Государственное образовательное учреждение
«Приднестровский государственный университет им. Т.Г.Шевченко»
Рыбницкий филиал

Кафедра прикладной информатики в экономике

УТВЕРЖДАЮ
Директор Рыбницкого филиала
ГГУ им. Т.Г. Шевченко, профессор
_____ Павлинов И.А.
«___» _____ 2023 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

на 2023 / 2024 учебный год

Направления подготовки
38.03.05 Бизнес-информатика

Профиль подготовки
Архитектура предприятий

Квалификация
бакалавр

Форма обучения
заочная

Года набора___2020____

Рыбница, 2023

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с требованиями Государственного образовательного стандарта ВО по направлению подготовки 38.03.05 «Бизнес-информатика» (квалификация «бакалавр»), утвержденного приказом №1002 Министерства образования и науки Российской Федерации от 11.08.2016г.

Составитель (-ли) рабочей программы

Ст. преподаватель _____ Печерский И.А.

Рабочая программа утверждена на заседании кафедры прикладной информатики в экономике «19» 09 2023 г. протокол № 1

Зав. кафедры-разработчика
«19» 09 2023г. _____ Павлинов И.А. / профессор

Зав. выпускающей кафедрой
«19» 09 2023г. _____ Павлинов И.А. / профессор

1. *Цели и задачи освоения дисциплины*

Целью освоения дисциплины "Информационная безопасность" является формирование у обучаемых знаний в области теоретических основ информационной безопасности и защиты информации, умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в системах защиты информации в вычислительных системах и сетях. В результате изучения обязательной части цикла обучающийся должен уметь определять необходимый уровень безопасности информации, правильно организовать мероприятия по защите информации, применять в профессиональной деятельности нормативно-правовую базу информационной безопасности; знать основные понятия, объекты, цели и задачи защиты информации, угрозы информационной безопасности – их классификацию и источники возникновения, приемы защиты информации, виды и характеристики современных средств защиты, классификацию и характеристику компьютерных вирусов, общую характеристику средств нейтрализации компьютерных вирусов, нормативно-правовую базу информационной безопасности.

2. *Место дисциплины в структуре ООП ВО:*

Б.1.Б.25 Информационная безопасность.

Данная дисциплина является базовой. Преподается в течение четвертого года обучения (в восьмом семестре). Содержание дисциплины «Информационная безопасность» - одна из составляющих частей теоретической и практико-ориентированной подготовки студентов по направлению подготовки «Бизнес-информатика».

Для освоения дисциплины обучающиеся используют знания, умения, сформированные в ходе изучения дисциплин базовой части профессионального цикла: «Вычислительные системы, сети, коммуникации», «ИТ-инфраструктура предприятия».

Место учебной дисциплины – в совокупности дисциплин профессионального цикла.

3. *Требования к результатам освоения дисциплины:*

Изучение дисциплины направлено на формирование следующих компетенций:

Код компетенции	**Формулировка компетенции**
Общепрофессиональные компетенции:	
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3	способностью работать с компьютером как средством управления информацией, работать с информацией из различных источников, в том числе в глобальных компьютерных сетях
Профессиональные компетенции:	
ПК-7	использование современных стандартов и методик, разработка регламентов для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий
ПК-9	организация взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия
ПК-11	умение защищать права на интеллектуальную собственность
ПК-21	умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия

В результате освоения дисциплины студент должен:

3.1. Знать:

В соответствии с ФГОС ВО:

- основы защиты информации;
- принципы криптографических преобразований;
- типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду;

3.2. Уметь:

В соответствии с ФГОС ВО:

- реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации;
- проводить анализ степени защищенности информации и осуществлять повышение уровня зашиты с учетом развития математического и программного обеспечения вычислительных систем;
- разрабатывать средства и системы защиты информации;

3.3. Владеть:

В соответствии с ФГОС ВО:

- навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях
- навыками работы с программно-аппаратными средствами защиты информации;
- нормативными документами, регламентирующими оценку защищенности ИТ

4. Структура и содержание дисциплины (модуля)

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

Курс	Количество часов						Форма итогового контроля
	Трудоемкость, з.е./часы	В том числе					
		Аудиторных				Самост. работы	
		Всего	Лекций	Лаб. раб.	Практич. зан.		
IV	5 / 180	26	10	-	16	150	Зачет с оценкой
Итого:	**5 / 180**	**26**	**10**	**-**	**16**	**150**	**4**

