

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

Новороссийский филиал

Кафедра «Информатика, математика и общегуманитарные науки»

УТВЕРЖДАЮ

Директор Новороссийского
Филиала Финансового университета

Е.Н. Сейфиева
«*Сейфиева*» 2023 г.

Рабочая программа дисциплины

Управление информационной безопасностью

для студентов, обучающихся по направлению подготовки

38.03.05 Бизнес-информатика

Профиль «ИТ-менеджмент в бизнесе»

*Рекомендовано Ученым советом Новороссийского филиала Финансового университета
протокол № 26 от «27» августа 2023 г.*

*Одобрено кафедрой «Информатика, математика и общегуманитарные науки»
протокол № 01 от «27» августа 2023 г.*

Новороссийск 2023

Д.В. Тимшина. Информационная безопасность. Рабочая программа дисциплины предназначена для студентов, обучающихся по направлению подготовки бакалавров 38.03.05 «Бизнес-информатика», профиль «ИТ-менеджмент в бизнесе», очная форма обучения – Новороссийск: Новороссийский филиал Финуниверситета, кафедра «Информатика, математика и общегуманитарные науки», 2020. – 44 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.

© Новороссийский филиал Финуниверситета

СОДЕРЖАНИЕ

1. Наименование дисциплины.....	4
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине.....	4
3. Место дисциплины в структуре образовательной программы.....	6
4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	6
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	6
5.1. Содержание дисциплины	6
5.2. Учебно-тематический план	9
5.3. Содержание семинаров, практических занятий.....	11
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	14
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы.....	14
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю (согласно таблице 2).....	16
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	25
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	37
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	38
10. Методические указания для обучающихся по освоению дисциплины	38
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)	43
11.1. Комплект лицензионного программного обеспечения	43
11.2. Современные профессиональные базы данных и информационные справочные системы	43
11.3. Сертифицированные программные и аппаратные средства защиты информации	43
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	44

1. Наименование дисциплины

«Информационная безопасность».

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

Дисциплина «Информационная безопасность» по направлению 38.03.05 «Бизнес-информатика», профиль «ИТ-менеджмент в бизнесе» обеспечивает формирование следующих компетенций:

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПКН-12	Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать слабости архитектуры вычислительного оборудования, систем хранения данных, их особенности и возможности в плане противостояния вирусам, проникновения извне и хищения информации; методы разграничения доступа к данным в СХД. Уметь проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных по различным параметрам ИБ (информационной безопасности): парольная защита, шифрование данных и т.д.; уметь разграничивать доступ с данным, хранящимся в СХД и ЦОД.
		2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать рынок вычислительного оборудования, СХД (системы хранения данных) и коммуникационного оборудования для использования в ЦОД (центр обработки данных) и методы защиты этого оборудования от хищений информации и атак вирусов и хакеров; методы и приемы инфраструктурных решений наиболее отвечающим требованиям ИБ; опыт создания ЦОД с современными инфраструктурными решениями в области ИБ. Уметь консультировать в выборе вычислительного оборудования и СХД для создания ЦОД с

			использованием принципов и методов ИБ.
УК-7	Способность создавать и поддерживать безопасные условия жизнедеятельности и, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий	1. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда.	Знать разделы техники безопасности на рабочем месте, которые влияют на ИБ (отсутствие ИБП - источник бесперебойного питания), передача паролей другому лицу, свободный доступ в кабинет и т.д.). Уметь выявлять проблемы, связанные с нарушением ТБ на рабочем месте, влияющие на ИБ; устранять проблемы нарушения ТБ на рабочем месте, влияющие на ИБ.
		2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях.	Знать определение прямых рисков, грозящих уничтожению технических средств в результате стихийных бедствий и чрезвычайной ситуации (ЧС); план мероприятий при наступлении ЧС на территории предприятия и прилегающих территориях, и мероприятиях по защите населения. Уметь действовать согласно плану мероприятий на время ЧС по оказанию помощи населению и минимизированию возможного ущерба от уничтожения технических средств.
		3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей.	Знать основы безопасности жизнедеятельности людей; план действия на случай угрозы жизни людей при ЧС и защиты от возможного уничтожения технических средств. Уметь действовать согласно плана при наступлении ЧС или иной угрозе.
		4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания.	Знать план действий в экстремальной ситуации и ЧС; основные способы выживания и минимизации ущерба от возможного уничтожения технических средств. Уметь применять на практике основные способы выживания при наступлении экстремальной ситуации или ЧС; действовать согласно плана действий при наступлении экстремальной ситуации или ЧС.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к модулю общепрофессиональных дисциплин направления.

