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

Филиал ПГУ им. Т.Г. Шевченко в г. Рыбница

Кафедра прикладной информатики в экономике

УТВЕРЖДАЮ
Директор филиала ПГУ им. Т.Г. Шевченко в г. Рыбница
профессор _____ И.А. Павлинов
«20» 03 2018г.

РАБОЧАЯ ПРОГРАММА

на 2018/2019 учебный год

Учебной ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки:

09.03.03 Прикладная информатика
(Код и наименование направления подготовки)

Профиль подготовки:

«Прикладная информатика в экономике»
(наименование профиля подготовки)

Квалификация (степень) выпускника

Бакалавр

Форма обучения:

очная

Рыбница 2018

Рабочая программа дисциплины «***Информационная безопасность***» /сост.

А.А. Ляху – Рыбница: ГОУ филиала ПГУ им. Т.Г. Шевченко в г. Рыбница, 2018 - 11 с.

Рабочая программа предназначена для преподавания дисциплины базовой части блока дисциплин (модулей) студентам очной формы обучения по направлению подготовки 09.03.03 – «Прикладная информатика», профиль подготовки – «Прикладная информатика в экономике».

Рабочая программа составлена с учетом Федерального Государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 – «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации № 207 от 12 марта 2015 года.

Составитель _____ **А.А. Ляху, ст. преподаватель**

1. *Цели и задачи освоения дисциплины.*

В результате изучения курса студент должен знать основы теории информационной безопасности , международные стандарты обеспечения информационной безопасности, основы криптографической защиты информации, методики аудита состояния информационной безопасности предприятия.

Студент должен получить навыки поиска и применения в профессиональной деятельности положений международных стандартов в области информационной безопасности, выбора и применения инструментальных средств обеспечения информационной безопасности, реализации простейших криптографических методов защиты информации.

2. *Место дисциплины в структуре ООП ВО.*

Дисциплина входит в базовую часть цикла дисциплин основной образовательной программы подготовки бакалавра по направлению 09.03.03 – «Прикладная информатика».

Формируемые компетенции определяются Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 – «Прикладная информатика».

Освоение дисциплины предполагает знание курса информатики и программирования, информационные системы и технологии.

3. *Требования к результатам освоения дисциплины.*

В соответствии с требованиями ФГОС-3+ ВО в результате освоения дисциплин обучающийся должен овладеть комплексом компетенций. Выполнение этого требования проверяется при аттестации образовательной программы, в том числе путём контроля остаточных знаний обучающихся.

Таблица 1. Распределение компетенций, формируемых в ходе изучения дисциплины

Коды компетенций	Название компетенции	Форма текущего контроля качества компетенции
ОПК – общепрофессиональные компетенции профиля		
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Опорный конспект Задания к лабораторным работам Тестирование
ПК - профессиональные компетенции профиля		
ПК-24	способностью готовить обзоры научной литературы и электронных информационно-образовательных ресурсов для профессиональной деятельности	Опорный конспект Задания к лабораторным работам Тестирование

В результате освоения дисциплины студент должен:

Знать:

- основы теории информационной безопасности;
- международные стандарты в области обеспечения информационной безопасности;
- основы криптографической защиты информации;
- методы, методики и базовые стандарты проведения аудита состояния системы информационной безопасности предприятия.

Уметь:

- осуществлять поиск и применять в профессиональной деятельности положения международных стандартов в области информационной безопасности;
- выбирать и применять инструментальные средства обеспечения информационной безопасности;
- работать с современными системами обеспечения информационной безопасности.

Владеть:

- навыками реализации простейших криптографических методов;
- методами проведения аудита информационной безопасности предприятия.

4. Структура и содержание дисциплины (модуля).

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

Семестр	Трудоемкость, з.е./часы	Количество часов					Форма итогового контроля
		В том числе					
		Аудиторных				Самостоятельной работы	
		Всего	Лекций	Лабораторных работ	Практических занятий		
5	4/144	54	18	36		54	Экзамен
Итого:	**4/144**	**54**	**18**	**36**		**54**	**Экзамен**

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	Основные понятия информационной безопасности.	34	6		8	20
2	Криптографические методы защиты информации.	30	6		16	8
3	Аудит информационной безопасности.	24	6			18
4	Программные средства защиты информации.	20			12	8
Итого:		**108**	**18**		**36**	**54**

4.3. Тематический план по видам учебной деятельности.

