Федеральное государственное образовательное бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)

Новороссийский филиал Финуниверситета

Кафедра «Информатика, математика и общегуманитарные науки»

Д.В. Тимшина

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Рабочая программа дисциплины
для студентов, обучающихся по направлению
38.03.05 «Бизнес-информатика»
Профиль «ИТ-менеджмент в бизнесе»
заочная форма обучения

Рекомендовано Ученым советом Новороссийского филиала Финуниверситета протокол № 14 от «29» августа 2019 г.

Одобрено кафедрой «Информатика, математика и общегуманитарные науки» протокол № 01 от «27» августа 2019 г.

Новороссийск 2019

Д.В. Тимшина. Информационная безопасность компьютерных систем

Рабочая программа дисциплины предназначена для обучающихся по направлению 38.03.05 «Бизнес-информатика», профиль «ИТ-менеджмент в бизнесе» (заочная форма обучения) – Новороссийск: Новороссийский филиал Финуниверситета, кафедра «Информатика, математика и общегуманитарные науки», 2019. – 41 с.

Рабочая программа дисциплины содержит требования к результатам освоения дисциплины, содержание дисциплины, тематику семинарских занятий и технологии их проведения, формы самостоятельной работы, контрольные вопросы и систему оценивания, учебно-методическое и информационное обеспечение дисциплины.

СОДЕРЖАНИЕ

1. Наименование дисциплины

«Информационная безопасность компьютерных систем»

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Дисциплина «**Информационная безопасность компьютерных систем**» по направлению 38.03.05 «Бизнес-информатика» профиль «ИТ-менеджмент в бизнесе» обеспечивает формирование следующих компетенций: ПК-11, ПК-21 и ПКП-1

Код компетенции	Наименование компетенции	Индикатор достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПК-11	Умение защищать права на интеллектуальную собственность	-	**Знать:** - основные права на интеллектуальную собственность организаций; - основные законы и нормативные акты в области интеллектуальной собственности и безопасности информации. **Уметь:** - защищать права на интеллектуальную собственность организаций. **Владеть:** - методами и средствами защиты прав на интеллектуальную собственность организаций; - методами и средствами защиты информации.
ПК-21	Умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия	-	**Знать:** - основные законы, нормативные акты, международные и национальные стандарты в области информационной безопасности и защиты информации; - свойства и признаки информации, особенности информационно-аналитических и компьютерных систем; - основные информационные процессы, источники и каналы утечки информации на защищаемых объектах (компьютерных системах); - основы построения систем обработки, передачи и хранения информации, их современное состояние развития; - методы и средства защиты информации и управления информационной безопасностью ИТ-инфраструктуры предприятия.

			Уметь: - консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры организации; - оценивать информационные риски и строить эффективную систему управления информационной безопасностью ИТ-инфраструктуры предприятия; - анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результатов этого анализа; воспроизводить и корректно использовать основные понятия, связанные с обработкой, хранением, передачей и защитой информации в компьютерных системах. **Владеть:** - методами и средствами защиты информации в компьютерных системах; - навыками консультирования в области управления информационной безопасностью ИТ-инфраструктуры предприятия.
ПКП-1	Способность формировать цели, приоритеты и ограничения управления качеством ресурсов ИТ и изменение их по мере изменения внешних условий и внутренних бизнес-потребностей		**Знать:** - стандарты и методики оценки качества ресурсов ИТ, управления активами ИТ и конфигурациями ИТ; - способы определения потребностей в уровне качества ресурсов ИТ. **Уметь:** - формировать цели, приоритеты и ограничения управления качеством ресурсов ИТ; - контролировать качество ресурсов ИТ; - определять соответствие качества ресурсов ИТ потребностям; - формировать целевое качество ресурсов ИТ и контролировать его достижение; - организовать формирование и совершенствование системы показателей качества ресурсов ИТ, критериев их оценки; - контролировать и анализировать текущие значения показателей качества ресурсов ИТ; - планировать целевые значения показателей качества ресурсов ИТ с учетом потребностей; - организовать достижение целевых значений показателей качества ресурсов ИТ с учетом потребностей. **Владеть:** - методами контроля качества ресурсов ИТ; - методами анализа качества ресурсов ИТ, целей, приоритетов и ограничений управления качеством ресурсов ИТ.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность компьютерных систем» относится к дисциплине по выбору.

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Набор 2017 г., заочная форма обучения Таблица 1

Вид учебной работы по дисциплине	Всего (в з/ед. и часах)	Семестр (модуль) 5 (в часах)
Общая трудоемкость дисциплины	3 зач. ед. / 108 час	108 час
Контактная работа - Аудиторные занятия	12	12
Лекции	4	4
Семинары, практические занятия	8	8
Самостоятельная работа	96	96
Вид текущего контроля	контрольная работа	контрольная работа
Вид промежуточной аттестации	зачет	зачет

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Информационная безопасность в системе национальной безопасности

Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности.

Тема 2. Правовое и организационное обеспечение информационной безопасности

Государственная политика РФ в области правового обеспечения информационной безопасности. Особенности информации как объекта права. Законодательство РФ в сфере информационных технологий. Структура государственных органов РФ, осуществляющих правотворчество и правоприменение в области информационной безопасности. Государственная, служебная, коммерческая и банковская тайны.

Значение организационного обеспечения информационной безопасности. Характеристика организационных методов.

Стандарты и рекомендации в области защиты информации. Критерии защищенности компьютерных систем. Политика безопасности и гарантированность.

Тема 3. Основы управления информационными рисками

Понятие информационного риска. Основные направления управления информационными рисками. Информационные риски и безопасность информации. Анализ информационных рисков.

Особенности информации как объекта защиты в компьютерных системах. Защищенные информационные системы. Организация работы в защищенных системах.

Тема 4. Информационные уязвимости объектов

Антропогенные информационные уязвимости. Техногенные информационные уязвимости. Организационно-правовые и комбинированные информационные уязвимости.

Тема 5. Угрозы информационной безопасности и их источники

Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Случайные и преднамеренные угрозы.

Угрозы безопасности информации в распределенных системах.

Информационная война как высшая форма угрозы информационной безопасности.

Тема 6. Методы и средства обеспечения информационной безопасности компьютерных систем

Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам.

