

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ**

**ГОСУДАРСТВЕННАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**
«Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»

**КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
УПРАВЛЕНИЯ**

Д.В. Глотова, Н.С. Пальчикова

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

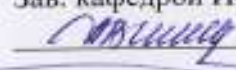
УЧЕБНОЕ ПОСОБИЕ

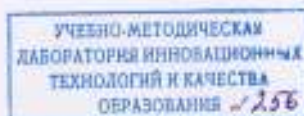
для студентов

специальности 38.05.01 Экономическая безопасность

очной и заочной форм обучения

Утверждено
на заседании кафедры информационных
систем и технологий управления
Протокол № 18 от 18 февраля 2020 г.
Зав. кафедрой ИСТУ

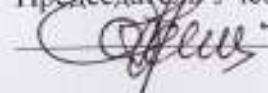
 А.В. Шершнёва



Одобрено
учебно-методическим советом
ГО ВПО «ДонНУЭТ»

Протокол № 8 от 17.03. 2020 г.

Председатель Учебно-методического совета

 Л.А. Омелянович

Донецк
ГО ВПО «ДонНУЭТ»
2020

УДК 004.056:33(076.6)
ББК 32.973.26-018.2я73+65-98я73

Г54

Рецензенты:

А.В. Шершнёва, канд. экон. наук, доц.;
Ю.В. Нефёдова, канд. экон. наук, доц.;

Глотова Д.В.

Г 54 Информационная безопасность [текст]: учеб. пособ. для студ. специальности 38.05.01 Экономическая безопасность очной и заочной форм обучения; Государственная организация высшего профессионального образования «Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского», каф. информац. систем и технологий упр. – Донецк: [ГО ВПО «ДонНУЭТ»], 2020 – 155 с.

Учебное пособие охватывает такие смысловые модули, как: «Информационная безопасность в экономических информационных системах», «Инструменты защиты информации в экономических информационных системах», «Проверка состояния информационной безопасности в экономических информационных системах». Значительное внимание уделено способам противодействия вредоносным программам в экономических информационных системах, особенностям применения криптографических систем шифрования данных, а также разбору методов защиты информации в корпоративных вычислительных сетях и сети Интернет.

Учебное пособие предназначено для студентов экономических направлений подготовки очной и заочной форм обучения.

УДК 004.056:33(076.6)
ББК 32.973.26-018.2я73+65-98я73

©Д.В.Глотова, Н.С. Пальчикова,
2020
©ГО ВПО «Донецкий
национальный университет
экономики и торговли имени
Михаила Туган – Барановского»,
2020

Оглавление

Введение	6
СМЫСЛОВОЙ МОДУЛЬ 1.	7
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ	7
Тема 1. Введение в информационную безопасность. Модели информационной безопасности.	7
1.1. История становления информационной безопасности.	7
1.2. Этапы развития информационной безопасности.	9
1.3. Базовые понятия дисциплины.	11
1.4. Модели информационной безопасности.	18
Контрольные вопросы по теме 1.	21
Тема 2. Выявление возможных нарушений и атак в экономических информационных системах (ЭИС).	22
2.1. Анализ угроз информационной безопасности.	22
2.2. Классификация угроз информационной безопасности.	23
2.3. Модель нарушителя.	27
2.4. Уязвимости ЭИС.	31
2.5. Понятие и виды компьютерных преступлений.	34
Контрольные вопросы по теме 2.	42
Примеры тестовых заданий по смысловому модулю 1.	43
СМЫСЛОВОЙ МОДУЛЬ 2.	47
ИНСТРУМЕНТЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ	47
Тема 3. Противодействие вредоносным программам в ЭИС.	47
3.1. Основные понятия.	47
3.2. Классификация вредоносных программ.	49
3.2.1. Программные закладки.	49
3.2.2. Вирусы.	51
3.2.3. Черви.	55
3.2.4. Троянские программы.	58
3.2.5. Другие вредоносные программы.	63
3.2.6. Макровирусы.	68
3.3. Способы распространения вредоносных программ.	73
3.4. Последствия заражения вредоносной программой.	75
Вопросы для самоконтроля по теме 3.	79
Тема 4. Применение криптографических систем шифрования данных.	80
4.1. Понятия криптографии.	80
4.2. Понятия о симметричных и асимметричных криптосистемах.	82
4.3. Системы с открытым ключом.	83
4.4. Управление ключами.	86
4.5. Генерация ключей.	86
4.6. Накопление ключей.	87
4.7. Распределение ключей.	88
4.8. Понятие криптоанализа.	89
Контрольные вопросы по теме 4.	92
Тема 5. Методы защиты информации в корпоративных вычислительных сетях.	93
5.1. Идентификация и аутентификация.	93
5.2. Системы аутентификации электронных данных.	98
5.3. Способы атаки на пароль.	99

