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

Кафедра Бизнес-информатики и информационных технологий

УТВЕРЖДАЮ
Декан экономического факультета
Смоленский Н. Н.
(подпись, расшифровка подписи)
"17" 09 2016 г

РАБОЧАЯ ПРОГРАММА

Учебной ДИСЦИПЛИНЫ

«Информационная безопасность»

38.03.05 Бизнес-информатика

(Код и наименование направления подготовки)

Электронный бизнес

(наименование профиля подготовки)

квалификация (степень) выпускника
Бакалавр

Форма обучения:
очная

Тирасполь 2016

Рабочая программа дисциплины «***Информационная безопасность***» /автор Д. т. н., В. К. Сарьян – Тирасполь: ГОУ ПГУ, 2016. - 14 с.

РАБОЧАЯ ПРОГРАММА ПРЕДНАЗНАЧЕНА ДЛЯ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ ВАРИАТИВНОЙ ЧАСТИ ПРОГРАММЫ БАКАЛАВРИАТА СТУДЕНТАМ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 38.03.05 – *БИЗНЕС-ИНФОРМАТИКА*

Рабочая программа составлена с учетом Федерального Государственного образовательного стандарта высшего образования по направлению подготовки 38.03.05 - *Бизнес-информатика*, утвержденного приказом *№1002 от 11.08.2016 МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ.*

Автор _____ **/ Ф.И.О./**
(подпись)

__.__.2016 г.

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 ВПО

Дисциплина «Информационная безопасность» относится к вариативной части программы бакалавриата по направлению 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-1, ПК-9

Код компетенции	**Формулировка компетенции**
ОПК-1	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью 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	48	18	12	16	26+36	Экзамен
Итого:	**3/ 108**	**48**	**18**	**12**	**16**	**62**	**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	Общие вопросы информационной безопасности	***14***	***4***	***4***		***6***
2	Государственная система информационной безопасности	***13***	***4***			***4***
3	Угрозы информационной безопасности и методы их реализации	***14***	***2***	***4***	***4***	***4***
4	Методы и средства обеспечения информационной безопасности информационных систем	***18***	***6***	***4***	***8***	***4***
5	Стандартизация в области информационной безопасности	***22***	***2***	***4***		***8***
Итого:		***81***	***18***	***16***	***12***	***26***
Подготовка к экзамену						***36***
Всего:		***108***	***18***	***16***	***12***	***60***

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. Взаимодействие человеко-машинных и интернет-вещей в информационно-коммуникационной среде. Понятие доверенной среды интероперабельности (семантической, технологической, социальной и др), трансграничности, контекста и др.	Лекция-презентация
2	2	4	**Государственная система информационной безопасности.** Национальные интересы в информационно-коммуникационной сфере и ее обеспечение. Концепция информационной безопасности. Использование средств ИКТ для обеспечения безопасности жизнедеятельности информационного общества.	Лекция-презентация
3	3	2	**Угрозы информационной безопасности и методы их реализации.** Понятие угрозы. Классификация угроз информационной безопасности. Виды угроз. Человеческий фактор.	Лекция-презентация

4	4	6	**Методы и средства обеспечения информационной безопасности информационных систем.** Модели, методы защиты информации. Информационная безопасность сетей, Интернет вещей, облачные технологии. Безопасность в международных платёжных системах. Обеспечение информационной безопасности в системе оповещения и эвакуации при чрезвычайных ситуациях в транспорте, системе организации охранного видеонаблюдения и т.д. Системы защиты информации за рубежом	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	3	4	Работа с реестром Windows. основные возможности обеспечения безопасности с помощью реестра ОС от вредоносных программ	Методические указания
3	4	4	Парольная защита. Advanced Office Password Recovery. Оценка стойкости парольных систем	Методические указания
4	5	2	Создание электронной подписи в документе	Методические указания
5	5	2	Подготовка документации для формирования профиля защиты	Методические указания
Итого:		***16***		

Лабораторные работы

№ п/п	Номер раздела дисциплины	Объем часов	Тема лабораторного занятия	Наименование лаборатории	Учебно-наглядные пособия
1	3	4	Спам и методы борьбы с ним	Компьютерный класс	Методические указания
2	4	4	Вопросы защиты от перехвата данных в семействе операционных систем Windows.	Компьютерный класс	Методические указания
3	4	4	Программа Steganos Security Suite Программа Digital Security Office	Компьютерный класс	Методические указания
Итого:		***12***			