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

№ раз-дела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеауд. работа (СР)
			Л	ПЗ	ЛР	
1.	Основы информационной безопасности	176	10	16	-	150
	Итого:	***176***	***10***	***16***	***-***	***150***
	Зачет	4				
	Всего:	**180**				

4.3. Тематический план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекций	Учебно-наглядные пособия
1	1.	2	Информационная безопасность, ее составляющие. Стандарты информационной безопасности.	Презентации, раздаточный материал
2	1.	2	Классификация угроз информационной безопасности.	Презентации, раздаточный материал
3	1.	2	Компьютерные вирусы, классификация.	Презентации, раздаточный материал
4	1.	2	Защита от компьютерных вирусов. Антивирусные программы. Обнаружение вируса.	Презентации, раздаточный материал
5	1.	2	Информационная безопасность вычислительных сетей. Механизмы обеспечения информационной безопасности	Презентации, раздаточный материал
Итого:		**10**		

Практические (семинарские) занятия

№ п/п	Номер раздела дисциплины	Объем часов	Тема лабораторного занятия	Наименование лаборатории	Учебно-наглядные пособия
1	1.	4	Анализ рисков информационной безопасности	Компьютерная аудитория	Методические указания, раздаточный материал
2	1.	4	Построение концепции информационной безопасности предприятия	Компьютерная аудитория	Методические указания, раздаточный материал
3	1.	4	Алгоритмы поведения вирусных и других вредоносных программ.	Компьютерная аудитория	Методические указания, раздаточный материал
4	1.	4	Алгоритмы предупреждения и обнаружения вирусных угроз	Компьютерная аудитория	Методические указания, раздаточный материал
Итого:		**16**			

Лабораторные работы

Лабораторные и семинарские занятия планом не предусмотрены

Самостоятельная работа студента

№ п/п	Номер раздела дисциплины	Тема и вид СРС	Трудоемкость (в часах)
1	1.	Международные стандарты информационного обмена. Модели безопасности и их применение	10
2	1.	Сущность и задачи обеспечения информационной безопасности	6
3	1.	Криптографические методы	10

4	1.	Асимметричные криптосистемы. Элементы теории чисел	6
5	1.	Методы и средства защиты от удаленных атак через Internet	8
6	1.	Проблема информационной безопасности общества	4
7	1.	Нормативно-правовые основы информационной безопасности в ПМР и РФ	4
8	1.	Ответственность за нарушения в сфере информационной безопасности. Основные положения важнейших законодательных актов ПМР и РФ	4
9	1.	Классификация угроз "информационной безопасности"	10
10	1.	Каналы несанкционированного доступа к информации	8
11	1.	Классификация и особенности антивирусных программ	10
12	1.	Профилактика компьютерных вирусов	6
13	1.	Обнаружение неизвестного вируса. Общий алгоритм	6
14	1.	Особенности обеспечения информационной безопасности в компьютерных сетях	10
15	1.	Сетевые модели передачи данных	8
16	1.	Адресация в глобальных сетях. Основы IP-протокола. Система доменных имен	10
17	1.	Классификация удаленных угроз в вычислительных сетях	10
18	1.	Типовые удаленные атаки и их характеристика	6
19	1.	Причины успешной реализации удаленных угроз в вычислительных сетях	6
20	1.	Принципы защиты распределенных вычислительных сетей	4
21	1.	Механизмы обеспечения "информационной безопасности". Идентификация и аутентификация пользователей	4
Итого:			**150**

5. *Примерная тематика курсовых проектов (работ)*

Курсовые работы(проекты) планом не предусмотрены.

6. *Образовательные технологии*

В процессе освоения дисциплины «Информационная безопасность» используются следующие образовательные технологии:

- лекции;
- компьютерные занятия;
- самостоятельная работа студентов, в которую включается освоение информационных технологий и интерпретации результатов;
- консультации преподавателей.

Применение каждой формы обучения предполагает применение новых IT – технологий.

Проведение аудиторных занятий (лекций и лабораторных работ) предполагает использование аудиовизуальных электронных и компьютерных средств мультимедиа, имеющихся в арсенале Университета.

