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

Кафедра Бизнес-информатики и информационных технологий

УТВЕРЖДАЮ
декан экономического факультета
к. э. н., И. Н. Узун
(подпись, расшифровка подписи)
"09" 10 2019 г

РАБОЧАЯ ПРОГРАММА

Учебной ДИСЦИПЛИНЫ

«Информационная безопасность»

5.38.03.05 Бизнес-информатика

(Код и наименование направления подготовки)

Электронный бизнес

(наименование профиля подготовки)

квалификация (степень) выпускника
Бакалавр

Форма обучения:
очная

Тирасполь 2019

Рабочая программа дисциплины «***Информационная безопасность***» /составитель Саломатина Е.В. – Тирасполь: ГОУ ПГУ, 2019. - 10 с.

РАБОЧАЯ ПРОГРАММА ПРЕДНАЗНАЧЕНА ДЛЯ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ ВАРИАТИВНОЙ ЧАСТИ ПРОГРАММЫ БАКАЛАВРИАТА СТУДЕНТАМ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 5.38.03.05 – *БИЗНЕС-ИНФОРМАТИКА*

Рабочая программа составлена с учетом Федерального Государственного образовательного стандарта высшего профессионального образования по направлению подготовки 5.38.03.05 - *Бизнес-информатика*, утвержденного приказом *№1002 от 11.08.2016 МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ.*

Составитель _____ **/ Ф.И.О./**

__.__.2019 г. (подпись)

1. Цели и задачи освоения дисциплины

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;
- обучение разработке средств и систем защиты информации;
- развитие способности творчески подходить к решению профессиональных задач.

Задачами дисциплины являются:

- знание правовых основ, политики и стандартов информационной безопасности ИС;
- знакомство с криптографическими моделями, алгоритмами шифрования;
- оценка защищенности и обеспечения информационной безопасности компьютерных систем;

2. Место дисциплины в структуре ООП ВО

Дисциплина «Информационная безопасность» Б1.В.06 относится к вариативной части программы бакалавриата по направлению 5.38.03.05 «Бизнес - информатика», преподается в 3 семестре. При изучении дисциплины учитывается материал, полученный студентами в рамках дисциплин «Теоретические основы информатики», «Операционные среды, системы и оболочки», «Управление ИТ-сервисами и контентом».

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

3. Требования к результатам освоения дисциплины:

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-3, ПК-9, ПК-21

Код компетенции	**Формулировка компетенции**
ОПК-3	способностью работать с компьютером как средством управления информацией, работать с информацией из различных источников, в том числе в глобальных компьютерных сетях
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия
ПК-21	умение выполнять технико-экономическое обоснование проектов по совершенствованию и регламентацию бизнес-процессов и ИТ-инфраструктуры предприятия

В результате освоения дисциплины обучающийся должен:

3.1. **Знать**:

- об основных направлениях государственной политики в области информационной безопасности;
- о современных направлениях развития систем информационной безопасности;
- об основных принципах информационного противоборства;
- об основных типах угроз информационной безопасности;
- терминологию в области информационной безопасности;
- методы и средства обеспечения информационной безопасности;
- методы нарушения конфиденциальности, целостности и доступности информации.

3.2. **Уметь**:

- проводить анализ угроз информационной безопасности;
- выполнять основные этапы решения задач информационной безопасности;
- применять на практике основные общеметодологические принципы теории информационной безопасности.

3.3. **Владеть:**

- методами обеспечения информационной безопасности.

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 итогового контроля
	Трудоемкость, з.е./часы	В том числе					
		Аудиторных				Самост. работы	
		Всего	Лекций	Лаб. раб.	Практич. зан		
3	3/ 108	54	18	18	18	54	Зачет с оценкой
Итого:	**3/ 108**	**54**	**18**	**18**	**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
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
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.	Лекция-презентация

			Информационная безопасность человека	
4	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. Законодательные меры. Административные меры. Организационно-технические меры. Программно-технические средства. Криптографические методы. Стеганографические методы. Методы и средства технической защиты.	Лекция-презентация
5	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:		18		

Практические (семинарские) занятия

№ п/п	Номер раздела дисциплины	Объем часов	Тема практического занятия	Учебно-наглядные пособия
1	1	4	Веб-квест «Информационная безопасность»	Методические указания
2	2	4	Методы информационного воздействия	Методические указания
3	3	4	Парольная защита. Advanced Office Password Recovery. Оценка стойкости парольных систем	Методические указания
4		4	Создание электронной подписи в документе	Методические указания
5		2	Работа с реестром Windows. основные возможности обеспечения безопасности с помощью реестра ОС от вредоносных программ	Методические указания
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	Программа Steganos Security Suite Программа Digital Security Office	Компьютерный класс	Методические указания
4		6	Настройка виртуальной лаборатории VMware Player. Виртуальные машины: CUEHali (CUEHaliLight) COSserver (3,6 ГБ)	Компьютерный класс	Методические указания