Самостоятельная работа студента

Раздел дисциплины	№ п/п	Тема и вид СРС	Трудоемкость (в часах)
Раздел 1	1	*Веб-квест «Информационная безопасность».* Подготовка	2

		реферативного доклада.	
	2	*Общие вопросы информационной безопасности.* Работа с информационными ресурсами.	4
Раздел 2	3	*Концепция информационной безопасности*. Работа с основной и дополнительной литературой	4
Раздел 3	4	*Человеческий фактор как самый чувствительный компонент информационной безопасности.* Работа с основной и дополнительной литературой	2
	5	*Спам и методы борьбы с ним*. Самостоятельная работа под контролем преподавателя (в форме индивидуальных консультаций).	2
Раздел 4	6	*Программы удаленного доступа.* Подготовка по заданиям для самостоятельного индивидуального исполнения.	2
	7	*Оценка стойкости парольных систем.* Подготовка к занятиям практического цикла.	2
Раздел 5	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:			***26***

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

В соответствии с ФГОС 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.	2
Итого:			**10**

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. Основные угрозы доступности информации:
   - *непреднамеренные ошибки пользователей*
   - злонамеренное изменение данных
   - хакерская атака
   - *отказ программного и аппаратно обеспечения*
   - *разрушение или повреждение помещений*
   - перехват данных

2. Суть компрометации информации
   - внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
   - несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
   - *внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений*

3. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

- *с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды*
- с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
- способна противостоять только информационным угрозам, как внешним так и внутренним
- способна противостоять только внешним информационным угрозам

4. Методы повышения достоверности входных данных
   - *Замена процесса ввода значения процессом выбора значения из предлагаемого множества*
   - Отказ от использования данных
   - Проведение комплекса регламентных работ
   - *Использование вместо ввода значения его считывание с машиночитаемого носителя*
   - *Введение избыточности в документ первоисточник*
   - Многократный ввод данных и сличение введенных значений
5. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)
   - *МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения*
   - МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
   - МЭ работают только на сетевом уровне, а СОВ – еще и на физическом
6. Сервисы безопасности:
   - *идентификация и аутентификация*
   - *шифрование*
   - инверсия паролей
   - *контроль целостности*
   - регулирование конфликтов
   - *экранирование*
   - *обеспечение безопасного восстановления*
   - кэширование записей
7. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
   - *несанкционированного управления удаленным компьютером*
   - внедрения агрессивного программного кода в рамках активных объектов Web-страниц
   - перехвата или подмены данных на путях транспортировки
   - вмешательства в личную жизнь
   - поставки неприемлемого содержания
8. Причины возникновения ошибки в данных
   - *Погрешность измерений*
   - *Ошибка при записи результатов измерений в промежуточный документ*
   - Неверная интерпретация данных
   - *Ошибки при переносе данных с промежуточного документа в компьютер*
   - Использование недопустимых методов анализа данных
   - Неустранимые причины природного характера
   - *Преднамеренное искажение данных*
   - *Ошибки при идентификации объекта или субъекта хозяйственной деятельности*
9. К формам защиты информации не относится…
   - *аналитическая*
   - правовая
   - организационно-техническая
   - *страховая*
10. Наиболее эффективное средство для защиты от сетевых атак
    - *использование сетевых экранов или «firewall»*
    - использование антивирусных программ

- посещение только «надёжных» Интернет-узлов
- использование только сертифицированных программ-броузеров при доступе к сети Интернет

