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

Новороссийский филиал Финуниверситета

Кафедра «Информатика, математика и общегуманитарные науки»

УТВЕРЖДАЮ
Директор филиала
_____ Е.Н. Сейфиева
«29» 08 2019 г.

Д.В. Тимшина

Информационная безопасность в экономических системах

Рабочая программа дисциплины
для студентов, обучающихся по направлению
38.03.01 «Экономика»
Профиль «Анализ и управление рисками организации»
очная 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 в экономических системах. Рабочая программа дисциплины предназначена для студентов, обучающихся по направлению подготовки бакалавров 38.03.01 «Экономика», профиль «Анализ и управление рисками организации» (очная форма обучения) – Новороссийск: Новороссийский филиал Финуниверситета, кафедра «Информатика, математика и общегуманитарные науки», 2018. – 46с.

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 рабочей программы дисциплины

1. Наименование дисциплины

«Информационная безопасность в экономических системах»

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

Цель дисциплины – формирование у студентов знаний и навыков по проблеме обеспечения защиты информационных ресурсов в экономических системах хозяйствующих субъектов, по оценке и управлению информационными рисками; создание представления об основах информационной безопасности в экономических системах, принципах и методах противодействия несанкционированному информационному воздействию; развитие способностей к логическому и алгоритмическому мышлению.

Задачи дисциплины:

– изучить место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

– основные нормативные правовые акты в области информационной безопасности и защиты информации; технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации в экономических системах;

– сформировать умения проведения анализа и оценки угроз информационной безопасности объекта;

– обучить работе с современными технологиями обеспечения информационной безопасности;

– сформировать системные представления об управлении информационными рисками;

– изучить методы и средства комплексной защиты информации (информационных ресурсов) в экономических системах организаций.

Дисциплина «Информационная безопасность в экономических системах» по направлению 38.03.01 «Экономика» профиль «Анализ и управление рисками организации» обеспечивает формирование следующей компетенции:

Код компетенции	Наименование компетенции	Индикатор достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПКП-3	Способность поддержания устойчивого функционирования системы управления рисками	1. Соблюдает и поддерживает нормы профессиональной этики, нормы корпоративного управления и корпоративной культуры по рискам.	**Знать:** - знать типы рисков и мероприятий по воздействию на риск; - знать нормы профессиональной этики и корпоративной культуры в области информационной безопасности и информационных рисков; - основные законы, нормативные акты, стандарты в области информационной безопасности и защиты информации; - методы и средства защиты информации в экономических системах; - современные подходы к управлению информационными рисками. **Уметь:** - проводить мероприятия по воздействию на риск; - использовать нормы профессиональной этики и корпоративной культуры в области информационной безопасности и информационных рисков; - использовать основные законы, нормативные акты, стандарты в области информационной безопасности и защиты информации; - применять методы и средства защиты информации в экономических системах; - применять современные подходы к управлению информационными рисками.

		2. Устанавливает и поддерживает деловые контакты, связи, отношения, коммуникации с сотрудниками компании, проводит интервью с ответственными за риск работниками	**Знать:** - основные информационные процессы, источники и каналы утечки информации на защищаемых объектах в экономических системах для поддержки деловых коммуникаций; **Уметь:** - контролировать информационные процессы, источники и каналы утечки информации, используемые в деловых коммуникациях, для снижения информационных рисков.
		3. Оказывает помощь сотрудникам в выявлении и оценке новых рисков, представляет аналитическую информацию о рисках для руководителей и ответственных за мероприятия по рискам работников.	**Знать:** - классификацию угроз информационной безопасности в экономических системах; - основные методы и средства обеспечения информационной безопасности хозяйствующих субъектов, защищенных систем и технологий. **Уметь:** классифицировать угрозы в области информационной безопасности, выявлять и анализировать новые информационные риски с целью создания эффективной СУИР.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность в экономических системах» является дисциплиной по выбору, изучаемой в 7-м семестре, профильного блока дисциплин по выбору для направления подготовки 38.03.01 «Экономика» профиля «Анализ и управление рисками организации» очной формы обучения.