Криптографические методы защиты информации. Методы стеганографии.

Классификация методов шифрования. Методы симметричного шифрования. Блочное и потоковое шифрование. Абсолютно надежный шифр. Несимметричное шифрование.

Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности компьютерных систем.

Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.

Тема 7. Риски информационной безопасности и проблема построения комплексной системы защиты информации

Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения. Построение комплексной оптимальной системы защиты. Оценка рисков и организация управления процессом защиты информации.

Тема 8. Особенности защиты информации в распределенных компьютерных системах

Особенности защиты информации в распределенных компьютерных системах. Защита информации в каналах связи. Межсетевое экранирование. Подтверждение подлинности информации и взаимодействующих процессов.

Обеспечение информационной безопасности процессов функционирования систем электронной торговли и дистанционного банковского обслуживания клиентов.

Методы и средства обеспечения безопасной работы в глобальной сети Интернет.

Тема 9. Обработка и передача информации в компьютерных и управляющих системах и сетях связи, вопросы информационной безопасности и защиты информации для компьютерных и управляющих систем и сетей

Компьютерная информация; системное, прикладное и специальное программное обеспечение; понятие «открытой» системы; модель взаимодействия элементов «открытых» систем, компьютерная система. Виды защищаемой информации: семантическая и признаковая.

Основные понятия информационной защиты сети. Средства информационной защиты компьютерных сетей. Защита по протоколу Керберос.

Исторический аспект развития проблемы защиты информации. Развитие идей и концепций защиты информации.

Тема 10. Защита компьютерных систем от вирусов и вредоносных программ

Классификация вирусов и вредоносных программ. Источники проникновения вирусов и средства защиты от вирусов и вредоносных программ. Комплексный подход к задаче защите от вирусов и вредоносных программ. Основные правила защиты. Методы и средства защиты от вирусов и вредоносных программ.

5.2. Учебно-тематический план

Набор 2017 года, заочная форма обучения Таблица 2

№ п/п	Наименование тем (разделов) дисциплины	Трудоемкость в часах						Формы текущего контроля успеваемости
		Всего	Аудиторная работа				Самостоятельная работа	
			Общая	Лекции	Семинары, практические занятия	Занятия в интерактивных формах		
1	Информационная безопасность в системе национальной безопасности	10	1	1	0	0,5	9	Рефераты, доклады, беседы, дискуссии, презентации
2	Правовое и организационное обеспечение информационной безопасности	14	1	1	0	0,5	13	Рефераты, доклады, беседы, дискуссии, презентации
3	Основы управления информационными рисками	10	1	1	0	0,5	9	Рефераты, доклады, беседы, дискуссии, презентации
4	Информационные уязвимости объектов	10	1	1	0	0,5	9	Рефераты, доклады, беседы, дискуссии, презентации
5	Угрозы информационной безопасности и их источники	10	1	0	1	0,5	9	Рефераты, доклады, беседы, дискуссии, презентации
6	Методы и средства обеспечения информационной безопасности компьютерных систем	10	2	0	2	1	8	Рефераты, доклады, беседы, дискуссии, презентации
7	Риски информационной безопасности и проблема построения комплексной системы защиты информации	10	1	0	1	0,5	9	Рефераты, доклады, беседы, дискуссии, презентации

8	Особенности защиты информации в распределенных компьютерных системах	12	2	0	2	1	10	Рефераты, доклады, беседы, дискуссии, презентации
9	Обработка и передача информации в компьютерных и управляющих системах и сетях связи, вопросы информационной безопасности и защиты информации для компьютерных и управляющих систем и сетей	12	1	0	1	0,5	11	Рефераты, доклады, беседы, дискуссии, презентации
10	Защита компьютерных систем от вирусов и вредоносных программ	10	1	0	1	0,5	9	Рефераты, доклады, беседы, дискуссии, презентации
	В целом по дисциплине	108	12	4	8	6	96	Согласно учебному плану: контрольная работа
	Итого в %					50%		

5.3. Содержание семинаров, практических занятий

Таблица 3

Наименование тем (разделов) дисциплины	**Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)**	**Формы проведения занятий**
Тема 5. Угрозы информационной безопасности и их источники	1. Приведите определения эндогенных, экзогенных, антропогенных и техногенных угроз информационной безопасности. 2. Приведите классификацию техногенных угроз информационной безопасности. 3. Что такое угрозы конфиденциальности, целостности и доступности информации? 4. Раскройте понятие «Информационная война» и приведите примеры **Раздел 8:** [6 - 12]; **Раздел 9:** [2 -5].	Групповое обсуждение вопросов. Компьютерный практикум
Тема 6 Методы и средства обеспечения информационной безопасности компьютерных систем	Что такое стеганография? 2. Что такое криптография? 3. Что называется криптосистемой? 4. Что такое криптоанализ? 5. Приведите классификацию методов шифрования. 6. Перечислите требования, которым должны отвечать современные методы шифрования. 7. Приведите процедуру использования открытого ключа. 8. Приведите алгоритм зашифрования с помощью таблицы Виженера. 9. Приведите алгоритм расшифрования с помощью таблицы (матрицы) Виженера. 10. В чем заключается различие блочных и поточных шифров? 11. Что устанавливает электронная подпись? 12. Как создается электронная подпись? **Раздел 8:** [6 - 12]; **Раздел 9:** 2 -5].	

