ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«Приднестровский государственный университет им. Т.Г. Шевченко»

Бизнес-информатики и информационных технологий

УТВЕРЖДАЮ
Декан экономического факультета
к.э.н., **И. Н. Узун**
(подпись, расшифровка подписи)
"__" 05 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине

Б1.О.30 «Информационная безопасность»
на 2021-2022 учебный год

5.38.03.05 Бизнес-информатика
(Код и наименование направления подготовки)

Электронный бизнес
(наименование профиля подготовки)

Квалификация
Бакалавр
(квалификация (степень) выпускника)

Форма обучения:
очная

Год набора 2021

Тирасполь 2021

Рабочая программа **«Информационная безопасность»** разработана в соответствии с требованиями Государственного образовательного стандарта ВО по направлению подготовки 5.38.03.05- бизнес-информатика и основной профессиональной образовательной программы (учебного плана) по профилю подготовки – Электронный бизнес

Составитель рабочей программы
К.т.н., доцент кафедры
бизнес-информатики и информационных технологий _____ Е.В. Саломатина
(подпись)

Рабочая программа утверждена на заседании кафедры бизнес-информатики и информационных технологий
«15» 04 202 г., протокол №

Зав. кафедры-разработчика
«16» 03 202 г. _____ доцент, к.ф.-м.н. Л. Ю. Надькин

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«Приднестровский государственный университет им. Т.Г. Шевченко»

Бизнес-информатики и информационных технологий

УТВЕРЖДАЮ

Декан экономического факультета
к.э.н., **И. Н. Узун**
(подпись, расшифровка подписи)
“____”_____2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине

Б1.О.30 «Информационная безопасность»
на 2021-2022 учебный год

5.38.03.05 Бизнес-информатика
(Код и наименование направления подготовки)

Электронный бизнес
(наименование профиля подготовки)

Квалификация
Бакалавр
(квалификация (степень) выпускника)

Форма обучения:
очная

Год набора 2021

Тирасполь 2021

Рабочая программа **«Информационная безопасность»** разработана в соответствии с требованиями Государственного образовательного стандарта ВО по направлению подготовки 5.38.03.05- бизнес-информатика и основной профессиональной образовательной программы (учебного плана) по профилю подготовки – Электронный бизнес

Составитель рабочей программы
К.т.н., доцент кафедры
бизнес-информатики и информационных технологий Е.В. Саломатина
(подпись)

Рабочая программа утверждена на заседании кафедры бизнес-информатики и информационных технологий
« __ » _____ 202 г., протокол №

Зав. кафедры-разработчика
« __ » _____ 202 г. _____ доцент, к.ф.-м.н. Л. Ю. Надькин

1. *Цели и задачи освоения дисциплины*

Рабочая программа учебной дисциплины «Информационная безопасность» составлена в соответствии с учебным планом подготовки бакалавров по направлению 5.38.03.05 Бизнес-информатика в соответствии с федеральным государственным образовательным стандартом высшего образования и утвержденными стандартами, и положениями Университета. Основными целями изучения данной дисциплины являются: формирование целостной системы знаний в области теоретических основ информационной безопасности; формирование навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах; развитие способности творчески подходить к решению профессиональных задач.

Задачами изучения дисциплины являются:

- ознакомление с понятийным аппаратом в области информационной безопасности;
- рассмотрение базовых содержательных положений в области информационной безопасности;
- изучение современной доктрины информационной безопасности;
- определение целей и принципов защиты информации;
- установление факторов, влияющих на защиту информации;
- установление структуры угроз защищаемой информации;
- определение сущности компонентов защиты информации.;

2. *Место дисциплины в структуре ОПОП*

Дисциплина Б1.О.30 «Информационная безопасность» является обязательной и относится к базовой части дисциплин программы бакалавриата по направлению 5.38.03.05 «Бизнес информатика», преподается в 2-м семестре. При изучении дисциплины учитывается материал, полученный студентами в рамках дисциплин «Теоретические основы информатики», «Управление ИТ-сервисами и контентом».

