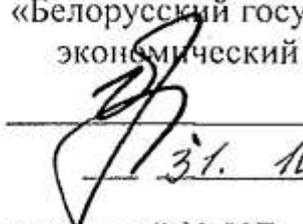


Учреждение образования
«Белорусский государственный экономический университет»

УТВЕРЖДАЮ

Ректор учреждения образования
«Белорусский государственный
экономический университет»

 В.Н. Шимов

31. 10. 2017 г.

Регистрационный № УД - 3409-17/уч.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности

1-25 81 10 Экономическая информатика

2017

СОСТАВИТЕЛИ:

Гордич А.А., доцент кафедры информационных технологий учреждения образования «Белорусский государственный экономический университет», кандидат технических наук, доцент.

РЕЦЕНЗЕНТЫ:

Минченков Ю.В., доцент кафедры менеджмента технологий учреждения образования «Белорусский государственный университет», кандидат физико-математических наук, доцент;

Кривец А.Ф., доцент кафедры информационно-вычислительных систем учреждения образования «Военная академия Республики Беларусь», кандидат технических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой информационных технологий учреждения образования «Белорусский государственный экономический университет»

(протокол № 2 от 21 сентября 2017 г.);

Научно-методическим советом учреждения образования «Белорусский государственный экономический университет»

(протокол № 1 от 19.10.2017)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дисциплина «Безопасность информационных систем» предназначена для освоения магистрантами, обучающимися по специальности 1-25 81 10 «Экономическая информатика» магистерской программы «Цифровые бизнес-коммуникации», современных методов и средств защиты информации в корпоративных информационных системах из проблемной области, в которой они специализируются.

Цели изучения дисциплины:

- формирование аналитических способностей, позволяющих делать обоснованный выбор системы комплексной защиты корпоративной информации при решении задач из проблемной области, в которой магистранты специализируются;
- подготовка к участию в разработке и создании комплексной системы защиты корпоративной информационной системы;
- подготовка к использованию современных методов и средств защиты информации в корпоративных информационных системах;
- ознакомление с основами построения систем управления безопасностью корпоративных информационных систем.

Задачи изучения дисциплины сводятся к следующему:

- получение знаний о методах и средствах защиты информации в корпоративных информационных системах;
- освоение теоретических основ построения комплексной защиты корпоративной информационной системы;
- знакомство с современными системами управления безопасностью корпоративных информационных систем;
- освоение принципов криптографической и стеганографической защиты информации;
- выработка навыков защиты информации в корпоративных информационных системах.

I. Требования к академической компетенции специалиста

Магистрант должен:

- АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач;
- АК-2. Владеть системным и сравнительным анализом;
- АК-3. Владеть исследовательскими навыками;
- АК-4. Уметь работать самостоятельно;
- АК-5. Быть способным порождать новые идеи (обладать креативностью);
- АК-6. Владеть междисциплинарным подходом при решении проблем;
- АК-7. Иметь навыки использования технических устройств, управления информацией и работы с компьютером;
- АК-8. Уметь формулировать проблему и ставить задачу в конкретной предметной области;
- АК-9. Владеть навыками устной и письменной коммуникации;

–АК-10. Уметь учиться и повышать свою квалификацию в течение всей жизни.

2. Требования к социально-личностным компетенциям специалиста

Магистрант должен:

- СЛК-2. Быть способным к социальному воздействию;
- СЛК-3. Овладеть способностью к межличностным коммуникациям;
- СЛК-6. Уметь работать в команде.

3. Требования к профессиональным компетенциям специалиста

Магистрант должен уметь:

- ПК-1. Находить современные системы управления безопасностью корпоративных информационных систем;
- ПК-10. Определять сферы применения научно-технических идей и разработок для защиты информации в корпоративных информационных системах;
- ПК-11. Ориентироваться во внешней среде инновационного предпринимательства.

В результате изучения дисциплины «Безопасность информационных систем» магистрант должен:

знать:

- основные понятия информационной безопасности;
- угрозы информационной безопасности для корпоративных информационных систем;
- криптографические методы защиты информации, процедуры формирования и проверки электронной цифровой подписи;
- стеганографические методы защиты информации;
- принципы комплексной защиты корпоративной информации;
- методы защиты информации в компьютерных сетях;
- принципы построения виртуальных защищенных сетей;
- основы межсетевого экранирования;
- стандарты информационной безопасности;
- основы построения систем управления безопасностью корпоративных информационных систем;
- принципы аудита и мониторинга безопасности корпоративных информационных систем;

уметь:

- использовать современные криптосистемы шифрования;
- готовить предложения по созданию комплексных систем защиты корпоративной информации;
- использовать современные стеганографические системы защиты информации;
- реализовывать процедуры формирования и проверки электронной цифровой подписи;

- использовать виртуальные защищенные каналы;
- анализировать системы управления безопасностью корпоративных информационных систем;

владеть:

- навыками применения современных программных средств для реализации процедур криптографической и стеганографической защиты информации;
- навыками формирования и проверки электронной цифровой подписи;
- методами аудита и мониторинга безопасности корпоративных информационных систем.

Изучение дисциплины осуществляется на лекциях и лабораторных занятиях. Основное внимание уделяется изучению новых методологий и обзорам современных программных средств обеспечения безопасности корпоративных информационных систем. Закрепление теоретических знаний и практических навыков, а также развитие исследовательских и познавательных способностей реализуется в рамках самостоятельной и управляемой самостоятельной работы студентов (УСРС).

В соответствии с учебным планом специальности 1-25 81 10 «Экономическая информатика» и магистерской программой «Цифровые бизнес-коммуникации» учебная программа рассчитана на 48 часов, из них аудиторных занятий 24 часа. Распределение по видам занятий для дневной и заочной форм обучения: лекций – 10 часов (6 часов для заочной), лабораторных занятий – 14 часов (6 часов для заочной).