			SecurityOnion (2,6 ГБ)		
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
Раздел 2	3	*Концепция информационной безопасности*. Работа с основной и дополнительной литературой	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:			***54***

5. Примерная тематика курсовых проектов (работ) (если имеются):

В соответствии с учебным планом не предусмотрены.

6. Образовательные технологии

Семестр	***Вид занятия (Л, ПР, ЛР)***	***Используемые интерактивные образовательные технологии***	***Количество часов***
2	Л	- мозговой штурм	2
	ЛР	- работа в группах (workshops).	6
	ПР	- обсуждение конкретных ситуаций.	4
Итого:			**12**

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

7.1. Для текущего контроля:

1. Что такое информационная безопасность:
   а) защита информации;
   б) уровень обеспечения защиты несанкционированного доступа;
   в) состояние защищенности о внешних и внутренних угроз;
   г) контроль целостности;
   д) обеспечение защиты контролируемой зоны;
   е) шифрование файлов.
2. Назначение ЭЦП:
   а) обеспечение целостности;
   б) обеспечение доступности;
   в) обеспечение авторства;
   г) обеспечение конфиденциальности;

д) обеспечение неотказуемости.

3. Поставьте в порядке важности национальные интересы:

а) Информационное обеспечение государственной политики Российской Федерации.

б) Развитие современных информационных технологий, отечественной индустрии информации.

в) Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.

г) Защита информационных ресурсов от несанкционированного доступа

4. Какой вид идентификации и аутентификации получил наибольшее распространение?

а) одноразовые пароли

б) постоянные пароли

в) системы PKI

5. Таргетированная атака -

а) Атака на конкретный компьютер пользователя

б) Атака на компьютерную систему крупного предприятия

в) Атака сетевое оборудование

6. Что относится к классической триаде CIA в Информационной Безопасности?

а) Авторизация

б) Аутентификация

в) Конфиденциальность

г) Риск

д) Доступность

е) Идентификация

ж) Целостност

7. Злоумышленник совершил взлом сети компании, при этом были похищены данные пользователей. Какое свойство безопасности было нарушено?

а) Авторизация

б) Аутентификация

в) Конфиденциальность

г) Риск

д) Доступность

е) Идентификация

ж) Целостност

8. Какие IDS (СОВ) обнаруживают атаки, сравнивая входящие пакеты с образцами пакетов известных тип атак.

а) Эвристические

б) Сигнатурные

в) Интеллектуальные

9. Какая это атака: "Во время произведения пополнения счета в 83.8 WMZ на счет пришло 83.0 WMZ, жертва обычно думает, что это сбой в системе округления".

а) Это атака "E-Banking"

б) Это атака "Салями".

в) Это "replay" атака.

г) Никакой атаки тут нет, это и есть сбой в системе округления.

7.2. Для промежуточного контроля:

1. Понятие целостности, доступности и конфиденциальности информации.
2. Программное обеспечение Malware. Методы социальной инженерии. Фишинг.
3. Принципы безопасности системы защиты информации
4. Методы и средства защиты.
5. Концепция информационной безопасности
6. Стратегия национальной безопасности Доктрина информационной безопасности РФ.
7. Законодательство в области информационной безопасности.
8. Понятие угрозы безопасности информации. Виды угроз безопасности информации.
9. Источники угроз безопасности информации.
10. Нарушители безопасности информации. Виды и цели нарушителей.

11. Потенциал и возможности нарушителей. Способы реализации угроз нарушителем.
12. Информационная безопасность человека
13. Идентификация угроз безопасности информации и их источников.
14. Модель нарушителя.
15. Принцип оценки актуальности угроз.
16. Оценка возможности реализации угрозы.
17. Оценка степени ущерба.
18. Оценка актуальности угрозы.
19. Организация защиты информации.
20. Организационные меры.
21. Законодательные меры.
22. Административные меры.
23. Организационно-технические меры.
24. Программно-технические средства.
25. Криптографические методы.
26. Стеганографические методы.
27. Методы и средства технической защиты.
28. Государственные и международные органы стандартизации в области информационной безопасности.
29. Международные стандарты в области информационной безопасности и защиты информации