Полученные знания и умения, приобретенные студентами, должны быть использованы в процессе изучения других дисциплин, при подготовке курсовых работ, выполнении научно-исследовательской работы студентов (НИРС), написании выпускной квалификационной работы, а также востребованы в процессе обучения в магистратуре.

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

Набор 2018 г. и набор 2019 г., очная форма обучения

Таблица 1

Вид учебной работы по дисциплине	**Всего (в з/е и часах)**	**Семестр (модуль) 7 (в часах)**
Общая трудоемкость дисциплины	3 зач. ед. 108 час.	7 семестр 108 час.
Контактная работа – Аудиторные занятия	34	34
Лекции	16	16
Семинары, практические занятия	18	18
Самостоятельная работа	74	74
Вид текущего контроля	эссе	эссе
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. Понятийный аппарат дисциплины. Основы управления информационными рисками

Понятийный аппарат и основы терминологии информационной безопасности. Понятия «информационная безопасность», «информационный риск», «защита информации».

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

Особенности информации как объекта защиты в экономических информационных системах. Защищенные экономические информационные системы. Организация работы в защищенных системах.

Тема 2. Угрозы информационной безопасности в экономических системах, их источники и характеристика

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

Характеристика физических каналов негативного воздействия на информационные ресурсы экономических систем.

Угрозы безопасности информации в распределенных системах.

Информационная война как высшая форма угрозы информационной безопасности.

Тема 3. Правовое и организационное обеспечение информационной безопасности в экономических системах

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 информационной безопасности.

Стандарты и рекомендации в области защиты информации. Критерии защищенности экономических систем. Политика безопасности в экономических системах.

Тема 4. Методы и средства обеспечения информационной безопасности

Концепция построения комплексной системы обеспечения информационной безопасности и защиты информации. Основные показатели защищенности экономических систем.

Дублирование информации в экономических системах, повышение отказоустойчивости и надежности их функционирования. Блокировка ошибочных операций и оптимизация взаимодействия пользователей с компьютерными системами.

Минимизация ущерба от случайных угроз (аварии, стихийные бедствия).

Тема 5. Средства защиты и механизмы противодействия утечки информации по техническим каналам

Система охраны информационных объектов. Инженерные конструкции, средства видеонаблюдения и системы сигнализации, их назначение, технические возможности и характеристики. Подсистемы доступа на объекты. Методы и средства идентификации и аутентификации субъектов доступа.

Организация работы с документацией.

Механизмы противодействия ведению видеоразведки, прослушиванию в помещениях и применении коммуникационного оборудования. Защита компьютерных систем от наводок и электромагнитных излучений. Активные и пассивные методы. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.

Методы борьбы с инсайдерами.

Тема 6. Защита информации от несанкционированного доступа и изменения структур в экономических системах

Понятие «несанкционированный доступ» (НСД) к информации. Защита информации от НСД в экономических системах. Система разграничения доступа к информации и ее структура. Средства и возможности операционных систем и офисных ППП по защите от НСД к документам. Разграничение доступа к информации в базах данных.

Методы и средства защиты от несанкционированного изменения структур компьютерных систем. Механизмы, затрудняющие несанкционированное изучение и использование программного обеспечения. Методы контроля целостности информации. Доверенная загрузка ОС. Защита от НСД к внутреннему монтажу, средствам коммутации и от подключения нештатных устройств.

Тема 7. Криптографические методы защиты информации

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. Методы криптографии для идентификации и аутентификации удаленных процессов.

Тема 8. 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.

Тема 9. Защита информации в сетях и распределенных системах

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

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

Основные понятия информационной защиты сети. Средства информационной защиты компьютерных сетей. Защита по протоколу Керберос. Методы и средства обеспечения безопасной работы в глобальной сети Интернет.