Семестр	*Вид занятия (Л, ПР, ЛР)*	*Используемые интерактивные образовательные технологии*	*Количество часов*
8	Л	Презентации, раздаточный материал	10
	ПР	Разбор конкретных ситуаций с использованием компьютерных средств	16
Итого:			26

7. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Для оценки качества усвоения курса используются следующие формы контроля:

- **текущий** – контроль выполнения практических работ, тестирование;
- **рубежный** - предполагает использование тестовых материалов для контроля знаний, учет суммарных результатов по итогам текущего контроля за соответствующий период, систематичность работы и творческий рейтинг (участие в конференции, публикации, творческие идеи и т.д.). Рубежный контроль осуществляется в один этап;
- **итоговый** – осуществляется посредством тестирования и зачета.

Вопросы для зачета

1. Понятие "информационная безопасность"
2. Проблема информационной безопасности общества
3. Составляющие информационной безопасности
4. Система формирования режима информационной безопасности
5. Нормативно-правовые основы информационной безопасности в ПМР и РФ
6. Ответственность за нарушения в сфере информационной безопасности. Основные положения важнейших законодательных актов ПМР и РФ
7. Стандарты информационной безопасности распределенных систем
8. Сервисы безопасности в вычислительных сетях
9. Административный уровень обеспечения информационной безопасности
10. Классификация угроз "информационной безопасности"
11. Каналы несанкционированного доступа к информации
12. Вирусы как угроза информационной безопасности
13. Характерные черты компьютерных вирусов
14. Классификация компьютерных вирусов по среде обитания
15. Классификация компьютерных вирусов по особенностям алгоритма работы
16. Классификация компьютерных вирусов по деструктивные возможностям
17. Виды "вирусоподобных" программ
18. Характеристика "вирусоподобных" программ
19. Утилиты скрытого администрирования
20. Классификация и особенности антивирусных программ
21. Профилактика компьютерных вирусов
22. Обнаружение неизвестного вируса. Общий алгоритм
23. Особенности обеспечения информационной безопасности в компьютерных сетях
24. Сетевые модели передачи данных
25. Адресация в глобальных сетях. Основы IP-протокола.
26. Адресация в глобальных сетях. Система доменных имен
27. Классификация удаленных угроз в вычислительных сетях
28. Типовые удаленные атаки и их характеристика
29. Причины успешной реализации удаленных угроз в вычислительных сетях
30. Принципы защиты распределенных вычислительных сетей
31. Механизмы обеспечения "информационной безопасности". Идентификация и аутентификация пользователей
32. Механизмы обеспечения "информационной безопасности". Криптография и шифрование
33. Механизмы обеспечения "информационной безопасности". Методы разграничение доступа
34. Технология виртуальных частных сетей (VPN)

8. *Учебно-методическое и информационное обеспечение дисциплины*

8.1. Основная литература:

1. К. Дж. Джонс, М. Шема, Б. С. Джонсон Анти-хакер. Средства защиты компьютерных сетей. Справочник профессионала. / Пер. с англ., - М.: СП ЭКОМ, 2003. – 688 с.
2. Штребе М., Перкинс Ч., Монкур М. Безопасность сетей NT4: Пер. с англ., в 2-х т., т. 1. – М.: Мир, 1999. – 358 с.
3. Штребе М., Перкинс Ч., Монкур М. Безопасность сетей NT4: Пер. с англ., в 2-х т., т. 2. – М.: Мир, 1999. – 367 с.
4. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 3-е издание, стереотипное. – М.: Горячая линия-Телеком, 2005. – 147 с.
5. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2001. – 320 с.
6. Байбурин В.Б., Бровкова М.Б. Введение в защиту информации: Учебное пособие. – М. Форум: ИНФРА-М, 2004. – 128 с.
7. Краснюк Д.В., Хованский В.А. Инженерно-техническая безопасность: Учебно-практическое пособие. – М.: МЭСИ, 1999. – 88 с.
8. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. – 384 с.
9. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001. – 352 с.

8.2. Дополнительная литература

1. Девянин П.Н. Теоретические основы компьютерной безопасности: Уч. пособие для вузов. /П.Н. Девянин, Д.И. Михальский, Д.И. Правиков, А.Ю.Щербаков – М.: Радио и связь, 2003. – 192с.
2. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1997. - 241с.
3. Зегжда Д., Ивашко А. Как построить защищенную информационную систему. /Д. Зегжда, А. Ивашко.– СПб.: Мир и семья, 2003. – 98с.
4. Завгородний в.и. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2011. – 264с.
5. Лаптев В.Н. Информационная безопасность и защита информации: Курс лекций. – Краснодар: КубГАУ, 2010. – 132с.
6. Зима В. Компьютерные сети и защита передаваемой информации. /В. Зима, А. Молдовян., Н. Молдовян. – СПб.: СПбГУ, 2005. – 198с.
7. Информационная безопасность и защита информации: Практикум. /В.И. Лойко., В.Н. Лаптев, Д.Ю. Жмурко. – Краснодар: КубГАУ, 2010. - 128с.
8. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 2007. – 157с.