11. Информация, составляющая государственную тайну не может иметь гриф…
    - *«для служебного пользования»*
    - «секретно»
    - «совершенно секретно»
    - «особой важности»
12. Разделы современной криптографии:
    - *Симметричные криптосистемы*
    - *Криптосистемы с открытым ключом*
    - Криптосистемы с дублированием защиты
    - *Системы электронной подписи*
    - Управление паролями
    - Управление передачей данных
    - *Управление ключами*
13. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности
    - рекомендации X.800
    - *Оранжевая книга*
    - Закон «Об информации, информационных технологиях и о защите информации»
14. Утечка информации – это …
    - *несанкционированный процесс переноса информации от источника к злоумышленнику*
    - процесс раскрытия секретной информации
    - процесс уничтожения информации
    - непреднамеренная утрата носителя информации
15. Основные угрозы конфиденциальности информации:
    - *маскарад*
    - карнавал
    - переадресовка
    - *перехват данных*
    - блокирование
    - *злоупотребления полномочиями*
16. Элементы знака охраны авторского права:
    - *буквы С в окружности или круглых скобках*
    - буквы Р в окружности или круглых скобках
    - *наименования (имени) правообладателя*
    - наименование охраняемого объекта
    - *года первого выпуска программы*
17. Защита информации обеспечивается применением антивирусных средств
    - **да**
    - нет
    - не всегда
18. Средства защиты объектов файловой системы основаны на…
    - *определении прав пользователя на операции с файлами и каталогами*
    - задании атрибутов файлов и каталогов, независящих от прав пользователей
19. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза
    - активная
    - *пассивная*
20. Преднамеренная угроза безопасности информации
    - *кража*
    - наводнение

- повреждение кабеля, по которому идет передача, в связи с погодными условиями ошибка разработчика

21. Концепция системы защиты от информационного оружия не должна включать…
    - *средства нанесения контратаки с помощью информационного оружия*
    - механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
    - признаки, сигнализирующие о возможном нападении
    - процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей
22. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …
    - *обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации*
    - *реализацию права на доступ к информации»*
    - соблюдение норм международного права в сфере информационной безопасности
    - выявление нарушителей и привлечение их к ответственности
    - *соблюдение конфиденциальности информации ограниченного доступа*
    - разработку методов и усовершенствование средств информационной безопасности

7.3. Для итогового контроля:

1. Программа информационной безопасности России и пути ее реализации.
2. Концепция информационной безопасности.
3. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена.
4. Основные принципы защиты информации в компьютерных системах.
5. Основные понятия и определения защиты информации.
6. Правовое обеспечение информационной безопасности.
7. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
8. Организационное обеспечение информационной безопасности.
9. Понятие угрозы. Анализ угроз безопасности информации.
10. Причины, виды, каналы утечки и искажения информации.
11. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации.
12. Информационная безопасность в условиях функционирования в России глобальных сетей.
13. Общая проблема информационной безопасности информационных систем.
14. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение).
15. Компьютерные средства реализации защиты в информационных системах. Политика безопасности.
16. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
17. Использование защищенных компьютерных систем. Стандарты по оценке защищенных систем.
18. Методы перехвата и навязывания информации.
19. Компьютерные вирусы. Понятия о видах вирусов.
20. Современные антивирусные программы.
21. Общие подходы к построению парольных систем.
22. Особенности криптографического и стеганографического преобразования информации. Стойкость алгоритмов шифрования. Типы алгоритмов шифрования.
23. Особенности применения криптографических методов.
24. Электронная подпись.
25. Техническая защита от несанкционированного копирования. Базовые методы нейтрализации систем защиты от несанкционированного копирования.

26. Идентификация параметров персонального компьютера.
27. Подходы к построению защищенной операционной системы. Административные меры защиты.
28. Выбор модели безопасности.
29. Классификация способов несанкционированного доступа и жизненный цикл атак.
30. Нападения на политику безопасности и процедуры административного управления.
31. Нападения на постоянные и сменные компоненты системы защиты.
32. Нападения на протоколы информационного взаимодействия.
33. Нападения на функциональные элементы компьютерных сетей.
34. Способы противодействия несанкционированному сетевому и межсетевому доступу.
35. Аутентификация пользователя локальной сети.
36. Разграничение доступа к локальной сети.
37. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall). Критерии их оценки.
38. Защита виртуальных потоков на различных сетевых уровнях.
39. Защита удаленного доступа к локальной сети.
40. Безопасная доставка E-mail сообщений. Использование ключей и цифровых подписей.
41. Сертификация серверов Интернет. Безопасность работы в Интернет с использованием браузера.
42. Защита информации для электронной коммерции в Интернет.