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

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

5.2. Учебно-тематический план

Наборы 2018 г., 2019 г., очная 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	**Понятийный аппарат дисциплины. Основы управления информационными рисками**	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации

2	**Угрозы информационной безопасности в экономических системах, их источники и характеристика**	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
3	**Правовое и организационное обеспечение информационной безопасности в экономических системах**	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
4	**Методы и средства обеспечения информационной безопасности**	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
5	**Средства защиты и механизмы противодействия утечки информации по техническим каналам**	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
6	**Защита информации от несанкционированного доступа и изменения структур в экономических системах**	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
7	**Криптографические методы защиты информации**	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
8	**Защита компьютерных систем от вирусов и вредоносных программ**	12	3	1	2	1,5	9	Рефераты, доклады, беседы, дискуссии, презентации

9	**Защита информации в сетях и распределенных системах**	12	3	1	2	1,5	9	Рефераты, доклады, беседы, дискуссии, презентации
В целом по дисциплине		108	34	16	18	17	74	Согласно учебному плану: эссе
ИТОГО						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
Понятийный аппарат дисциплины. Основы управления информационными рисками	1. Чем обусловлена необходимость перехода от управления информационной безопасностью к управлению информационными рисками? 2. Дайте определение информационного риска в узком и расширенном смыслах. 3. Как соотносятся между собой понятия «информационный риск» и «экономическая безопасность предприятия»? 4. Приведите принципы управления информационными рисками. 5. Перечислите задачи управления информационными рисками и раскройте их содержание. 6. Каковы возможные стратегии управления информационными рисками? 7. Раскройте алгоритм управления информационными рисками. 8. Определите понятие «система управления информационными рисками» и раскройте научные принципы ее построения. 9. Перечислите задачи, решаемые в процессе создания системы управления информационными рисками. Рекомендуемые источники: Раздел 8: [1-4, 6, 8, 9, 11] Раздел 9: [1, 2].	Опрос. Групповые дискуссии по теме занятия. Изучение профессиональной терминологии в области информационной безопасности, информационного противоборства, управления информационным и рисками.
Угрозы информационной безопасности в экономических системах, их источники и характеристика	1. Что понимается под угрозами безопасности информации? 2. Приведите системную классификацию угроз. 3. Приведите определения эндогенных, экзогенных, антропогенных и техногенных угроз информационной безопасности. 4. Приведите классификацию техногенных угроз информационной безопасности. 5. Что такое угрозы конфиденциальности, целостности и доступности информации? 6. Перечислите и охарактеризуйте случайные угрозы. 7. Дайте общую характеристику преднамеренных угроз. 8. Приведите методы традиционного шпионажа и диверсий. 9. В чем состоит особенность определения несанкционированного доступа к	Опрос. Доклады, рефераты, групповые дискуссии, презентации по теме занятия. Учебное задание: Определение видов и форм информации,

	информации? 10. Какие физические процессы лежат в основе появления побочных электромагнитных излучений и наводок? 11. Охарактеризуйте особенности угроз безопасности информации, связанных с несанкционированной модификацией структур ИС. 12. Назовите особенности такого вида угроз как вредительские программы. 13. Поясните классификацию злоумышленников. 14. Раскройте понятие «Информационная война» и приведите примеры. Рекомендуемые источники: Раздел 8: [1-10, 11] Раздел 9: [1, 2].	подверженной угрозам, видов, возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов организаций, целей и задач деятельности организаций.
Правовое и организационное обеспечение информационной безопасности в экономических системах	1. Перечислите задачи государства в области безопасности информации. 2. Основные положения Доктрины информационной безопасности Российской Федерации. 3. Охарактеризуйте основные законы РФ, регулирующие отношения в области информационных технологий. 4. Назовите государственные органы, обеспечивающие безопасность информационных технологий, и решаемые ими задачи. 5. Дайте общую характеристику организационным методам защиты информации в ИС. 6. Стандарты в области защиты и безопасности информации. 7. Что такое государственная, служебная, коммерческая и банковская тайны? 8. Что такое организационное обеспечение ИБ? 9. Приведите характеристику организационных методов информационной безопасности. 10. Что понимается под термином «политика безопасности» организации? Рекомендуемые источники: Раздел 8: [1-10, 11] Раздел 9: [1, 2].	Опрос. Рефераты, доклады, беседы, групповые дискуссии, презентации по теме занятия.
Методы и средства обеспечения	1. Приведите направления защиты информации от случайных угроз. 2. Дайте общую характеристику дублированию информации (резервному	Доклады, рефераты,