Тема 7 Риски информационной безопасности и проблема построения комплексной системы защиты информации	1. Раскройте алгоритм управления информационными рисками. 2. Определите понятие «система управления информационными рисками» и раскройте научные принципы ее построения. 3. Перечислите задачи, решаемые в процессе создания системы управления информационными рисками **Раздел 8:** [6, 8 - 10]; **Раздел 9:** [2 -5].	
Тема 8 Особенности защиты информации в распределенных компьютерных системах	1. Поясните принципы защиты речевой информации в каналах связи. 2. Перечислите и охарактеризуйте методы защиты от прослушивания акустических сигналов. 3. Охарактеризуйте средства борьбы с закладными подслушивающими устройствами **Раздел 8:** [6, 7, 10,11]; **Раздел 9:** [2 -5].	
Тема 9 Обработка и передача информации в компьютерных и управляющих системах и сетях связи, вопросы информационной безопасности и защиты информации для компьютерных и управляющих систем и сетей	1. В чем заключается сущность матричного (дискреционного) метода доступа? 2. Сравните матричный и мандатный методы доступа. 3. Перечислите основные способы неявного задания матрицы доступа и охарактеризуйте их. 4. Какие элементы содержит система разграничения доступом и как они взаимодействуют в процессе обслуживания запроса на доступ к объекту? 5. Приведите основные возможности ОС Windows по разграничению доступа. 6. Какими возможностями по разграничению доступа обладают приложения MS Office? 7. Назовите основные принципы разработки алгоритмов, программ и технических средств. 8. В чем заключается суть современных технологий программирования? 9. Дайте характеристику автоматизированной системы разработки программных средств. 10. Каким образом достигается защита от несанкционированного изменения структур КС на этапах разработки и эксплуатации? 11. Как осуществляется контроль целостности информации? 12. Как работает алгоритм защиты информации по протоколу Керберос? **Раздел 8:** [6, 8, 10 - 12]; **Раздел 9:** [2 -5].	

Тема 10 Защита компьютерных систем от вирусов и вредоносных программ	Перечислите этапы жизненного цикла компьютерного вируса. 2. Приведите классификацию компьютерных вирусов. 3. Дайте характеристику загрузочным вирусам. 4. Дайте характеристику вирусам-мутантам. 5. Дайте характеристику макрокомандным вирусам. 6. Дайте характеристику программе-вирусу. 7. Дайте характеристику вирусу «троянский конь». 8. Дайте характеристику вирусу «червь». 9. Дайте характеристику антивирусным программам. 10. Перечислите рекомендации по антивирусной защите. 11. Какие компоненты входят в межсетевые экраны? 12. Перечислите основные функции межсетевого экрана (firewall). 13. Перечислите симптомы заражения компьютера вирусом **Раздел 8:** [7 - 11]; **Раздел 9:** [2 -5].	

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 4

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Информационная безопасность в системе национальной безопасности	1. Изучение профессиональной терминологии в области информационной безопасности и информационного противоборства 2. Системные связи информационной безопасности с другими видами национальной безопасности	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену
Правовое и организационное обеспечение информационной безопасности	1. Общая характеристика организационных методов защиты информации в ИС. 2. Задачи государства в области безопасности информации.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену
Основы управления информационными рисками	1. Возможные стратегии управления информационными рисками 2. Принципы управления информационными рисками.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену
Информационные уязвимости объектов	1. Классификация информационных уязвимостей 2. Антропогенные и техногенные информационные уязвимости.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену
Угрозы информационной безопасности и их источники	1. Определение видов и форм информации, подверженной угрозам. 2. Возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену

Методы и средства обеспечения информационной безопасности компьютерных систем	1. Способы противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности. 2. Классификация методов шифрования.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену
Риски информационной безопасности и проблема построения комплексной системы защиты информации	1. Методика оценки информационных рисков. 2. Задачи решаемые в процессе создания системы управления информационными рисками.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену
Особенности защиты информации в распределенных компьютерных системах	1. Методы и средства защиты информации в распределенных компьютерных системах. 2. Принципы защиты речевой информации в каналах связи.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену
Обработка и передача информации в компьютерных и управляющих системах и сетях связи, вопросы информационной безопасности и защиты информации для компьютерных и управляющих систем и сетей	1. Каналы перехвата при передаче информации системами связи: электромагнитные, электрические, индукционные. 2. Матричный и мандатный методы доступа.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену
Защита компьютерных систем от вирусов и вредоносных программ	1. Классификация компьютерных вирусов. 2. Характеристика антивирусных программ. 3. Рекомендации по антивирусной защите.	Подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к экзамену

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерные задания контрольной работы.

Используя таблицу Виженера, решить задачи зашифрования исходного текста и расшифрования шифртекста. Исходные данные для решения задач приведены в таблице ниже.

Таблица 5

Номер задачи	Исходный текст	Ключ зашифро-вания	Шифртекст (криптограмма)	Ключ расшиф-рования
1	Система защиты информации	шифр	ЙБНСНЕЭЛЮНМЧЗ	шпион
2	Метод высокочастотного навязывания	ключ	ЧЮШЫТЫОЭМЛХХ	норма
3	Симметричные и асимметричные шифры	вирус	ДНЖАЪЗТЭФК	метр
4	Источник, фактор и причина риска	метод	ГИЫХВРКШЧ	лазер
5	Информационная безопасность	бит	ЛЭЗЩДЙУИ	луч
6	Информационный риск	знак	ЖЮХЧЮНАЪН	фон
7	Конфиденциальность информации	блок	ЙКЧПХТУСЙЗЧФЗ	звук
8	Внешние и внутренние угрозы	язык	ЪКТДГЩЩМВЕБДХ	цель
9	Каналы утечки звуковой информации	гост	ББТСЯИОУЬБТУС	сбой
10	Источник информационного риска	схема	ЮЙФЙИНГДАЕЕДХ	цепь
11	Уязвимость компьютерной системы	шаг	УЛЫЛЗОРО	люк
12	Система управления информационными рисками	буква	СЙЮДЮНГОБЕДКБ	сеть
13	Анализ информационных рисков	червь	ЬЪЦЫПИЖА	лицо
14	Методы традиционного шпионажа и диверсий	строка	РЖЬЕЭЕТФШЭКЦШТ	рука
15	Случайные и преднамеренные угрозы	число	ЗЮБТЛЫОЙГШИМ	глаз
16	Несанкционированная модификация программной структуры информационной системы	акростих	ЯРПШЧХАГЧК	план
17	Несанкционированный доступ к информации	пульт	ЭЯШЭИЫП	эхо
18	Стандарты управления системами информационной	алгоритм	НЮМЬУЮКФРШН	гриф

	безопасности			
19	Организационные методы защиты информации	скрытие	СРЕЖШХЕЮЪЕ	речь
20	Надежность и отказоустойчивость информационных систем	риск	БРХЩРУЪУРЮЪЛ	ритм
21	Помехоустойчивое кодирование информации	закон	ЭГТБЧЙЬЬОЯГШ	ухо
22	Методы биометрической идентификации человека	угроза	ВМЮЙЭГЩМБРРДЮКУ	свод
23	Абсолютно надежный шифр	код	ЫЧРПМРАПЮМ	урок
24	Дискреционный и мандатный методы доступа	сбор	ЭГРАТЩЯРЙКВЮХ	среда
25	Система разграничения доступа к информации	сигнал	ИЗЧХЖЦРХФЮМИКЭДГ	дверь