9. *Материально-техническое обеспечение дисциплины (модуля):*

Для проведения лекционных и лабораторных занятий необходимы:

1) Лекционная аудитория, оборудованная видеопроекционным оборудованием для презентаций.

2) Компьютерная аудитория, оборудованный для проведения лабораторных работ персональными компьютерами, с операционной системой Windows XP и новее, др. программным обеспечением Microsoft Office, объединенными в сеть и с выходом в Интернет.

10. *Методические рекомендации по организации изучения дисциплины:*

Рабочая учебная программа по дисциплине «Информационная безопасность» составлена в соответствии с требованиями Федерального Государственного

образовательного стандарта ВО по направлению 38.03.05 «Бизнес-информатика» и учебного плана по профилю подготовки (или специализации) «Архитектура предприятий».

Изучение дисциплины проходит в форме лекционных занятий, выполнения практических работ в компьютерной аудитории. Самостоятельная работа заключается в самостоятельном изучении тем студентом, а так же их конспектировании.

11. Технологическая карта дисциплины

Курс *4* группа *РФ20ВР62БИ1* семестр *8*.
Преподаватель – лектор *Печерский Игорь Александрович*
Преподаватели, ведущие практические занятия *Печерский Игорь Александрович*
Кафедра *прикладной информатики в экономике*
Весовой коэффициент дисциплины в совокупной рейтинговой оценке, рассчитываемой по всем дисциплинам (***если введена модульно-рейтинговая система***) *модульно-рейтинговая система не введена*

Наименование дисциплины / курса	Уровень//ступень образования (бакалавриат, специалитет, магистратура)	Статус дисциплины в рабочем учебном плане (А, Б, В, Г) (***если введена модульно-рейтинговая система***)	Количество зачетных единиц / кредитов

Смежные дисциплины по учебному плану *(перечислить):*

Предшествующие: «Вычислительные системы, сети, коммуникации», «ИТ-инфраструктура предприятия».

ВВОДНЫЙ МОДУЛЬ
(входной рейтинг-контроль, проверка «остаточных» знаний по смежным дисциплинам)

Тема, задание или мероприятие входного контроля	Виды текущей аттестации	Аудиторная или внеаудиторная	Минимальное количество баллов	Максимальное количество баллов
Итого:				

БАЗОВЫЙ МОДУЛЬ
(проверка знаний и умений по дисциплине)

Тема, задание или мероприятие текущего контроля	Виды текущей аттестации	Аудиторная или внеаудиторная	Минимальное количество баллов	Максимальное количество баллов
Текущая работа	Лабораторные работы	Аудиторная	20	60
	Работа на лекциях	Аудиторная	10	20
	Самостоятельная работа	Внеаудиторная	10	20
Итого:			40	100

ДОПОЛНИТЕЛЬНЫЙ МОДУЛЬ

Тема, задание или мероприятие дополнительного контроля	Виды текущей аттестации	Аудиторная или внеаудиторная	Минимальное количество баллов	Максимальное количество баллов
Составление рефератов по темам дисциплины, изученным самостоятельно			5	10
ИТОГО			**5**	**10**

Необходимый минимум для получения итоговой оценки или допуска к промежуточной аттестации ____ баллов (*если введена модульно-рейтинговая система*).

Дополнительные требования для студентов, отсутствующих на занятиях по уважительной причине:

- *устное собеседование с преподавателем по проблемам пропущенных лекционных занятий,*
- *выполнение и защита пропущенных лабораторных работ в рамках часов, отведенных на организацию самостоятельной работы студента;*
- *обязательное выполнение внеаудиторных контрольных и письменных работ.*

Составитель _____ /Печерский Игорь Александрович

Согласовано:

Директор филиала ПГУ им. Т.Г. Шевченко в г. Рыбница

_____/ Павлинов Игорь Алексеевич, профессор