Рекомендуемые формы контроля – устный опрос, защита лабораторных работ, контрольные работы, индивидуальные задания, зачет.

Знания и навыки, приобретенные при освоении курса «Безопасность информационных систем», могут использоваться для выполнения научных работ и магистерских диссертаций.

II. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Основные понятия информационной безопасности

Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности. Политика информационной безопасности. Разработка политики безопасности организации.

Тема 2. Информационная безопасность компьютерных сетей

Анализ угроз сетевой безопасности. Угрозы и уязвимости беспроводных сетей. Обеспечение информационной безопасности компьютерных сетей. Методы обеспечения информационной безопасности.

Тема 3. Криптографическая и стеганографическая защита информации

Основные понятия криптографической защиты информации. Симметричные и асимметричные криптосистемы шифрования. Электронная цифровая подпись (ЭЦП). Функции хэширования. Стеганографические системы защиты информации.

Тема 4. Комплексная защита корпоративной информации

Структура системы защиты информации в корпоративной информационной системе (КИС). Комплексный подход к обеспечению информационной безопасности КИС. Функции межсетевых экранов. Экранирующий маршрутизатор. Концепция построения виртуальных защищенных сетей (VPN). Основные понятия и функции сети VPN. Средства обеспечения безопасности VPN.

Тема 5. Управление информационной безопасностью

Задачи управления информационной безопасностью. Архитектура управления информационной безопасностью КИС. Аудит и мониторинг безопасности КИС. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты информационной безопасности Республики Беларусь.

**УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ «Безопасность информационных систем»
для дневной формы получения высшего образования**

Номер темы	Название темы	Количество аудиторных часов				Литература	Форма контроля знаний
		Лекции	Лабораторные занятия	Количество часов УСРС			
				Лекции	Лабораторные занятия		
1	Основные понятия информационной безопасности	2				[1, 2-6]	Защита лабораторной работы по теме 1
2	Информационная безопасность компьютерных сетей	2	4			[1-5, 7-14]	Защита лабораторной работы по теме 2
3	Криптографическая и стеганографическая защита информации	2	6			[1-5, 7-14]	Защита лабораторной работы по теме 3
4	Комплексная защита корпоративной информации	2	2			[1, 3-6, 10-12]	Защита лабораторной работы по теме 4
5	Управление информационной безопасностью	2	2			[1, 3, 6]	Защита лабораторной работы по теме 5
Итого		10	14				ЗАЧЕТ

**УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ «Безопасность информационных систем»
для заочной формы получения высшего образования**

Номер темы	Название темы	Количество аудиторных часов				Литература	Форма контроля знаний
		Лекции	Лабораторные занятия	Количество часов УСРС			
				Лекции	Лабораторные занятия		
1	Основные понятия информационной безопасности	2				[1, 2-6]	
2	Информационная безопасность компьютерных сетей					[1-5, 7-14]	
3	Криптографическая и стеганографическая защита информации	2	4			[1-5, 7-14]	Защита лабораторной работы по теме 3
4	Комплексная защита корпоративной информации	2	2			[1, 3-6, 10-12]	Защита лабораторной работы по теме 4
5	Управление информационной безопасностью					[1, 3, 6]	
Итого		6	6				ЗАЧЕТ

ЛИТЕРАТУРА

Основная

1. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах. – М. : Форум : Инфра-М, 2016. – 591 с.
2. Ганжа, В.А. Компьютерные сети. Информационная безопасность и сохранение информации /В.А.Ганжа, В.В.Сидорик, О.И.Чичко. – Минск: БГУИР, 2014. – 128 с.
3. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы /В.Олифер, Н.Олифер. СПб: Питер, 2016. - 991 с.
4. Баранова, Е.К. Информационная безопасность и защита информации / Е.К.Баранова, А.В.Бабаш. – М. : Риор : Инфра-М, 2016. - 320 с.
5. Нестеров, С. А. Информационная безопасность. – М. : Юрайт, 2016. - 321 с.
6. Гришина, Н.В. Информационная безопасность предприятия. – М. : Форум : Инфра-М, 2016. – 238 с.

Дополнительная

7. Информатика. Базовый курс /С.В.Симонович. СПб: Питер, 2016. – 637 с.
8. Основы криптологии /Ю.С.Харин [и др.] - Минск: Новое знание, 2003. - 381с.
9. Шнайер, Б. Прикладная криптография - М. : Триумф, 2002. – 758 с.
10. Романец, Ю.В. Защита информации в компьютерных системах и сетях /Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин. - М. : Радио и связь, 1999. – 328 с.
11. Ерохин, В.В. Безопасность информационных систем /В.В.Ерохин, Д.А.Погоньшева, И.Г.Степченко. – М. : Флинта : Наука, 2015. – 182 с.
12. Партыка, Т.Л. Информационная безопасность / Т.Л.Партыка, И.И.Попов. – М. : Форум : Инфра-М, 2007. – 367 с.
13. Бабаш, А.В. Информационная безопасность /А.В.Бабаш, Е.К.Баранова, Ю.Н.Мельников. – М. : КноРус, 2016. – 131 с.
14. Баранова, Е.К. Криптографические методы защиты информации / Е.К.Баранова, А.В.Бабаш. – М. : КноРус, 2015. – 196 с.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО

НА 2018/2019 учебный год

№ п/п	Дополнения и изменения	Основание
	Дополнений и изменений нет	

Учебная программа пересмотрена и одобрена на заседании кафедры информационных технологий (протокол № 10 от 31 мая 2018 г.)

Заведующий кафедрой
информационных
технологий



М.Н. Садовская