Примерные темы докладов/ рефератов

1. Основные понятия и составляющие информационной безопасности
2. Доктрина информационной безопасности Российской Федерации и ее основные положения
3. Классификация угроз информационной безопасности. Наиболее распространенные угрозы информационной безопасности
4. Классификация компьютерных вирусов и вредоносных программ
5. Источники проникновения вирусов и средства защиты от вирусов и вредоносных программ
6. Комплексный подход к задаче защиты от вирусов и вредоносных программ в компьютерной системе
7. Защита компьютерных систем от электромагнитных излучений и наводок. Активные и пассивные методы
8. Симметричные, асимметричные и гибридные криптоалгоритмы и их использование на современном этапе
9. Автоматизированные системы шифрования и области их применения
10. Основные понятия политики информационной безопасности предприятия
11. Основные понятия информационной защиты сетей
12. Средства информационной защиты сетей и защита по протоколу Керберос

13. Виды стандартов информационной безопасности

14. Стандарт «Оранжевая книга» (понятие «доверенная система»; определение «Уровня гарантированности»; политика безопасности и ее элементы)

15. Отличия алгоритмов DES и ГОСТ 28147-89

16. Уголовный кодекс Российской Федерации: преступления в сфере компьютерной информации

17. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации в ФЗ «Об информации, информационных технологиях и защите информации»

18. Методы и средства обеспечения безопасной работы в глобальной сети Интернет

19. Обеспечение информационной безопасности процессов функционирования систем электронной торговли

20. Обеспечение информационной безопасности процессов функционирования систем дистанционного банковского обслуживания

21. Защита информации в каналах связи

22. Применение методов криптографии для идентификации и аутентификации удаленных процессов

23. Межсетевое экранирование и его использование для защиты информации в распределенных компьютерных системах

24. Средства операционных систем и Microsoft Office по защите от несанкционированного доступа к документам

25. Методы контроля целостности информации. Защита от НСД к внутреннему монтажу, средствам коммутации, от подключения нештатных устройств

Контрольную работу выполнить и оформить согласно методическому указанию.

Пример титульного листа представлен в приложении.

ПРИЛОЖЕНИЕ

Образец титульного листа контрольной работы

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финуниверситет)

Новороссийский филиал Финуниверситета

Кафедра «Информатика, математика и общегуманитарные науки»

КОНТРОЛЬНАЯ РАБОТА

по дисциплине «Информационная безопасность компьютерных систем»

Выполнил: студент
Иванов А. Б.
Направление:
«Бизнес-информатика»
Группа: 1б-бби100
Номер зачетной книжки:
11флб00838
Курс: 1
Руководитель:
Тимшина Д.В.

Новороссийск 20_ _

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций представлен в разделе 2, который характеризует перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине.

Примерные тестовые задания

1. Основные угрозы доступности информации:

а) непреднамеренные ошибки пользователей

б) злонамеренное изменение данных

в) хакерская атака

г) отказ программного и аппаратного обеспечения

д) разрушение или повреждение помещений

е) перехват данных.

2. Суть компрометации информации:

а) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

б) несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

в) 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 (компьютерной) системы – это состояние автоматизированной системы, при котором она, ...

а) 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

б) 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

в) способна противостоять только информационным угрозам, как внешним так и внутренним

г) способна противостоять только внешним информационным угрозам.

4. Методы повышения достоверности входных данных:

а) замена процесса ввода значения процессом выбора значения из предлагаемого множества

б) отказ от использования данных

в) проведение комплекса регламентных работ

г) использование вместо ввода значения его считывание с машиночитаемого носителя

д) введение избыточности в документ первоисточник

е) многократный ввод данных и сличение введенных значений.

5. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ):

а) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

б) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

в) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом.

6. Сервисы безопасности:

а) идентификация и аутентификация

б) шифрование

в) инверсия паролей

г) контроль целостности

д) регулирование конфликтов

е) экранирование

ж) обеспечение безопасного восстановления

и) кэширование записей.

7. Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...

а) несанкционированного управления удаленным компьютером

б) внедрения агрессивного программного кода в рамках активных объектов Web-страниц

в) перехвата или подмены данных на путях транспортировки

г) поставки неприемлемого содержания.

8. Причины возникновения ошибки в данных:

а) погрешность измерений

б) ошибка при записи результатов измерений в промежуточный документ

в) неверная интерпретация данных

г) ошибки при переносе данных с промежуточного документа в компьютер

д) использование недопустимых методов анализа данных

е) неустранимые причины природного характера

ж) преднамеренное искажение данных

и) ошибки при идентификации объекта или субъекта хозяйственной деятельности.

9. К формам защиты информации не относится...

а) аналитическая

б) правовая

в) организационно-техническая

г) страховая.

10. Наиболее эффективное средство для защиты от сетевых атак:

а) использование сетевых экранов или «firewall»

б) использование антивирусных программ

в) посещение только «надёжных» Интернет-узлов

г) использование только сертифицированных программ-браузеров при доступе к сети Интернет.

11. Информация, составляющая государственную тайну, не может иметь гриф...

а) «для служебного пользования»

б) «секретно»

в) «совершенно секретно»

г) «особой важности».

12. Разделы современной криптографии:

а) Симметричные криптосистемы

б) Криптосистемы с открытым ключом

в) Криптосистемы с дублированием защиты

г) Системы электронной подписи

д) Управление паролями

е) Управление передачей данных

ж) Управление ключами.

13. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности:

а) рекомендации X.800

б) Оранжевая книга

в) Закон «Об информации, информационных технологиях и о защите информации».

14. Утечка информации – это ...

а) несанкционированный процесс переноса информации от источника к злоумышленнику

б) процесс раскрытия секретной информации

в) процесс уничтожения информации

г) непреднамеренная утрата носителя информации.

15. Основные угрозы конфиденциальности информации:

а) маскарад

б) карнавал

в) переадресовка

г) перехват данных

д) блокирование

е) злоупотребления полномочиями.

