технологии и программное обеспечение соответствующие содержанию профессиональных задач
	ОПК-6- Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	$ИД_{ОПК-6.1.}$ Способен понимать принципы работы специализированных пакетов прикладных программ, предназначенные для выполнения профессиональных задач $ИД_{ОПК-6.2.}$ Способен онимать принципы современных информационных технологий и и спользовать инструментарий обработки и анализа данных, современные информационные технологии и программное обеспечение соответствующие содержанию профессиональных задач
	ПК-3. Способен осуществлять сбор и анализ информации для целей бизнес-анализа	$ИД_{ПК-3.1}$ Способен выявлять, анализировать и оценивать (степень) уровень риска и разрабатывать мероприятия по их минимизации $ИД_{ПК-3.2}$ Способен оформлять результаты бизнес-анализа в соответствии с выбранными подходами $ИД_{ПК-3.3}$ Способен применять информационные технологии в целях проведения бизнес-анализа

4. Структура и содержание дисциплины (модуля)

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

Семестр	Количество часов						Форма контроля
	Трудоемкость, з.е./часы	В том числе					
		Аудиторных				Самост. Работы (СР)	
		Всего	Лекций	Практ. зан. (ПЗ)	Лаб. занятий (ЛЗ)		
2	3 з.е/108	108	22	38	-	48	зачёт с оценкой
Итого:	3 з.е. /108	108	22	38	-	48	зачёт с оценкой

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

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			СР
			Л	ПЗ	ЛЗ	
1.	Раздел 1 Неформальные методы защиты информации	52	10	18	-	24
2.	Раздел 2 Формальные методы зашиты информации	56	12	20	-	24
Всего:		108	22	38	-	48

4.3. Тематический план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно-наглядные пособия
Раздел 1 Неформальные методы защиты информации				
1	1	2	Введение. Основные понятия информационной	УП

			безопасности.	
2	1	2	Угрозы информационной безопасности. Каналы утечки информации	УП
3	1	2	Законодательные средства защиты информации	УП
4	1	2	Организационные средства защиты информации.	УП
5	1	2	Морально-этические средства защиты информации	УП
Итого по разделу		10		
Раздел 2 Формальные методы зашиты информации				
6	2	2	Физические средства защиты информации	УП
7	2	2	Технические средства защиты информации	УП
8	2	2	Программные средства защиты информации	УП
9	2	2	Идентификация и аутентификация	УП
10	2	2	Криптография	УП
11	2	2	ЭЦП и алгоритмы хеширования	УП
Итого по разделу		12		
Итого:		**22**		

УП –Учебные пособия

Практические (семинарские) занятия

№ п/п	Номер раздела дисциплины	Объем часов	Тема практического занятия	Учебно-наглядные пособия
Раздел 1 Неформальные методы защиты информации				
1	1	2	Доктрины ИБ	МР
2	1	2	Политика безопасности Windows	МР
3	1	2	Управление доступом в Windows	МР
4	1	2	Парольная защита информации	МР
5	1	2	Безопасность внешних накопителей	
6	1	2	Антивирусное ПО	МР
7	1	2	Архивирование данных	МР
8	1	2	Защита текстовых документов	МР
9	1	2	Защита электронных таблиц	МР
Итого по разделу часов		18		
Раздел 2 Формальные методы зашиты информации				
10	2	2	Аппаратные средства защиты информации	МР
11	2	2	Тоены для защиты информации	МР
12	2	2	Управление доступом	МР
13	2	2	Обеспечение безопасности ОС	МР
14	2	2	Идентификация и аутентификация	МР
15	2	2	Биометрическая аутентификация пользователей	МР
16	2	2	Криптографические способы защиты информации	МР
17	2	2	Симметричные и ассиметричные шифры.	МР
18	2	2	Алгоритмы хеширования	МР
19	2	2	ЭЦП	МР
Итого по разделу часов		20		
Итого:		**38**		

МР -Методические рекомендации

Лабораторные работы не предусмотрены.

Самостоятельная работа обучающегося

№ п/п	Раздел дисциплины	Тема и вид СРО	Трудоемкость
Раздел 1 Неформальные методы защиты информации			
1	1	Основные понятие информационной безопасности. ДЗ	4
2	1	Угрозы информационной безопасности. ДЗ	4
3	1	Каналы утечки информации. ДЗ	4
4	1	Законодательные средства защиты информации ДЗ	4
5	1	Организационные средства защиты информации . ДЗ	4
6	1	Морально-этические средства защиты информации . ДЗ	4
		Итого по разделу 1 часов	24
Раздел 2 Формальные методы зашиты информации			
7	2	Физические и технические средства защиты информации ДЗ	4
8	2	Современные симметричные криптосистемы Методы стеганографии Асимметричные криптосистемы. ДЗ	4
9	2	Программные средства защиты информации . ДЗ	4
10	2	Антивирусное ПО. ДЗ	4

11	2	Идентификация и аутентификация. ДЗ	4
12	2	Криптография. ДЗ	4
		Итого по разделу 2 часов	24
		Итого:	48

ДЗ – домашнее задание; СИТ – самостоятельное изучение темы; ИДЛ – изучение дополнительной литературы.

5. Примерная тематика курсовых проектов (работ): не предусмотрены

6. Учебно-методическое и информационное обеспечение дисциплины (модуля):

Учебный процесс обеспечивается соответствующими службами. Это, во-первых компьютерные классы с локальными сетями; библиотека с постоянно обновляемым фондом; доступный Internet и методическими разработками кафедры.