7.3. Для реферативного доклада:

1. Анализ доступной платежной системы с точки зрения информационной безопасности.
2. Безопасность облачных технологий в информационной среде.
3. Взгляд на методы и средства информационной безопасности при внедрении Интернет-вещей (IoT).
4. Доверие и безопасность в информационном обществе
5. Информационная безопасность и анализ контента в Интернет
6. Информационно-психологическая война и типы информационного оружия
7. Кибершпионаж – технологии выявления и предупреждения.
8. Методы обеспечения информационной безопасности в социальных сетях
9. Мобильная безопасность: мобильные технологии для государства и бизнеса
10. Применение Big Data для обеспечения безопасности информационных систем
11. Проблемы информационной безопасности умного города.
12. Центры компетенции и реагирования на угрозы информационной безопасности
13. Планирование действий в чрезвычайных ситуациях

8. Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1. Основная литература:

1. Гафнер В. В. Информационная безопасность: учеб. пособие / В.В. Гафнер. — Ростов н/Д: Феникс, 2010. — 324 с.
2. Соколов А., Степанюк О. Защита от компьютерного терроризма. – Спб.: Арлит, 2002. –495 стр.

8.2. Дополнительная литература:

1. Системы защиты информации в ведущих зарубежных странах: учебное пособие к проведению практических занятий/ М.А. Буранова, В.В. Пугин. – Самара: ПГУТИ, 2017. – 14 с..
2. Информационная безопасность: методические указания к практическим занятиям / А.В. Крыжановский, И.С. Поздняк – Самара: ПГУТИ, 2018. – 38 с.

8.3. Программное обеспечение и Интернет-ресурсы

1) Сайт НОУ «ИНТУИТ» (http://www.intuit.ru)
2) Информационный портал по безопасности (http://www.securitylab.ru/)
3) Сайт, созданный для публикации новостей, аналитических статей, мыслей, связанных с информационными технологиями, бизнесом и Интернетом (http://habrahabr.ru/)

6) Журнал «Хакер» онлайн (http://www.xakep.ru/)
7) ФСТЭК России (http://fstec.ru/)
8) Лаборатория Касперского (http://www.kaspersky.ru/)

8.4. Методические указания и материалы по видам занятий
Методические указания по выполнению лабораторный и практических работ. (электронный вариант)

9. Материально-техническое обеспечение дисциплины (модуля):

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

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

10. Методические рекомендации по организации изучения дисциплины:

Обучение складывается из аудиторных занятий, включающих лекционный курс, практические занятия, лабораторные работы и самостоятельной работы. Основное учебное время выделяется на лабораторно - практические занятия по закреплению знаний и получении практических навыков.

Работа с учебной литературой рассматривается как вид учебной работы по дисциплине и выполняется в пределах часов, отводимых на её изучение (в разделе СРС).

Каждый обучающийся обеспечен доступом к библиотечным фондам университета и кафедры.

Самостоятельная работа студентов подразумевает подготовку к лабораторно - практическим занятиям, текущему и промежуточному тестированию и включает написание рефератов, работу с учебной литературой, выполнение индивидуальных домашних заданий.

Исходный уровень знаний студентов определяется тестированием, текущий контроль усвоения предмета определяется устным опросом в ходе занятий, ответами на тестовые задания.

В конце изучения учебной дисциплины проводится контроль знаний в виде экзамена.

Рабочая учебная программа по дисциплине «Информационная безопасность» составлена в соответствии с требованиями Федерального Государственного образовательного стандарта ВО по направлению 5.38.03.05 «Бизнес-информатика» и учебного плана по профилю подготовки «Электронный бизнес»

11. Технологическая карта дисциплины

Курс _____2___ группа ЭФ18ДР62ЭБ1 семестр __3___
Преподаватель – лектор доцент Е. В. Саломатина
Преподаватели, ведущие практические занятия - доцент Е. В. Саломатина
Кафедра – Бизнес- информатики и информационных технологий
Весовой коэффициент дисциплины в совокупной рейтинговой оценке, рассчитываемой по всем дисциплинам **(*если введена модульно-рейтинговая система*)**

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):*			
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
Итого:				
ДОПОЛНИТЕЛЬНЫЙ МОДУЛЬ				
Тема, задание или мероприятие дополнительного контроля	Виды текущей аттестации	Аудиторная или внеаудиторная	Минимальное количество баллов	Максимальное количество баллов
Или				
Итого максимум:				

Составитель доцент
Е. В. Саломатина

И. о. Зав. кафедрой БИиИТ доцент
Саломатина Е. В