16. Элементы знака охраны авторского права:

а) буквы С в окружности или круглых скобках

б) буквы Р в окружности или круглых скобках

в) наименования (имени) правообладателя

г) наименование охраняемого объекта

д) года первого выпуска программы.

17. Защита информации обеспечивается применением антивирусных средств

а) да

б) нет

в) не всегда.

18. Средства защиты объектов файловой системы основаны на…

а) определении прав пользователя на операции с файлами и каталогами

б) 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

а) активная

б) пассивная.

20. Преднамеренная угроза безопасности информации:

а) кража

б) наводнение

в) повреждение кабеля, по которому идет передача, в связи с погодными условиями

г) ошибка разработчика.

21. Концепция системы защиты от информационного оружия не должна включать…

а) средства нанесения контратаки с помощью информационного оружия

б) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры

в) признаки, сигнализирующие о возможном нападении

г) 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 ...

а) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

б) реализацию права на доступ к информации

в) соблюдение норм международного права в сфере информационной безопасности

г) выявление нарушителей и привлечение их к ответственности

д) соблюдение конфиденциальности информации ограниченного доступа

е) разработку методов и усовершенствование средств информационной безопасности.

23. Компьютерные вирусы - это:

а) вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера

б) программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК

в) программы, являющиеся следствием ошибок в операционной системе

г) вирусы, сходные по природе с биологическими вирусами.

24. Что не относится к объектам информационной безопасности РФ?

а) природные и энергетические ресурсы

б) информационные системы различного класса и назначения, информационные технологии

в) система формирования общественного сознания

г) права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности.

25. Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?

а) неправомерный доступ к компьютерной информации

б) создание, использование и распространение вредоносных программ для ЭВМ

в) умышленное нарушение правил эксплуатации ЭВМ и их сетей

г) все перечисленное выше.

26. Политика безопасности:

а) фиксирует правила разграничения доступа

б) отражает подход организации к защите своих информационных активов

в) описывает способы защиты руководства организации.

27. При анализе стоимости защитных мер следует учитывать:

а) расходы на закупку оборудования

б) расходы на закупку программ

в) расходы на обучение персонала.

28. Протоколирование и аудит могут использоваться для:

а) предупреждения нарушений ИБ

б) обнаружения нарушений

в) восстановления режима ИБ

29. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

а) выработка и проведение в жизнь единой политики безопасности

б) унификация аппаратно-программных платформ

в) минимизация числа используемых приложений.

30.Экранирование может использоваться для:

а) предупреждения нарушений ИБ

б) обнаружения нарушений

в) локализации последствий нарушений.

31. В число основных принципов архитектурной безопасности входят:

а) следование признанным стандартам

б) применение нестандартных решений, не известных злоумышленникам

в) разнообразие защитных средств.

32. В число основных принципов архитектурной безопасности входят:

а) усиление самого слабого звена

б) укрепление наиболее вероятного объекта атаки

в) эшелонированность обороны.

33. Риск является функцией:

а) размера возможного ущерба

б) числа пользователей ИС

в) уставного капитала организации.

34. Первый шаг в анализе угроз – это:

а) идентификация угроз

б) аутентификация угроз

в) ликвидация угроз.

35. Управление рисками включает в себя следующие виды деятельности:

а) определение ответственных за анализ рисков

б) оценка рисков

в) выбор эффективных защитных средств.

36. Цифровой сертификат содержит:

а) открытый ключ пользователя

б) секретный ключ пользователя

в) имя пользователя.

37. Криптография необходима для реализации следующих сервисов безопасности:

а) контроль конфиденциальности

б) контроль целостности

в) контроль доступа.

38. Экран выполняет функции:

а) разграничения доступа

б) облегчения доступа

в) усложнения доступа.

39. Демилитаризованная зона располагается:

а) перед внешним межсетевым экраном

б) между межсетевыми экранами

в) за внутренним межсетевым экраном.

40. Криптография необходима для реализации следующих сервисов безопасности:

а) идентификация

б) экранирование

в) аутентификация.

41. Экранирование на сетевом и транспортном уровнях может обеспечить:

а) разграничение доступа по сетевым адресам

б) выборочное выполнение команд прикладного уровня

в) контроль объема данных, переданных по TCP-соединению.

42. Туннелирование может использоваться на следующем уровне модели OSI:

а) сетевом

б) сеансовом

в) уровне представления.

43. Принцип усиления самого слабого звена можно переформулировать как:

а) принцип равнопрочности обороны

б) принцип удаления слабого звена

в) принцип выявления главного звена, ухватившись за которое можно вытянуть всю цепь.

44. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:

а) просчеты при администрировании ИС

б) необходимость постоянной модификации ИС

в) сложность современных ИС

45. Для внедрения бомб чаще всего используются ошибки типа:

а) отсутствие проверок кодов возврата

б) переполнение буфера

в) нарушение целостности транзакций.

Перечень контрольных вопросов к зачету

1. Сущность информационных рисков. Определение (понятие «информационный риск»).
2. Прямые и косвенные информационные риски. Причина, фактор и источник риска. Основные направления управления информационными рисками.
3. Анализ информационных рисков.
4. Построение системы управления информационными рисками (СУИР). Принципы построения СУИР.
5. Информация как объект защиты. Свойства информации как объекта защиты.
6. Программа и стратегии управления информационными рисками предприятия.
7. Схема управления информационными рисками с учетом выбора стратегии управления информационными рисками.
8. Понятие «угрозы безопасности информации». Классификация угроз безопасности информации.
9. Внешние и внутренние угрозы безопасности информации. Случайные и преднамеренные угрозы. Приведите примеры.
10. Методы традиционного шпионажа и диверсий. Приведите примеры.
11. Современные средства прослушивания и принципы их действия. Приведите примеры.
12. Современные средства визуального наблюдения (видеоразведка). Приведите примеры.