Знания, приобретённые в процессе изучения дисциплины «Информационная безопасность» используются при изучении дисциплин «Объектно-ориентированные анализ и программирование», «Управление жизненным циклом ИС» а также других профессиональных дисциплин цикла, преподавание которых требует рассмотрения вопросов, связанных с использованием теоретических знаний и практических навыков информационной безопасности

3. *Требования к результатам освоения дисциплины:*

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций: УК-8; ОПК-2, ПК-8

Категория (группа) компетенций	**Код и наименование**	**Код и наименование индикатора достижения универсальной компетенции**
Универсальные компетенции и индикаторы их достижения		
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	ИД УК-8.1. Знает причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций; основы безопасности жизнедеятельности, телефоны служб спасения. ИД УК-8.2. Умеет выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность возникновения потенциальной

		опасности для обучающегося и принимать меры по ее предупреждению в условиях образовательного учреждения; оказывать первую помощь в чрезвычайных ситуациях. ИД УК-8.3. Владеет методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками поддержания безопасных условий жизнедеятельности.
Общепрофессиональные компетенции и индикаторы их достижения		
Научное мышление	ОПК-2. Способен проводить исследование и анализ рынка информационных систем и информационно-коммуникационных технологий, выбирать рациональные решения для управления бизнесом;	ИД ОПК-3.1. Знает как выбирать решения в области информационных систем для управления бизнесом. ИД ОПК-3.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. ИД ОПК-3.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
Обязательные профессиональные компетенции и индикаторы их достижения		
Управление проектами в области ИТ на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров	ПК-8. Организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	ИД-1$_{ПК-8.}$ Знают об основных направлениях государственной политики в области информационной безопасности; о современных направлениях развития систем информационной безопасности. ИД-5$_{ПК-8.}$ Умеют применять на практике основные общеметодологические принципы теории информационной безопасности. ИД-5$_{ПК-8.}$ Владеть методами обеспечения информационной безопасности.

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. работы**	
		Всего	**Лекций**	**Лаб. раб.**	**Практич. занятия**		
1	3/ 108	54	18	18	18	54	Зачет с оценкой
Итого:	**3/108**	**54**	**18**	**40**	**18**	**54**	**Зачет с оценкой**

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	Общие вопросы информационной безопасности	***24***	***4***	***4***		***16***
2	Государственная система информационной безопасности	***16***	***4***	***4***		***8***
3	Угрозы информационной безопасности и методы их реализации	***26***	***4***	***4***	***8***	***10***
	Меры обеспечения защиты информации	***28***	***4***	***4***	***8***	***12***
	Стандартизация в области информационной безопасности	***14***	***2***	***2***	***2***	***8***
Итого:		**108**	**18**	**18**	**18**	**54**

4.3. Тематический план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно-наглядные пособия
1	1	4	**Общие вопросы информационной безопасности.** Основные понятия и определения. Понятие целостности, доступности и конфиденциальности информации. Программное обеспечение Malware. Методы социальной инженерии. Фишинг. Принципы безопасности системы защиты информации. Методы и средства защиты. Концепция информационной безопасности	Лекция-презентация
Итого по разделу часов		**4**		
2	2	4	**Государственная система информационной безопасности.** Национальные интересы в информационно-коммуникационной сфере и ее обеспечение. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ. Законодательство в области информационной безопасности.	Лекция-презентация
Итого по разделу часов		**4**		
3	3	4	**Угрозы информационной безопасности и методы их реализации.** Понятие угрозы безопасности информации. Виды угроз безопасности информации. Источники угроз безопасности информации. Нарушители безопасности информации. Виды и цели нарушителей. Потенциал и возможности нарушителей. Способы реализации угроз нарушителем. Информационная безопасность человека. Угрозы неприкосновенности частной жизни граждан. Кодекс справедливого использования информации. Планирование действий в чрезвычайной ситуации	Лекция-презентация
4		4	**Меры обеспечения защиты информации.** Идентификация угроз безопасности информации и их источников. Модель нарушителя. Принцип оценки актуальности угроз. Оценка возможности реализации угрозы. Оценка степени ущерба. Оценка актуальности угрозы. Организация защиты информации. Организационные меры.	Лекция-презентация

			Законодательные меры. Административные меры. Организационно-технические меры. Программно-технические средства. Криптографические методы. Стеганографические методы. Методы и средства технической защиты.	
5		2	**Стандартизация в области информационной безопасности.** Государственные и международные органы стандартизации в области информационной безопасности. Международные стандарты в области информационной безопасности и защиты информации	Лекция-презентация
Итого по разделу часов		**10**		
Итого:		18		

Практические занятия

№ п/п	Номер раздела дисциплины	Объем часов	Тема практического занятия	Учебно-наглядные пособия
1	1	4	Веб-квест «Информационная безопасность»	Методические указания
Итого по разделу часов		4		
2	2	4	Методы информационного воздействия	Методические указания
Итого по разделу часов		**4**		
3	3	4	Парольная защита. Advanced Office Password Recovery. Оценка стойкости парольных систем	Методические указания
4		4	Изучение государственных органов обеспечения информационной безопасности зарубежных стран	Методические указания
5		2	Работа с реестром Windows. основные возможности обеспечения безопасности с помощью реестра ОС от вредоносных программ	Методические указания
Итого по разделу часов		**10**		
Итого:		***18***		