7.4. 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. Кибершпионаж – технологии выявления и предупреждения.
7. Методы обеспечения информационной безопасности в социальных сетях
8. Мобильная безопасность: мобильные технологии для государства и бизнеса
9. Применение Big Data для обеспечения безопасности информационных систем
10. Проблемы информационной безопасности умного города.
11. Роль защитных экранов в обеспечении безопасности интернет-порталов.
12. Фильтрация контента как один из способов обеспечения информационной безопасности.
13. Центры компетенции и реагирования на угрозы информационной безопасности

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

8.1. Основная литература:

1. МСЭ-Т Рекомендация X.805 (10/2003) Архитектура безопасности для систем обеспечивающих связь “от конца до конца”
2. Ховард М., Лебланк Д. Защищенный код/Пер. с англ. – М.: Издательско-торговый дом «Русская Редакция», 2003. – 704 стр.
3. Основы информационной безопасности. Курс лекций. Учебное пособие / Издание второе, исправленное / Галатенко В.А. Под редакцией члена-корреспондента РАН В.Б. Бетелина / М.: Интуит.ру «Интернет-университет Информационных технологий», 2004. – 264 с. - ISBN 5955600159.
4. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2005. – 144 с.
5. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др]. – М.: Горячая линия – Телеком, 2006. – 544 с.
6. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1995.

8.2. Дополнительная литература:

1. Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd Edition. Ross J. Anderson. - John Wiley and Sons, 2008. – 1040 p. - ISBN 0470068523, 9780470068526.
2. С. С. Корт. Теоретические основы защиты информации. - Гелиос АРВ, 2004 г. - 240 стр. - ISBN 5-85438-010-2.
3. Щербаков А. Ю., Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.:Книжный мир, 2009. — 352 с — ISBN 978-5-8041-0378-2.
4. А. А. Губенков, В. Б. Байбурин. Информационная безопасность. - Новый издательский дом, 2005 г. - 128 стр. - ISBN 5-9643-0091-X.
5. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с — ISBN 978-5-388-00069-9.
6. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с — ISBN 5-9556-0053-1.
7. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с — ISBN 5-94074-383-8.
8. А. Ю. Щеглов. Защита компьютерной информации от несанкционированного доступа. - Наука и техника, 2004 г. - 384 стр. - ISBN 5-94387-123-3.
9. Ричард Э. Смит. Аутентификация. От паролей до открытых ключей. [Authentication: From Passwords to Public Keys] - Вильямс, 2002 г. - 432 стр. - ISBN 5-8459-0341-6, 0-201-61599-1.
10. Л. К. Бабенко, С. С. Ищуков, О. Б. Макаревич. Защита информации с использованием смарт-карт и электронных брелоков. - Гелиос АРВ, 2003 г. - 352 стр. - ISBN 5-85438-093-5.
11. Информационная безопасность / Information Security. - Оружие и технологии России, 2008 г. - 256 стр. - ISBN 978-5-93799-043-3.
12. Джон Чирилло. Обнаружение хакерских атак. [Hack Attacks Revealed] - Питер, 2003 г. - 864 стр. - ISBN 5-318-00533-0.
13. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. — 176 с — ISBN 978-985-463-258-2.
14. Кевин Д. Митник, Вильям Л. Саймон. Искусство вторжения. - ДМК пресс, Компания АйТи, 2005 г. - 280 стр. - ISBN 5-98453-020-1, 0-76456-959-7.
15. Дмитрий Скляров. Искусство защиты и взлома информации. - БХВ-Петербург, 2004 г. - 288 стр. - ISBN 5-94157-331-6.

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/)
4) Архив изданий по информационной безопасности(http://www.itsec.ru/articles2/allpubliks)
5) Отслеживание тенденций, аналитика, информирование о наиболее значимых событиях (http://bugtraq.ru/)
6) Журнал «Хакер» онлайн (http://www.xakep.ru/)
7) ФСТЭК России (http://fstec.ru/)
8) Лаборатория Касперского (http://www.kaspersky.ru/)
9) Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В.В. Соломатина (http://www.vniins.ru/)
10) Международный консорциум по сертификации в области информационной безопасности (https://www.isc2.org/)
11) Институт специалистов по компьютерной безопасности SANS (http://www.sans.org/)

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 38.03.05 «Бизнес-информатика» и учебного плана по профилю подготовки «Электронный бизнес»

11. Технологическая карта дисциплины

Курс _____2_____ группа ____201_____ семестр _____3_____
Преподаватель – лектор д. т. н., профессор В. К. Сарьян
Преподаватели, ведущие практические занятия - д. т. н., профессор В. К. Сарьян
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:				

Автор

д. т. н., профессор
В. К. Сарьян

И. о. Зав. кафедрой (обслуживающей дисциплину)

ст. преподаватель
Саломатина Е. В