Содержание учебно-методического, информационного и материально-технического обеспечения данной дисциплины, начиная со списка литературы.

6.1. Основная литература:

№ п/п	Наименование учебника, учебного пособия	Автор	Год издания	Кол-во экземпляров	Электронная версия	Место размещения электронной версии
	Основная литература					
1.	Введение в информационную безопасность автоматизированных систем : учебное пособие	Бондарев В. В.	2016	-	есть	каб. ЭИР
2.	Информационная безопасность: Учебное пособие	Ясенев В.Н.	2017	-	есть	каб. ЭИР
	Дополнительная литература					
1.	Введение в криптографию: Теоретико-числовые основы защиты информации. Учебное пособие	Деза Е.И., Котова Л. В.	2022	-	есть	каб. ЭИР

6.2. Программное обеспечение и Интернет-ресурсы:

1. https://www.itsec.ru/information-security - журнал, посвященный актуальным вопросам ИБ
2. https://wikisec.ru/ –энциклопедия информационной безопасности

6.3. Методические указания и материалы по видам занятий:

https://view.joomag.com/ЗКИ/0654461001476108645?preview – электронные методические указания к выполнению лабораторных работ по «Защите компьютерной информации», разработчик Богданова В.А.

https://sites.google.com/view/bogdanova-zki/главная?authuser=1 – сайт поддержки в изучении информационной безопасности, разработчик Богданова В.А.

7. Материально-техническое обеспечение дисциплины (модуля):

Материально-техническое обеспечение включает в себя специально оборудованные кабинеты и аудитории: компьютерные классы, аудитории, оборудованные мультимедийными средствами обучения.

Использование электронных учебников и дисков-тренажеров в процессе обучения должно обеспечиваться наличием во время самостоятельной подготовки рабочего места для каждого обучающегося в компьютерном классе имеющего выход в Интернет, в соответствии с объемом изучаемой дисциплины.

8. Методические рекомендации по организации изучения дисциплины:

В учебном процессе для формирования и развития профессиональных навыков студентов должны использоваться следующие формы работы:

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	*Количество часов*
I	Л	Мультимедийные презентации. Постановка проблемных ситуаций.	8
	ПР	Дискуссия, деловая игра, коллоквиум, конференция, дебаты, практическая ситуация, творческое задание, работа в малых группах.	10
Итого:			18 ч.

1. Лекции с мультимедийной презентацией информации.

2. Практические занятия рекомендуется проводить на основе широкого использования активных и интерактивных форм проведения занятий: семинаров в диалоговом режиме, деловых и ролевых игр, разбора конкретных ситуаций, групповых дискуссий, обсуждения результатов работы студенческих исследовательских групп.

В качестве особенности организации самостоятельной работы в процессе изучения дисциплины отметим то, что 48 часов выделено на самостоятельную работу на дневной форме обучения.

9. Технологическая карта дисциплины

Курс 2

Группа БП24ДР62ЭК1

Семестр 2

Преподаватель – лектор – к.п.н, доц. каф. В.А.Богданова

Преподаватель, ведущий практические занятия: к.п.н., доц. каф. В.А.Богданова

Кафедра Промышленность и информационные технологии

Семестр	Количество часов						Форма контроля
	Трудоемкость, з.е./часы	В том числе					
		Аудиторных				Самост. Работы (СР)	
		Всего	Лекций	Практ. зан. (ПЗ)	Лаб. занятий (ЛЗ)		
2	3 з.е/108	108	22	38	-	48	зачёт с оценкой
Итого:	3 з.е. /108	108	22	38	-	48	зачёт с оценкой

Форма текущей аттестации	**Расшифровка**	**Минимальное количество баллов**	**Максимальное количество баллов**
Контроль посещаемости занятий	*Посещение лекционных занятий*	0	10
	Посещение семинарских и практических занятий	0	0
Текущий контроль работы на семинарских и практических занятиях	Введение.	2	4
	Основные понятия информационной безопасности.	2	4
	Угрозы информационной безопасности	2	4
	Каналы утечки информации	2	5
	Законодательные средства защиты информации	2	5
	Организационные средства защиты информации	2	4
	Морально-этические средства защиты информации	2	4
	Физические средства защиты информации	2	4
	Технические средства защиты информации	2	5
	Программные средства защиты информации	2	4
	Программные средства защиты информации	2	4
	Антивирусное ПО	2	4
	Идентификация и аутентификация	2	5
	Криптография	2	4
Рубежный контроль	1. Контрольная работа №1	6	15
	2. Контрольная работа №2	6	15
Итого количество баллов по текущей аттестации		40	100
Промежуточная аттестация	Зачет с оценкой	10	30
Итого по дисциплине		40	100

Если студент набрал менее 40 баллов, либо желает повысить полученную им автоматическим путем оценку, он сдает экзамен. Общая сумма баллов при правильном и полном ответе на все вопросы равна 20. Полученные на промежуточной аттестации баллы суммируются с набранными баллами по текущей аттестации и оценка выставляется по следующей шкале в пересчете на применяемую в филиале 5-балльную шкалу оценок: 5 (отлично) - за 90 и более баллов; 4 (хорошо) - за 70–89 балла; 3 (удовлетворительно) - за 40 – 69 баллов.

Составитель _____ к.п.н., доцент В.А. Богданова

Зав. кафедрой ПиИТ _____ к.г.н., доцент Н.А. Маруних

Зам. директора по УМР _____ Н.А. Колесниченко