информационной безопасности	копированию). 3. Какие методы дублирования информации существуют? 4. В чем заключаются методы сосредоточенного дублирования? оперативного? многоуровневого? 5. Чем отличается синхронная репликация транзакций от асинхронной? 6. В чем заключается преимущество использования технологии RAID? 7. Что такое надежность и отказоустойчивость системы? 8. Раскройте сущность подходов к созданию отказоустойчивых систем. 9. Назовите пути повышения надежности и отказоустойчивости КС. 10. Что такое помехоустойчивое кодирование? 11. Какие преимущества имеют адаптивные системы по сравнению с другими отказоустойчивыми системами? 12. По каким направлениям происходит оптимизация взаимодействия человека с КС? 13. Каким образом достигается блокировка ошибочных операций в компьютерных системах? 14. Чем достигается минимизация ущерба от аварий и стихийных бедствий? Рекомендуемые источники: Раздел 8: [11-13, 15].	групповые дискуссии по теме занятия.
Средства защиты и механизмы противодействия утечки информации по техническим каналам	1. Приведите состав системы охраны объекта и охарактеризуйте защитные свойства инженерных конструкций. 2. Каковы состав, назначение и принцип действия элементов охранной сигнализации? 3. Охарактеризуйте подсистему доступа на объект. 4. Поясните принципы защиты речевой информации в каналах связи. 5. Что такое скремблирование? 6. Перечислите и охарактеризуйте методы защиты от прослушивания акустических сигналов. 7. Охарактеризуйте средства борьбы с закладными подслушивающими устройствами. 8. Приведите механизмы, используемые для защиты от злоумышленных действий обслуживающего персонала. Рекомендуемые источники: Раздел 8: [11-14].	Доклады, рефераты, групповые дискуссии, презентация по теме занятия.
Защита информации от несанкционированного	1. В чем заключается сущность матричного (дискреционного) метода доступа? 2. Сравните матричный и мандатный методы доступа.	Доклады, рефераты,

доступа и изменения структур в экономических системах	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 OS 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? Рекомендуемые источники: Раздел 8: [11-14].	групповые дискуссии, презентации по теме занятия. Учебное задание: Способы противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности.
Криптографические методы защиты информации	1. 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 Виженера. 10. В чем заключается различие блочных и поточных шифров? 11. Каково назначение электронной подписи? 12. Каков механизм формирования электронной подписи? Рекомендуемые источники: Раздел 8: [10-14].	Доклады, рефераты, групповые дискуссии, презентации по теме занятия. Решение и разбор задач.
Защита компьютерных	1. Перечислите этапы жизненного цикла компьютерного вируса.	Доклады,

систем от вирусов и вредоносных программ	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. Рекомендуемые источники: Раздел 8: [11, 12, 14, 15].	рефераты, групповые дискуссии, презентации по теме занятия.
Защита информации в сетях и распределенных системах	1. Какова роль системы FireWall в организации безопасной работы в сети Интернет? 2. Чем симметричное шифрование отличается от несимметричного? 3. Как работает алгоритм защиты информации по протоколу Керберос? 4. Каким образом обеспечивается информационная безопасность процессов функционирования систем электронной торговли и дистанционного банковского обслуживания клиентов? 5. Какие технологии и средства защиты информации используются в системах электронной коммерции? Рекомендуемые источники: Раздел 8: [11, 15].	Доклады, рефераты, групповые дискуссии, презентации по теме занятия. Учебное задание: Программно-аппаратные средства от НСД в сетях.