13. Понятие «несанкционированный доступ к информации» (НСДИ). Система разграничения доступа к информации. Каналы НСДИ.
14. Несанкционированная модификация технической и программной структуры компьютерной информационной системы (КС). Недекларированные возможности КС. Аппаратные и программные закладки.
15. Угрозы безопасности информации в распределенных системах.
16. Классификация злоумышленников. Технологические возможности злоумышленников по преодолению систем защиты информации.
17. Характеристика физических каналов негативного воздействия на ИР. Последствия воздействия.
18. Правовое регулирование в области безопасности информации. Задачи государства в данной области.
19. Основные положения Доктрины информационной безопасности Российской Федерации.
20. Характеристика основных законов РФ, регулирующих отношения в области ИТ.
21. Стандарты как механизм управления информационными рисками. Виды стандартов. Приведите примеры.
22. Организационная структура системы обеспечения информационной безопасности Российской Федерации. Государственные органы, обеспечивающие безопасность ИТ и решаемые ими задачи.
23. Организационные методы обеспечения информационной безопасности предприятия и их характеристика. Приведите примеры.
24. Направления защиты от случайных угроз и их характеристика.
25. Приведите характеристику дублирования информации в КС. Методы дублирования информации (оперативные и неоперативные; сосредоточенное и рассредоточенное и др.) их возможности и недостатки.
26. Понятие репликации и резервного копирования, их отличия. Технология RAID.
27. Пути повышения надежности и отказоустойчивости КС. Основные подходы к созданию отказоустойчивых систем.
28. Защита от ошибок: блокировка ошибочных операций и направления оптимизации взаимодействия пользователя с КС.

29. Противодействие техногенным авариям и стихийным бедствиям. Минимизация ущерба от аварий и стихийных бедствий.
30. Система охраны информационных объектов, ее состав и характеристика компонентов системы.
31. Характеристика технических возможностей современных инженерных конструкций, систем сигнализации, средств наблюдения, подсистем доступа на объекты.
32. Структура типовой системы охранной сигнализации и ее структура. Принцип действия элементов охранной сигнализации.
33. Структурная схема телевизионной системы видеоконтроля. Устройства обработки и коммутации видеоинформации.
34. Понятия «идентификация» и «аутентификация». Средства и методы идентификации и аутентификации субъектов доступа.
35. Организация работы с документацией на предприятиях.
36. Механизмы противодействия ведению видеоразведки, прослушиванию в помещениях и при использовании коммуникационного оборудования.
37. Характеристика методов защиты от прослушивания акустических сигналов.
38. Средства борьбы с закладными подслушивающими устройствами и их характеристики.
39. Методы борьбы с инсайдерами.
40. Модели доступа. Защита информации в компьютерных системах от несанкционированного доступа (НСД).
41. Система разграничения доступа к информации и ее структура.
42. Приведите сравнительную характеристику матричного и мандатного методов доступа.
43. Перечислите основные способы неявного задания матрицы доступа и охарактеризуйте их.
44. Средства ОС и MS Office по защите от несанкционированного доступа к документам.
45. Разграничение доступа к информации в базах данных.
46. Методы и средства защиты от несанкционированного изменения структур компьютерных систем. Приведите примеры.
47. Приведите основные возможности OS Windows по разграничению доступа.

48. Приведите основные возможности по разграничению доступа в приложениях MS Office.
49. Методы скрытия информации. Методы стеганографии.
50. Основные понятия криптографии.
51. Классификация методов шифрования. Требования к современным шифрам.
52. Методы симметричного шифрования. Блочное и потоковое шифрование.
53. Несимметричное шифрование. Абсолютно надежный шифр.
54. Особенности защиты информации в распределенных КС.
55. Основные понятия информационной защиты сети. Средства защиты сетей. Протокол Керберос. Защита по протоколу Керберос.
56. Защита информации в каналах связи. Приведите примеры.
57. Межсетевое экранирование. Принцип действия схем защиты с помощью брандмауэров (межсетевые экраны).
58. Системы дистанционного банковского обслуживания, принципы и схема их функционирования. Обеспечение информационной безопасности процессов функционирования систем дистанционного банковского обслуживания.
59. Системы электронной торговли, принципы и схема их функционирования. Обеспечение информационной безопасности процессов функционирования систем электронной торговли.
60. Методы и средства обеспечения безопасной работы в сети Интернет.
61. Классификация компьютерных вирусов и вредоносных программ. Приведите примеры.
62. Методы и средства борьбы с компьютерными вирусами и вредоносными программами.
63. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения.

Примеры оценочных средств для проверки каждой компетенции, формируемой дисциплиной

Компетенция	Типовые задания

ПК-11 Умение защищать права на интеллектуальную собственность	**Защищает права на интеллектуальную собственность:** **Задание 1. Элементы знака охраны авторского права:** а) буквы С в окружности или круглых скобках б) буквы Р в окружности или круглых скобках в) наименования (имени) правообладателя г) наименование охраняемого объекта д) года первого выпуска программы. **Задание 2. Что не относится к объектам информационной безопасности РФ?** а) природные и энергетические ресурсы б) информационные системы различного класса и назначения, информационные технологии в) система формирования общественного сознания г) права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности.
ПК-21 Умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия	**Консультирует заказчиков по вопросам совершенствования управления ИБ ИТ-инфраструктуры:** **Задание 1. Информационная безопасность автоматизированной (компьютерной) системы – это состояние автоматизированной системы, при котором она,** а) 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 б) 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 в) способна противостоять только информационным угрозам, как внешним, так и внутренним г) способна противостоять только внешним информационным угрозам. **Задание 2. Методы повышения достоверности входных данных:** а) замена процесса ввода значения процессом выбора значения из предлагаемого множества б) отказ от использования данных в) проведение комплекса регламентных работ г) использование вместо ввода значения его считывание с машиночитаемого носителя д) введение избыточности в документ первоисточник е) многократный ввод данных и сличение введенных значений **Задание 3. При анализе стоимости защитных мер следует учитывать:** а) расходы на закупку оборудования б) расходы на закупку программ в) расходы на обучение персонала.