Лабораторные работы

№ п/п	Номер раздела дисциплины	Объем часов	Тема лабораторного занятия	Наименование лаборатории	Учебно-наглядные пособия
1	3	4	Изучение зарубежных технических средств защиты информации	Компьютерный класс	Методические указания
2		4	Вопросы защиты от перехвата данных в семействе операционных систем Windows.	Компьютерный класс	Методические указания
3		4	Основы шифрования Программа Files Cipher, Max File Encryption	Компьютерный класс	Методические указания

4		6	Механизмы защиты данных, передаваемых между компьютерами (Удалённый рабочий стол, TeamViewer)	Компьютерный класс	Методические указания
Итого:		***18***			

Самостоятельная работа студента

Раздел дисциплины	**№ п/п**	**Тема и вид СРС**	**Трудоемкость (в часах)**
Раздел 1.	1.	*Веб-квест «Информационная безопасность».* Подготовка реферативного доклада..	8
	2.	*Общие вопросы информационной безопасности.* Работа с информационными ресурсами.	8
		Итого по разделу	**16**
Раздел 2.	3.	*Концепция информационной безопасности.* Работа с основной и дополнительной литературой	8
		Итого по разделу	**8**
Раздел 3.	4.	*Человеческий фактор как самый чувствительный компонент информационной безопасности.* Работа с основной и дополнительной литературой	4
	5.	*Спам и методы борьбы с ним.* Самостоятельная работа под контролем преподавателя (в форме индивидуальных консультаций).	6
	6.	*Программы удаленного доступа.* Подготовка по заданиям для самостоятельного индивидуального исполнения.	6
	7.	*Оценка стойкости парольных систем.* Подготовка к занятиям практического цикла.	6
	8.	*Международные стандарты в области информационной безопасности.* Работа с основной и дополнительной литературой	4
	9.	*Формирования профиля защиты предприятия.* Подготовка по заданиям для самостоятельного индивидуального исполнения	4
		Итого по разделу	**30**
Итого:			54

Вид занятия: лекция, практические занятия, лабораторные работы, самостоятельная работа.
Учебно-наглядные пособия: презентации, электронное методическое пособие.

5. Примерная тематика курсовых работ.

В соответствии с учебным планом не предусмотрены.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Обеспеченность обучающихся учебниками, учебными пособиями

№ п/п	Наименование **учебника, учебного пособия**	**Автор**	**Год издания**	**Кол-во экземпляров**	**Электронная версия**	**Место размещения электронной версии**
Основная литература						
1.	Информационная безопасность	Гафнер В. В.	2010	1	+	Кафедра БИиИТ
2.	Защита от компьютерного	Соколов А., Степанюк О.	2002	1	+	Кафедра БИиИТ

	терроризма					
Дополнительная литература						
1.	Системы защиты информации в ведущих зарубежных странах	Буранова М.А., Пугин В.В.	2017	1	+	Кафедра БИиИТ
2.	Информационная безопасность	Крыжановский А.В., Поздняк И.С.	2018	1	+	Кафедра БИиИТ
Раздел 1 ***Итого по дисциплине:***		***% печатных изданий-100; % электронных- 100.***				

6.2. Программное обеспечение и Интернет-ресурсы

- Информационный портал по безопасности (http://www.securitylab.ru/)
- Лаборатория Касперского (http://www.kaspersky.ru/)
- Безопасность в интернете. https://stepik.org/course/191/promo#toc

6.3. Методические указания и материалы по видам занятий.

Методические указания по выполнению лабораторных работ. (электронный вариант).

7. Материально-техническое обеспечение дисциплины.

Компьютерные классы для проведения практических и лабораторных занятий, оборудованные выходом в Интернет.

8. Методические рекомендации по организации изучения дисциплины:

Компьютерные классы для проведения практических и лабораторных занятий, оборудованные выходом в Интернет.

Университетский информационно-образовательный портал http://moodle.spsu.ru/enrol/index.php?id=2313

Техническое оборудование: компьютерный проектор и компьютер-ноутбук для чтения лекций..

9. Технологическая карта дисциплины[1]

Курс **1** группа *ЭФ21ДР62ЭБ1* семестр **2**

Преподаватель-лектор – к.т.н., доцент Е. В. Саломатина

Преподаватели, ведущие лабораторные и практические занятия –

к.т.н., доцент Е.В. Саломатина,

Кафедра Бизнес-информатики и информационных технологий

Балльно - рейтинговая система не используется на факультете.

[1] Модульно-рейтинговая система не введена.