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
Понятийный аппарат дисциплины. Основы управления информационным и рисками	1. Особенности информации как объекта защиты в экономических информационных системах. 2. Как соотносятся между собой понятия «информационный риск» и «экономическая безопасность предприятия»?	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, подготовка к зачету.
Угрозы информационной безопасности в экономических системах, их источники и характеристика	1. Характеристика физических каналов негативного воздействия на информационные ресурсы экономических систем. 2. Раскройте понятие «Информационная война» и приведите примеры.	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, подготовка к зачету.
Правовое и организационное обеспечение информационной безопасности в экономических системах	1. Основные положения Доктрины информационной безопасности Российской Федерации. 2. Значение организационного обеспечения информационной безопасности.	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, подготовка к зачету.
Методы и средства обеспечения информационной безопасности	1. Характеристика направлений оптимизации взаимодействия человека с КС. 2. Каким образом достигается блокировка ошибочных операций в компьютерных системах? 3. Чем достигается	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, подготовка к

	минимизация ущерба от аварий и стихийных бедствий?	зачету.
Средства защиты и механизмы противодействия утечки информации по техническим каналам	Механизмы, используемые для защиты от злоумышленных действий обслуживающего персонала	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, подготовка к зачету.
Защита информации от несанкционированного доступа и изменения структур в экономических системах	1. Возможности по разграничению доступа приложений MS Office.	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, подготовка к зачету.
Криптографические методы защиты информации	1. Что такое стеганография? 2. В чем заключается различие блочных и поточных шифров?	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, решение задач, подготовка к зачету.
Защита компьютерных систем от вирусов и вредоносных программ	Приведите характеристику загрузочных вирусов. Приведите характеристику макрокомандных вирусов. Дайте характеристику антивирусным программам.	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, подготовка к зачету.
Защита информации в сетях и распределенных системах	1. Виды защищаемой информации: семантическая и признаковая. 2. Исторический аспект развития проблемы защиты информации. 3. Развитие идей и концепций защиты	Работа с методическими материалами, конспектом лекции. Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме занятия, написание домашнего задания - эссе, подготовка к

	информации	зачету.

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю (согласно таблице 2)

Примерные варианты заданий

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

Таблица

Номер задачи	Исходный текст	Ключ зашиф-рования	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	акростих	ЯРПШЧХАГЧК	план

	системы			
17	Несанкционированный доступ к информации	пульт	ЭЯШЭИЫП	эхо
18	Стандарты управления системами информационной безопасности	алгоритм	НЮМЬУЮКФРШН	гриф
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

Примерный перечень заданий и вопросов для дискуссий

1. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.
2. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
3. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?
4. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?
5. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым

приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.

6. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.

7. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

8. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

9. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.

10. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.

11. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.

12. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.

13. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.

14. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа.

15. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.

16. Рассмотрите основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.

17. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.

18. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?

19. Объясните, что представляет собой стеганография?

20. Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования.
21. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.
22. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?
23. Раскройте основное содержание алгоритма электронной подписи.
24. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?
25. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.
26. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.
27. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?
28. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?
29. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.
30. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?
31. Дайте классификацию источников утечки информации по техническим каналам.
32. Назовите известные вам методы и средства контроля акустической информации.
33. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.
34. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.
35. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

36. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».

37. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.

38. С чем, по вашему мнению, связана необходимость организационно-правового обеспечения защиты информации? в чем заключается специфика этого обеспечения применительно к информации, обрабатываемой в автоматизированных системах?

39. Охарактеризуйте задачи, решаемые организационно-правовым обеспечением защиты информации в ЭС. Выделите особенности, связанные с «электронной» формой представления информации в ЭС.

40. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?

41. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.

42. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.

43. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.

44. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

45. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность? Каким требованиям должна удовлетворять концепция комплексной защиты?

46. Раскройте содержание функции защиты информации. Какие из функций образуют полное множество функций защиты?

47. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд,

преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

48. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.

49. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?