ПКП-1 Способность формировать цели, приоритеты и ограничения управления качеством ресурсов ИТ и изменение их по мере изменения внешних условий и внутренних бизнес-потребностей	**Формирует цели, приоритеты и ограничения управления качеством ресурсов ИТ и изменяет их по мере изменения внешних условий и внутренних бизнес-потребностей:** **Задание 1. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:** а) выработка и проведение в жизнь единой политики безопасности б) унификация аппаратно-программных платформ в) минимизация числа используемых приложений. **Задание 2. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:** а) просчеты при администрировании ИС б) необходимость постоянной модификации ИС в) сложность современных ИС

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Нормативно-правовые акты

1. Государственная программа Российской Федерации «Информационное общество (2011-2020 годы)» (в ред. Постановления Правительства РФ от 18.05.2011 N 399).
2. Программа «Цифровая экономика Российской Федерации», утверждена распоряжением Правительства от 28 июля 2017 № 1632-р.
3. Стратегия развития информационного общества в Российской Федерации, на 2017 – 2030 годы. Указ Президента РФ от 9 мая 2017 г. № 203.
4. Указ Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».
5. Федеральный закон «Об организации предоставления государственных и муниципальных услуг». N 210-ФЗ от 27 июля 2010 года.
6. Федеральный Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 13.07.2015 г.

Основная литература

7. Экономическая информатика : учебное пособие / Чистов Д.В. под ред. и др. — Москва : КноРус, 2017. — 512 с. — (для бакалавров). https://www.book.ru/book/919995

8. Гобарева Я.Л., Городецкая О.Ю., Золотарюк А.В. Бизнес-аналитика средствами Excel: Учебное пособие / Я.Л. Гобарева, О.Ю. Городецкая, А.В. Золотарюк. – 3-е изд., перераб. и доп. – М.: Вузовский учебник: ИНФРА-М, 2018. – 350 с. ЭБС ZNANIUM, URL: https://znanium.com/read?id=301962

Дополнительная литература

9. Информационные ресурсы и технологии в экономике: Учеб. пособие/ под ред. Б.Е. Одинцова, А.Н. Романова. – М.: Вузовский учебник: ИНФРАМ-М, 2019. [Режим доступа]: ЭБС: ZNANIUM, URL: https://znanium.com/read?id=355933
10. Информационные технологии в менеджменте (управлении): учебник и практикум для академического бакалавриата / Ю.Д. Романова [и др.]; / под ред. Ю.Д. Романовой. – 2-е изд., перераб. и дол. – М.: Изд-во Юрайт, 2019. – 411 с. ЭБС изд-ва Юрайт, https://ez.el.fa.ru:2428/book/informacionnye-tehnologii-v-menedzhmente-upravlenii-446052
11. Скорочкина Т.С. Информационные технологии визуализации бизнесинформации = Information technology of visualization of business information [Электронный ресурс]: учебное пособие / Т.С. Скорочкина. – М.: Финуниверситет, 2017. – 74 с. – Режим доступа: http://elib.fa.ru/fbook/scorochkina_1786.pdf/view

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. https://programs.gov.ru/Portal – Портал государственных программ Российской Федерации
2. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/ (http://library.fa.ru/files/elibfa.pdf)
3. Электронно-библиотечная система Znanium http://www.znanium.com (https://znanium.com/)
4. Электронно-библиотечная система BOOK.RU - https://www.book.ru/
5. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/ (https://urait.ru/)
6. Научная электронная библиотека eLibrary.ru – http://elibrary.ru
7. Официальный сайт ЗАО «Консультант Плюс». – www.consultant.ru/
8. Официальный сайт ООО «НПП Гарант-Сервис» – www.garant.ru/
9. Официальный сайт Microsoft – https://www.microsoft.com/ru-ru

10.Методические указания для обучающихся по освоению дисциплины

Для более полного и углубленного усвоения материала по дисциплине учебным планом предусмотрена самостоятельная работа студентов. Самостоятельная работа студентов организуется на основе целей и задач программы дисциплины, является основным методом обучения и неотъемлемым элементом изучения дисциплины.

Целями самостоятельной работы студентов являются:

- формирование навыков самостоятельной образовательной деятельности;
- выявления и устранения студентами пробелов в знаниях, необходимых для изучения данной дисциплины;
- осознания роли и места изучаемой дисциплины в образовательной программе, по которой обучаются студенты.

Самостоятельная работа студентов подразделяется на обязательную и контролируемую. Обязательная самостоятельная работа обеспечивают подготовку студента к текущим аудиторным занятиям. Результаты этой подготовки проявляются в активности студента на занятиях и качественном уровне сделанных докладов, презентаций, выполненных практических, контрольных и тестовых заданий и др. форм текущего контроля. Контролируемая самостоятельная работа направлена на углубление и закрепление знаний студента, развитие аналитических навыков по проблематике учебной дисциплины. Подведение итогов и оценка результатов таких форм самостоятельной работы осуществляется во время контактных часов с преподавателем. Самостоятельная работа студентов предполагает изучение теоретического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, учебно-методических материалов, законодательства РФ и т.д.

В процессе самостоятельной работы студенты:

- осваивают материал, предложенный им на лекциях с привлечением указанной преподавателем литературы;
- осуществляют работу с основной и дополнительной литературой, дополнительными материалами из зарубежных и российских литературных источников;
- готовятся к семинарским занятиям в соответствии с методическими указаниями к ним;
- выполняют практические задания, контрольные домашние работы с использованием соответствующих методических указаний;
- самостоятельно осваивают указанные преподавателем теоретические разделы изучаемой дисциплины;
- ведут подготовку к зачету/ экзамену.

Учитывая подготовленность того или иного студента, преподаватель может

поставить перед ним задачу по более углубленному изучению проблемы, подготовке реферата и сообщения результатов на занятиях.

Основная цель самостоятельной работы студента (СРС) при изучении дисциплины «Информационная безопасность компьютерных систем» состоит в формировании у студентов системы теоретических знаний и практических навыков в области выполнения функций планирования, организации и принятия управленческих решений в социально-экономических системах; закреплении теоретических знаний, полученных в ходе лекционных занятий и формировании практических навыков, связанных с эффективным использованием современных информационных технологий для решения прикладных задач как в процессе обучения в вузе и при выполнении выпускной квалификационной работы, так и в будущей профессиональной деятельности для решения функциональных задач.

Глубокое и прочное усвоение дисциплины предполагает активную деятельность студентов как во время аудиторных занятий, так и при самостоятельной работе. В результате освоения дисциплины у студентов должны быть сформированы указанные в рабочей программе дисциплины компетенции, выработана способность к анализу, самообразованию, саморазвитию.