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно-наглядные пособия
1	1	2	Роль информации в современном мире. Понятие информационной безопасности государства, компании.	лекционная аудитория, оборудованная мультимедий-ными средствами
2		2	Понятие информационной войны. Предпосылки возникновения информационных войн.	
3		2	Возможные каналы воздействия на информационные потоки государства, компании.	
4	2	2	Криптографическая защита информации. История возникновения криптографии.	
5		2	Шифрование информации методом простой замены. Дешифрование, использование частотного анализа алфавита языка.	
6		2	Шифрование/дешифрование информации по таблице Вижинера. Использование метода Хаффмана для сжатия и криптографической защиты информации.	
7	3	2	Актуальность аудита информационной безопасности предприятия. Информация подлежащая аудиту, цели и задачи аудита.	
8		2	Характеристика информации, как ресурса. Основные показатели, подлежащие оценке. Подходы к созданию комплексной системы ЗИ. Показатели первого и второго вида.	
9		2	Важность и полнота информации. Адекватность информации. Релевантность и толерантность информации. Закон старения информации.	
Итого:		**18**		

Практические занятия (семинары)

Практические занятия учебным планом не предусмотрены.

Лабораторные работы

№ п/п	Номер раздела дисциплины	Объем часов	Тема лабораторного занятия	Наименование лаборатории	Учебно-наглядные пособия
1	1	4	Обзор состояния информационной безопасности в настоящий момент для России и ПМР.	206 ауд.	Задания к лабораторным работам, опорный конспект
2		4	Ведение информационных войн в современном мире. Возможное применение информационного оружия различного вида.		
3	2	4	Создание программы частотного анализа текста. Исследование частот символов в файлах разного типа и их архивах.		
4		4	Шифрование текста методом простой замены. Дешифрование полученной криптограммы с использованием частотного анализа.		
5		4	Шифрование/дешифрование по таблице Вижинера.		
6		4	Обработка текстовых сообщений, используя метод Хаффмана.		
7	4	4	Исследование программных средств защиты информации, предоставляемых ОС Windows.		
8		4	Исследование возможностей архиваторов по шифрованию информации. Частотный анализ архивных файлов.		
9		4	Создание электронной подписи документа. Формирующий алгоритм и проверка подлинности электронной подписи.		
Итого:		**36**			

Самостоятельная работа студента

№ п/п	Раздел дисциплины	Тема и вид СРС	Трудоемкость (в часах)
1	1	Основные государственные структуры, обеспечивающие информационную безопасность России и ПМР.	4
2		Законодательные акты области информационной безопасности.	8
3		Международные стандарты в области информационной безопасности.	4
4		Виды информационного оружия и возможная защита от его применения.	4
5	2	Симметричные и ассиметричные методы шифрования.	8
6	3	Методы проведения аудита информационной безопасности предприятия.	8
7		Модель LCS. Основные этапы модели.	6
8		Комплекс мероприятий по усовершенствованию СИБ компании.	4
9	4	Электронная цифровая подпись документа.	8
10		Подготовка к экзамену по предмету	36
Итого:			**54/36**

5. *Примерная тематика курсовых проектов (работ).*

Выполнение курсовой работы учебным планом не предусмотрено.

6. *Образовательные технологии.*

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
5	Л	Классы с компьютером и мультимедиа проектором	36
5	ЛР	Компьютерный класс с доступом к сети интернет	36

Для повышения наглядности рассматриваемого материала применяются образовательные технологии, основанные на применении специализированных программных сред и технических средств работы с информацией. Например, лекции с мультимедийным сопровождением, с использованием

электронных учебников.

Отдельные темы рассматриваются с использованием технологии проблемного обучения: создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов во время лекции.