Примерные темы эссе

1. Основные понятия и составляющие информационной безопасности
2. Основные положения Доктрины информационной безопасности Российской Федерации
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
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 организации
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. Уголовный кодекс Российской Федерации: преступления в сфере компьютерной информации

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

17. Методы обеспечения безопасной работы в глобальной сети Интернет

18. Обеспечение информационной безопасности процессов функционирования систем электронной торговли

19. Обеспечение информационной безопасности процессов функционирования систем дистанционного банковского обслуживания

20. Применение методов криптографии для идентификации и аутентификации удаленных процессов

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

22. Средства операционных систем по защите от несанкционированного доступа к документам

23. Методы контроля целостности информации

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

Примерные темы докладов и рефератов

1. Защита информации в каналах связи
2. Защита от НСД к внутреннему монтажу, средствам коммутации, от подключения нештатных устройств
3. Средства обеспечения безопасной работы в глобальной сети Интернет
4. Активные и пассивные методы защиты компьютерных систем
5. Отличия алгоритмов DES и ГОСТ 28147-89

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

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в разделе 2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов 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. 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 организации.
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 организации 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. Классификация компьютерных вирусов и вредоносных программ. Приведите примеры.

55. Методы и средства борьбы с компьютерными вирусами и вредоносными программами.

56. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения.

57. Особенности защиты информации в распределенных КС.

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

59. Защита информации в каналах связи. Приведите примеры.

60. Межсетевое экранирование. Принцип действия схем защиты с помощью брандмауэров (межсетевые экраны).

61. Системы дистанционного банковского обслуживания, принципы и схема их функционирования. Обеспечение информационной безопасности процессов функционирования систем дистанционного банковского обслуживания.

62. Системы электронной торговли, принципы и схема их функционирования. Обеспечение информационной безопасности процессов функционирования систем электронной торговли.

63. Методы и средства обеспечения безопасной работы в сети Интернет.

Примеры оценочных средств для проверки каждой компетенции, формируемой дисциплиной

Компетенция	Индикаторы достижения компетенций	Типовые задания
ПКП-3 Способность поддержания устойчивого функционирования системы управления рисками	1. Соблюдает и поддерживает нормы профессиональной этики, нормы корпоративного управления и корпоративной культуры по рискам.	**Задание 1.** В организации функционирует система управления информационными рисками (СУИР), обеспечивающая защиту информации от рисков во всех звеньях. Чем определяется степень защищенности информационной системы предприятия от воздействия рисков?
	2. Устанавливает и поддерживает деловые контакты, связи, отношения, коммуникации с сотрудниками компании, проводит интервью с ответственными за риск работниками	**Задание 1.** Известно, что ожидаемый ущерб от определенного информационного риска незначителен, то какую стратегию управления риском необходимо выбрать. **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.
	3. Оказывает помощь сотрудникам в выявлении и оценке новых рисков, представляет аналитическую информацию о рисках для руководителей и ответственных за мероприятия по рискам работников.	**Задание 1.** Ниже на рисунке приведена схема видов угроз информации в компьютерных системах. Заполните пустые блоки видами угроз, исходя из предполагаемого перечня угроз: • Вредительские программы и компьютерные вирусы; • Сбои и отказы технических средств; • Стихийные бедствия и аварии; • Электромагнитные наводки и излучения; • Хищение носителей и отходов процессов обработки данных; • Алгоритмические ошибки; • Программные ошибки; • Несанкционированное удаление и изменение структур данных; • Ошибки пользователей сети; • Несанкционированный доступ к информации.

Рис. Угрозы безопасности информации

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

Нормативно-правовые акты

1. Гражданский Кодекс Российской Федерации (часть четвертая) № 230-ФЗ от 18.12.2006 г. (в редакции последующих законов). [Электронный ресурс], режим доступа: URL: http://www.consultant.ru/popular/gkrf4/.

2. Федеральный Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 г. (в редакции последующих законов) [Электронный ресурс], режим доступа:
http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=144689.