5.4. Использование токенов	104
5.5. Управление доступом	106
Контрольные вопросы по теме 5	107
Тема 6. Методы защиты информации в глобальной сети Интернет.	108
6.1. Средства защиты сети	108
6.2. Межсетевые экраны (firewall)	108
6.3. Межсетевые экраны прикладного уровня	109
6.4. Межсетевые экраны с пакетной фильтрацией	110
6.5. Гибридные межсетевые экраны	110
6.6. Организация и эксплуатация виртуальных частных сетей (VPN)	111
6.7. Определение виртуальных частных сетей VPN	112
6.8. Пользовательские VPN	114
6.9. Узловые VPN	115
6.10. Понятие стандартных технологий функционирования VPN	117
6.11. Общие понятия о функционировании IDS	119
6.12. Сетевые IDS	121
6.13. Узловые IDS	122
Контрольные вопросы по теме 6	124
Тестовые задания по смысловому модулю 2	125
СМЫСЛОВОЙ МОДУЛЬ 3.	129
ПРОВЕРКА СОСТОЯНИЯ БЕЗОПАСНОСТИ В ЭКОНОМИЧЕСКИХ	
ИНФОРМАЦИОННЫХ СИСТЕМАХ	129
Тема 7. Аудит информационной безопасности	129
7.1. Протоколирование и аудит	129
7.2. Активный аудит	132
7.3. Функциональные компоненты и архитектура активного аудита	134
Контрольные вопросы по теме 7	135
Тема 8. Анализ информационных рисков	136
8.1. Понятие информационного риска	136
8.2. Методики анализа, оценки и управления рисками информационной безопасности	137
8.3. Методы оценки рисков информационной безопасности	141
Контрольные вопросы по теме 8	144
Тестовые задания по смысловому модулю 3	145
Литература	148

Введение

Целью изучения дисциплины «Информационная безопасность» является формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты. Приобретенные знания позволят студентам правильно ориентироваться в категориях защищаемых информационных ценностей и приобрести минимально необходимый кругозор в проблемах информационной безопасности.

Дисциплина «Информационная безопасность» относится к вариативным учебным дисциплинам общенаучного цикла. Для успешного освоения дисциплины студент должен иметь навыки работы с персональным компьютером, знать простейшие способы форматирования текста, создания электронных таблиц, баз данных и основы алгоритмизации, приобретенные при изучении учебной дисциплины «Информатика» «Информационные технологии и системы в экономике».

В результате изучения учебной дисциплины студент должен

знать: базовый понятийный аппарат в области информационной безопасности; принципы и общие методы обеспечения информационной безопасности; критерии, условия и принципы отнесения информации к защищаемой; принципы и методы обработки конфиденциальных документов; методы и приемы защиты документированной информации от несанкционированного доступа;

уметь: практически выполнять технологические операции по защите и обработке конфиденциальных документов; разрабатывать политику предприятия в соответствии со стандартами безопасности; применить и настроить различные средства защиты информации; оценивать качество информационных ресурсов.

владеть: методами и формами защиты информации; технологией составления конфиденциальных документов; практическими навыками применения средств защиты информации при решении профессиональных задач, приёмами социальной адаптации информационных ресурсов и информационных технологий.