Во время проведения лабораторного занятия используются интерактивные технологии обучения, например, дискуссия, коллективное обсуждение какого-либо спорного вопроса, проблемы выбора наиболее эффективного метода решения поставленных задач. Такие субъект-субъектные отношения в ходе образовательного процесса способствуют формированию саморазвивающейся информационно-ресурсной среды.

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 лабораторных 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 экзамена.

Образцы тестов (заданий) для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины, а также для контроля самостоятельной работы студента

Вариант №1

1. Понятие информационной безопасности.
2. Шифрование информации. Метод простой замены.
3. Международные стандарты информационной безопасности.

Вариант №2

1. Виды информационного оружия.
2. Шифрование информации. Метод перестановки.
3. Аудит информационной безопасности предприятия.

Вариант №3

1. Возможные каналы утечки информации.
2. Шифрование информации. Использование таблицы Вижинера.
3. Программные средства защиты информации.

Итоговой формой контроля знаний, умений, владений по дисциплине «Информационная безопасность» является экзамен. Экзамен проводится по билетам, которые включают два теоретических вопроса и практическое задание.

Оценка знаний студентов производится по следующим критериям:

- оценка **«отлично»** выставляется студенту, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логично его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, причем не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач;
- оценка **«хорошо»** выставляется студенту, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;
- оценка **«удовлетворительно»** выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач;

– оценка **«неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

Список вопросов для экзамена

1. Понятие информационной безопасности. Национальные интересы государства.
2. Информационные войны. Предпосылки возникновения.
3. Виды информационного оружия. Защита от применения ИО.
4. Вред от потерь и искажения информации. Методы защиты.
5. Возможности воздействия на информационное поле государства. Внутренние и внешние воздействия.
6. Каналы утечки информации. Возможность похищения информации.
7. Способы и цели воздействия на каналы утечки информации.
8. Меры по предотвращению возможных потерь и искажений информации при передаче и хранении.
9. Актуальность аудита информационной безопасности.
10. Возможные виды аудита безопасности корпоративной информационной системы.
11. Виды аудита безопасности корпоративной информационной системы.
12. Международные стандарты в области аудита безопасности.
13. Мероприятия по усовершенствованию безопасности КИС.
14. Подходы к созданию комплексной системы защиты информации. Показатели первого и второго вида.
15. Показатели оценки информации как ресурса. Важность и полнота информации.
16. Адекватность информации. Закон старения информации.
17. Релевантность и толерантность информации.
18. Классификация методов и средств защиты информации. Общая схема проведения работ по ЗИ.
19. Программные методы защиты информации. Возможности по разграничению доступа, представляемые операционной системой.
20. Криптографические методы защиты информации. Шифрование, стенография, скремблирование.
21. Шифрование методом простой замены. Возможности частотного анализа символьной таблицы при дешифровании.
22. Шифрование по таблице Вижинера. Классический способ и со сдвигом.
23. Возможности по шифрованию информации при архивировании. Метод Хаффмана.
24. Электронная подпись документа. Назначение и целесообразность применения электронной подписи.

Образец теста для проведения итогового контроля по итогам освоения дисциплины, а также для контроля самостоятельной работы студента

1. Информационная война может проводиться:
   a) только после объявления войны, но до начала боевых действий;
   b) только после объявления войны и во время боевых действий;
   c) только после окончания войны;
   d) в любое время при наличии конфликта интересов;
   e) никогда.

2. Информационное оружие от обычных средств поражения отличает:
   a) миниатюрность;
   b) скрытность;
   c) масштабность;
   d) не нанесение физического урона.

3. Основной документ стран ЕС, в котором рассмотрены критерии оценки защищенности информационных технологий, называется:
   a) Красной книгой;
   b) Зеленой книгой;
   c) Белой книгой;
   d) Меморандумом безопасности;
   e) никак не называется.

4. Под интегральной информационной безопасностью понимается:
   a) физическая безопасность;
   b) безопасность аппаратных средств;

c) безопасность программного обеспечения;
d) безопасность связи;
e) комплексная совокупность всех перечисленных мер защиты.

5. Проблемой защиты информации путем ее преобразования занимается:
   a) криптология;
   b) криптография;
   c) криптоанализ;
   d) информатика;
   e) математика.