3. Конституция Российской Федерации. [Электронный документ].
Режим доступа:
URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=2875

4. Федеральный Закон от 20.02.1995 N 24-ФЗ (ред. от 10.01.2003) «Об информации, информатизации и защите информации» (принят ГД ФС РФ 25.01.1995) [Электронный документ]. Режим доступа: URL:

http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=40541;dst=0;ts=C4F75A6B408AF3F216D20C8155B09465;rnd=0.10125585133209825
5. Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92, № 3523–1. Режим доступа: URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=58240;dst=0;ts=E586DA8086F22852370686FE1CAAA6D2;rnd=0.696098705753684
6. Доктрина информационной безопасности Российской Федерации.
7. Закон Российской Федерации «О государственной тайне» № 5485-1 от 21.07.1993 г. (с изменениями).
8. Уголовный Кодекс Российской Федерации № 63-ФЗ от 13.06.1996 г. (с изменениями, последняя редакция), статьи 146, 147, 183, 272, 273, 274, 283, 284.
9. Федеральный Закон Российской Федерации «О коммерческой тайне» № 98-ФЗ от 29.07.2004 г. (с изменениями).
10. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (действующая редакция).

Основная литература

11. Гришина Н.В. Информационная безопасность предприятия: учебное пособие/ Н.В. Гришина. – 2-е изд., доп. – М.: ФОРУМ: ИНФРА-М, 2017. – 239 с. (Высшее образование. Бакалавриат). ЭБС ZNANIUM URL: https://znanium.com/read?id=188855.
12. Гришина Н.В. Основы информационной безопасности предприятия: учебное пособие/ Н.В. Гришина. – М.: ИНФРА-М, 2019. – 216 с. (Высшее образование. Бакалавриат). ЭБС ZNANIUM URL: https://znanium.com/read?id=343811
13. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие/ Е. К. Баранова, А. В. Бабаш. – 4-е изд., перераб. и доп. - М.: РИОР: ИНФРА-М, 2019. – 336 с. – (Высшее образование) URL: https://znanium.com/read?id=336219

Дополнительная литература

14. Дербин Е.А. Организационные основы обеспечения информационной безопасности предприятия [Электронный ресурс]: Учебное пособие для студентов, обуч. по напр. 090900.68 «Информационная безопасность» / Е.А. Дербин, С.М. Климов. – М.: Финансовый университет, кафедра

«Информационная безопасность», 2013. URL: http://elib.fa.ru/fbook/Elektr_uch._posobie_OOIB1.pdf/download/Elektr_uch._posobie_OOIB1.pdf.
15. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. – 392 с. – (Высшее образование: Бакалавриат; Магистратура). ЭБС ZNANIUM URL: http://znanium.com/catalog.php?bookinfo=474838
https://znanium.com/read?id=205045
17. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие/ В.Ф. Шаньгин. – М.: ИД «ФОРУМ» ИНФРА-М, 2017. – 592 с. ЭБС ZNANIUM URL: http://znanium.com/catalog.php?bookinfo=546679
https://znanium.com/catalog/document?id=85528.

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

1. Официальный сайт ЗАО «Консультант Плюс»: URL: – http://www.consultant.ru/
2. Официальный сайт ООО «НПП Гарант-Сервис»: URL: – www.garant.ru.
3. http://www.securitylab.ru
4. http://www.dsec.ru
5. http://www.infosec.ru

10. Методические указания для обучающихся по освоению дисциплины

Методические рекомендации по изучению дисциплины. Студентам необходимо ознакомиться:

- с содержанием рабочей программы дисциплины (далее – РПД), с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимися на образовательном портале Финуниверситета, с графиком консультаций преподавателей кафедры.

Рекомендации по подготовке к лекционным занятиям *(теоретический курс)*. Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить дисциплину. Именно поэтому контроль над

систематической работой студентов всегда находится в центре внимания кафедры. Студентам необходимо:

- перед каждой лекцией просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;

- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам, если разобраться в материале не удалось самостоятельно, то обратитесь к лектору (по графику его консультаций) или к преподавателю на семинарских занятиях. Не оставляйте «белых пятен» в освоении материала.