Самостоятельная работа студента в процессе освоения дисциплины «Информационная безопасность компьютерных систем» включает:

- изучение основной и дополнительной литературы по курсу и других источников: периодической печати, Интернет-ресурсов; учебных материалов электронных библиотечных систем, информационно-образовательного портала, нормативно-правовых актов и т.п.;
- выполнение контрольной работы;
- выполнение индивидуального задания;
- индивидуальные и групповые консультации по наиболее сложным вопросам дисциплины;
- подготовку к зачету.

На самостоятельную работу студентов отводится 96 часа учебного времени.

При подготовке к занятиям студент должен просмотреть конспекты лекций, рекомендованную литературу по данной теме; подготовиться к ответу на контрольные вопросы. Успешное изучение дисциплины требует от студентов посещения лекций, активной работы на семинарах, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой, интернет-источниками.

Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. Культура записи лекции – один из важнейших факторов успешного и творческого овладения знаниями. Последующая работа над текстом лекции

воскрешает в памяти содержание лекции, позволяет развивать аналитическое мышление. Лекции имеют обзорный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов, а также призваны способствовать формированию навыков самостоятельной работы с научной литературой. Работа с конспектом лекций предполагает просмотр конспекта в тот же день после занятий, пометку материала конспекта, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь за помощью к преподавателю на консультации, ближайшей лекции или семинаре. Регулярно отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам. Для выполнения контрольной работы студентам необходимо внимательно прочитать соответствующие разделы лекций, учебной и научной литературы и проработать задания, аналогичные тем, что приведены в контрольной работе.

Работу с основной и дополнительной литературой целесообразно начинать с освоения материала учебников, которые содержат необходимый материал по каждой теме.

Подготовка к семинарскому занятию зависит от темы занятия и вопросов, предложенных преподавателем, для подготовки к семинару.

Выполнение и оформление контрольной работы проводится в соответствии с методическими указаниями по выполнению контрольной работы. Контрольная работа сдается преподавателю для проверки в установленные преподавателем сроки.

На экзамене проверяются итоговые знания студента, а также учитывается результативность всех видов СРС.

Выполнение и оформление контрольной работы проводится в соответствии с методическими указаниями по выполнению контрольной работы. Контрольная работа сдается преподавателю для проверки в установленные преподавателем сроки.

Контрольная работа оформляется на ПК с использованием текстового процессора Microsoft Word на листах формата А4, ориентация – книжная.

Следует установить следующие размеры полей страницы: левое поле – 3 см, правое, верхнее и нижнее – 2 см.

Требования к оформлению текста контрольной работы:

– отступ первой строки (абзацный отступ) – 1,25 см;

– междустрочный интервал – 1,5 строки;

– гарнитура шрифта – Times New Roman;

– кегль шрифта (размер) – 14 пунктов;

– форматирование текста (выравнивание) – по ширине.

Каждую структурную часть контрольной работы нужно начинать с нового листа. Точка в конце заголовка структурной части работы не ставится.

Каждая цитата, заимствованные цифры, факты должны сопровождаться ссылкой на источник, описание которого приводится в списке использованной литературы. В ссылке указывается номер источника по списку и номера страниц, например: [5, С. 49-50].

Все аббревиатуры и сокращения слов должны быть расшифрованы в тексте работы при первом употреблении.

Рисунки необходимо снабжать подрисуночной подписью.

В конце подрисуночной подписи точку не ставят.

Все схемы и рисунки имеют одинарную сквозную нумерацию. Нельзя располагать подрисуночную подпись и рисунок на разных страницах. На все рисунки необходимо сделать ссылки в тексте контрольной работы.

Табличный материал (таблица) оформляется следующим образом. В левом верхнем углу пишут слово «Таблица» и ее порядковый номер в работе. Таблица должна иметь тематический заголовок, который располагают по центру без точки в конце.

Допускается использование в таблице кегля шрифта (размера) – 12 пунктов.

На последней странице контрольной работы студент обязан поставить дату сдачи контрольной работы на регистрацию и свою подпись.

Контрольная работа должна быть сброшюрована по левому краю.

Объем контрольной работы не более 15 страниц, включая титульный лист и список литературы. Приложения, если они есть, в общем объеме контрольной работы не учитываются.

Постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы дисциплины – залог успешной работы и положительной оценки.

Для оценки знаний студента используется балльно-рейтинговая оценка. Балльно-рейтинговая система представляет собой систему количественной оценки качества освоения образовательной программы высшего профессионального образования в сравнении с другими студентами. Принципы балльно-рейтинговой системы оценки успеваемости студентов:

- единство требований, предъявляемых к работе студентов;
- регулярность и объективность оценки результатов работы студентов;
- открытость и гласность результатов успеваемости студентов для всех участников образовательного процесса.

Балльная оценка текущего контроля успеваемости студента составляет максимум 40 баллов. Балльная оценка в зачетно-экзаменационную сессию составляет максимум 60 баллов.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

При осуществлении образовательного процесса обучающимися и профессорско-преподавательским составом используются: программное обеспечение, информационно-справочные системы, электронные библиотечные системы.

11.1. Комплект лицензионного программного обеспечения:

1. Антивирусная защита ESET NOD32
2. Windows, Microsoft Office

11.2 Современные профессиональные базы данных и информационные справочные системы:

- Информационно-правовая система «Консультант Плюс»
- Аналитическая система Bloomberg Professional.
- базы данных Росстата: ЦБСД, ЕМИСС, ССРД МВФ
- Электронная энциклопедия: http://ru.wikipedia.org/wiki/Wiki
- Система комплексного раскрытия информации «СКРИН» http://www.skrin.ru/

11.3 Сертифицированные программные и аппаратные средства защиты информации

Сертифицированные программные и аппаратные средства защиты информации не предусмотрены.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для осуществления образовательного процесса в рамках дисциплины необходимо наличие специальных помещений.

Специальные помещения представляют собой учебные аудитории для проведения лекций, семинарских и практических занятий, выполнения курсовых групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и

помещения для хранения и профилактического обслуживания учебного оборудования.

Проведение лекций и семинаров в рамках дисциплины осуществляется в помещениях:

– оснащенных демонстрационным оборудованием;

– оснащенных компьютерной техникой с возможностью подключения к сети «Интернет»;

– обеспечивающих доступ в электронную информационно-образовательную среду университета.

Специальные помещения должны быть укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.