6. Шифр Цезаря по сути является разновидностью шифра:
   a) замены;
   b) перестановки;
   c) аналитического преобразования;
   d) гаммирования.

7. количество элементов в таблице Вижинера, при количестве символов используемого алфавита N, равно:
   a) N;
   b) 2*N;
   c) N*N;
   d) N*N+2*N;
   e) количество элементов таблицы не зависит от количества символов алфавита.

8. При шифровании методом гаммирования гаммой называется:
   a) исходное сообщение;
   b) зашифрованное сообщение;
   c) специальная последовательность, с которой складывается исходное сообщение;
   d) совокупность исходного и зашифрованного сообщения;
   e) математическая функция преобразования исходного сообщения.

9. Частотный анализ символов алфавита используется при дешифровании сообщений, зашифрованных методом:
   a) замены;
   b) перестановки;
   c) аналитического преобразования;
   d) гаммирования;
   e) всех указанных методов.

10. Глубина дерева при использовании метода Хаффмана определяется:
    a) основанием выбранной системы счисления;
    b) количеством символов используемого алфавита;
    c) количеством символов исходного сообщения;
    d) размером ключа;
    e) глубина является константой.

11. Размер итогового сообщения при использовании метода Хаффмана:
    a) равен размеру исходного сообщения;
    b) больше размера исходного сообщения;
    c) больше либо равен размеру исходного сообщения;
    d) меньше размера исходного сообщения;
    e) меньше либо равен размеру исходного сообщения.

12. Аудит состояния информационной безопасности предприятия должны проводить:
    a) руководство предприятия;
    b) специалисты отдела АСУ;
    c) системные администраторы;
    d) специалисты сторонних фирм;
    e) специалисты структур госбезопасности.

13. Аудит состояния информационной безопасности проводится:
    a) ежемесячно;
    b) ежеквартально;
    c) ежегодно;
    d) один раз, при сдаче информационной системы предприятия в эксплуатацию;
    e) при любых изменения информационной системы предприятия;
    f) период определяется политикой информационной безопасности предприятия.

14. К характеристикам информации как ресурса относятся:
    a) объем;
    b) система счисления;
    c) важность;
    d) адекватность;
    e) степень сжатия;
    f) полнота.

Контроль самостоятельной работы студентов

Формы контроля самостоятельной работы студентов: доклад, ответы на тестирование.

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

8.1. Основная литература:

1. Галатенко В.А. Информационная безопасность. М.:Финансы и статистика, 2007. 158с.
2. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МИФИ, 2008.
3. Зима В.М., Молдовян А.А., Молдовян Н.А. Защита компьютерных ресурсов от несанкционированных действий пользователей. Учебное пособие. СПб., 2007.
4. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие. М.: ФОРУМ: ИНФРА–М, 2012. 368с.

8.2. Дополнительная литература:

1. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Военное издательство, 1992. 39с.
2. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М.: Военное издательство, 1992. 12с.
3. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: Военное издательство, 1992. 12с.
4. Федеральный закон «Об информации, информатизации и защите информации». Собрание законодательства Российской Федерации. 20 февраля 1995 г. Официальное издание. М.: Издательство «Юридическая литература», Администрация Президента Российской Федерации. С 1213–1225.
5. Аскеров Т.М. Защита информации и информационная безопасность. Учебное пособие/ Под общей редакцией К.И. Курбакова. М:Рос. экон. акад., 2001. 387с.
6. Мельников В. Защита информации в компьютерных системах. М.: «Финансы и статистика», «Электронинформ», 2007. 364с.
7. Нечаев В.И. Элементы криптографии (Основы теории защиты информации)Учебное пособие/ под редакцией В.А. Садовничего. М.: Высшая школа, 1999. 109с.
8. Ухлинов Л.М. Международные стандарты в области обеспечения безопасности данных в сетях ЭВМ. Состояние и направление развития. М.: Электросвязь, 1991.
9. Барсуков В.С., Водолазский В.В. Интегральная безопасность информационно–вычислительных и телекоммуникационных сетей (часть 1). Технология электронных коммуникаций. М., 2003.