Рекомендации по подготовке к семинарским занятиям. Студентам следует:

- приносить с собой рекомендованную преподавателем литературу к конкретному занятию;

- до очередного семинарского занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;

- при подготовке к семинарским занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно-правовые акты и материалы правоприменительной практики;

- теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;

- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении, при решении задач, заданных для самостоятельного решения;

- в ходе семинара давать конкретные, четкие ответы по существу вопросов;

- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.

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

Выполнение и оформление эссе проводится в соответствии с методическими указаниями по выполнению эссе. Эссе сдается преподавателю для проверки в установленные преподавателем сроки.

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

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.

Самостоятельная работа студента в процессе освоения дисциплины «Информационная безопасность в экономических системах» включает:

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

На самостоятельную работу студентов отводится 74 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 в основном обзорный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов, а также призваны способствовать формированию навыков самостоятельной работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой. 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 практических аудиторных и домашних заданий студентам необходимо внимательно прочитать соответствующие разделы лекций, учебной и научной литературы и проработать аналогичные задания, рассматриваемые преподавателем на лекционных занятиях.

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.

Методические рекомендации по выполнению различных форм самостоятельных домашних заданий. Самостоятельная работа – учебная, научно-исследовательская работа студентов, выполняемая во внеаудиторное время по заданию и под руководством преподавателя. Самостоятельная работа предполагает усвоение теоретического материала на базе изучения и систематизации материалов первоисточников, монографий, статей, моделирования информационных процессов. Преподаватель планирует содержание и объем самостоятельной работы, контролирует результаты самостоятельной работы. Самостоятельная работа включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины предлагается перечень заданий для самостоятельной работы.

Цель доклада - развитие навыков аналитической работы с научной литературой, анализа дискуссионных научных позиций, аргументации собственных взглядов. Подготовка научных докладов развивает творческий потенциал обучающихся. Научный доклад готовится под руководством преподавателя, который ведет семинарские занятия. Перед началом работы по

написанию научного доклада студент согласовывает с преподавателем тему, структуру, литературу, обсуждает ключевые вопросы доклада. Структура доклада: оглавление, введение (указывается актуальность, цель и задачи), основная часть, выводы автора, список литературы (не менее 5 источников). Объем доклада согласовывается с преподавателем. Общая оценка за доклад учитывает содержание доклада, его презентацию, а также ответы на вопросы.

Реферат может быть написан на одну из предлагаемых преподавателем тем. Реферат должен быть четко структурирован: введение, основная часть (делится на ряд параграфов), заключение. Введение содержит постановку проблемы, во введении следует объяснить, чем был обоснован выбор темы, охарактеризовать актуальность и значимость темы. Особое внимание следует обратить на изученность темы в научных источниках, проанализировать использованные источники. В основной части работы должна непосредственно раскрываться объявленная тема. Выводы должны содержать авторскую оценку решения проблемы.

Эссе - работа небольшого объема и свободной композиции, выражающая индивидуальные впечатления и соображения по конкретному вопросу и заведомо не претендующее на определяющую или исчерпывающую трактовку рассматриваемо вопроса.

Эссе сочетает подчеркнуто индивидуальную позицию автора с непринужденным изложением, ориентированным на разговорную речь, т.е. эссе - это авторское сочинение небольшого объема и свободной композиции, трактующее частную тему и представляющее попытку передать индивидуальные впечатления и соображения, так или иначе с нею связанные.

Признаки эссе:

- наличие конкретной темы или вопроса;
- работа, посвященная анализу широкого круга проблем не может быть выполнена в виде эссе;
- эссе раскрывает выражение индивидуальных впечатлений и соображений по конкретному вопросу;
- в содержании эссе оцениваются в первую очередь личностное мировоззрение и мысли автора.

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»
- 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.