8.3. Программное обеспечение и Интернет-ресурсы:

1. http://univertv.ru/video/matematika/ Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вас вопросу.
2. http://elibrary.ru Научная электронная библиотека eLIBRARY.RU. Крупнейший российский информационный портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 12 млн научных статей и публикаций. На платформе eLIBRARY.RU доступны электронные версии более 1400 российских научно-технических журналов, в том числе более 500 журналов в открытом доступе.
3. http://www.iqlib.ru/ Электронная библиотека IQlib образовательных и просветительских изданий. Образовательный ресурс, объединяющий в себе интернет-библиотеку и пользовательские сервисы для полноценной работы с библиотечными фондами. Свободный доступ к электронным учебникам, справочным и учебным пособиям. Аудитория электронной библиотеки IQlib - студенты, преподаватели учебных заведений, научные сотрудники и все те, кто хочет повысить свой уровень знаний.
4. http://eqworld.ipmnet.ru/ru/library.htm Учебно-образовательная физико-математическая библиотека. Электронная библиотека содержит DjVu- и PDF-файлы учебников, учебных пособий, сборников задач и упражнений, конспектов лекций, монографий, справочников и диссертаций по математике, механике и физике. Все материалы присланы авторами и читателями или взяты из Интернета (из www архивов открытого доступа).

8.4. 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.

9. Материально-техническое обеспечение дисциплины (модуля).

Для осуществления образовательного процесса по дисциплине «Информационная безопасность» необходим компьютерный класс, а также лекционная аудитория, оборудованная мультимедийными средствами для демонстрации лекций-презентаций.

Карта обеспечения дисциплины учебными материалами:

№ п/п	Наименование	Вид	Форма доступа
1	Учебно-методическая литература по дисциплине «Информационная безопасность»	Электронный	Электронная библиотека
2	Описание лабораторных работ	Электронный	Электронная библиотека
3	Мультимедийные материалы	Сетевой	Портал филиала ПГУ им. Т.Г. Шевченко в г. Рыбница
4	Электронная библиотека	Сетевой	Портал филиала ПГУ им. Т.Г. Шевченко в г. Рыбница

Карта обеспечения дисциплины оборудованием:

№ п/п	Номер аудитории	Кол-во	Наименование	Форма использования
1	Аудитория № 206	10	Компьютеры типа Pentium, объединенные локальной сетью. Операционная система Windows. Расширенный пакет Office (Word, Excel, Access, PowerPoint). Глобальная сеть.	Организация лабораторных работ, доступ к образовательным ресурсам во время самостоятельной работы студентов, работа с мультимедийными материалами на занятиях.

10. Методические рекомендации по организации изучения дисциплины.

При преподавании курса необходимо ориентироваться на современные образовательные технологии. Аудиторная и самостоятельная работы должны быть направлены на углубление и расширение полученных знаний, на закрепление приобретенных навыков и применение формируемых компетенций. Кроме того, рекомендуется использовать дифференцированное обучение и активные методы проверки знаний при

проведении проверочных работ, тестирования. Это достигается, например, путем организации индивидуальной самостоятельной работы студентов.

При проведении промежуточной аттестации, независимо от формы ее проведения (устной или письменной), важно учесть все виды работ, оценить уровень знаний студентов по всем разделам учебной дисциплины.

Примерный перечень экзаменационных вопросов должен доводиться до студентов в начале изучения дисциплины. При необходимости он может быть уточнен не позднее, чем за месяц до начала экзаменационной сессии. На его основе составляются экзаменационные билеты, утверждаемые заведующим кафедрой.

11. Технологическая карта дисциплины.

Кредитно-модульная система по дисциплине не предусмотрена.

Составитель _____ А.А. Ляху, ст. преподаватель

Зав. кафедрой прикладной информатики

в экономике _____ / Павлинов Игорь Алексеевич, профессор/

Согласовано:

1. Зав. выпускающей кафедры _____ / Павлинов Игорь Алексеевич, профессор/

2. Директор филиала ПГУ
им. Т.Г. Шевченко в г. Рыбница _____ / Павлинов Игорь Алексеевич, профессор/