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

2020 год набора, очная форма обучения

Таблица 1

Вид учебной работы по дисциплине	Всего (в з/ед. и часах)	Семестр (модуль) 7 (в часах)
Общая трудоемкость дисциплины	4 зач. ед. / 144 ч.	144
Контактная работа - Аудиторные занятия	50	50
<i>Лекции</i>	16	16
<i>Семинары, практические занятия</i>	34	34
Самостоятельная работа	94	94
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

2020 год набора, очная форма обучения

Таблица 2

№ п/ п	Наименование тем (разделов) дисциплины	Трудоемкость в часах						Формы текущего контроля успеваемости
		Всего	Аудиторная работа				Самосто ятельна я работа	
			Общая	Лекции	Семинары, практичес кие занятия	Занятия в интерактивн ых формах		
1	Информационная безопасность в системе национальной безопасности	8	2	1	1	1	6	Рефераты, доклады, беседы, дискуссии, презентации
2	Правовое и организационное обеспечение информационной безопасности	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации

3	Основы управления информационными рисками	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
4	Информационные уязвимости объектов	8	2	1	1	1	6	Рефераты, доклады, беседы, дискуссии, презентации
5	Угрозы информационной безопасности и их источники	10	4	2	2	2	6	Рефераты, доклады, беседы, дискуссии, презентации
6	Методы и средства обеспечения информационной безопасности компьютерных систем	14	4	2	2	2	10	Рефераты, доклады, беседы, дискуссии, презентации
7	Риски информационной безопасности и проблема построения комплексной системы защиты информации	12	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
8	Особенности защиты информации в распределенных компьютерных системах	12	4	2	2	2	8	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	4	2	2	2	8	Рефераты, доклады, беседы, дискуссии, презентации
10	Защита компьютерных систем от вирусов и вредоносных программ	8	2	0	2	1	6	Рефераты, доклады, беседы, дискуссии, презентации
В целом по дисциплине		144	50	16	34	17	94	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
Информационная безопасность в системе национальной безопасности	1. Что такое информационная безопасность? 2. Виды национальной безопасности. Приведите характеристику каждого вида. 3. Какие существуют системные связи информационной безопасности с другими видами национальной безопасности? Приведите примеры. Рекомендуемые источники: Раздел 8: [2,4,6-8] Раздел 9: [1, 2, 4, 6, 7]	Доклады, рефераты, групповые дискуссии, презентация основных подходов
Правовое и организационное обеспечение информационной безопасности	1. Перечислите задачи государства в области безопасности информации. 2. Раскройте основные положения Доктрины информационной безопасности Российской Федерации. 3. Охарактеризуйте основные законы РФ, регулирующие отношения в области информационных технологий и информационной безопасности. 4. Назовите государственные органы, обеспечивающие безопасность информационных технологий, и решаемые ими задачи. 5. Дайте общую характеристику организационным методам защиты информации в ИС. Рекомендуемые источники: Раздел 8: [1 - 7] Раздел 9: [1, 2, 6]	Доклады, рефераты, групповые дискуссии, презентации.
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 Рекомендуемые источники: Раздел 8: [6 - 10]	Рефераты, доклады, беседы, дискуссии, презентации

	Раздел 9: [4, 6]	
Информационные уязвимости объектов	<p>1. Что такое антропогенные информационные уязвимости?</p> <p>2. Что такое техногенные информационные уязвимости?</p> <p>3. Приведите классификацию информационных уязвимостей.</p> <p>Рекомендуемые источники: Раздел 8: [7, 8] Раздел 9: [4, 6]</p>	Доклады, рефераты, групповые дискуссии
Угрозы информационной безопасности и их источники	<p>1. Приведите определения эндогенных, экзогенных, антропогенных и техногенных угроз информационной безопасности.</p> <p>2. Приведите классификацию техногенных угроз информационной безопасности.</p> <p>3. Что такое угрозы конфиденциальности, целостности и доступности информации?</p> <p>4. Раскройте понятие «Информационная война» и приведите примеры.</p> <p>Рекомендуемые источники: Раздел 8: [6 - 9] Раздел 9: [4, 6]</p>	Доклады, рефераты, групповые дискуссии, презентации
Методы и средства обеспечения информационной безопасности компьютерных систем	<p>1. Что такое стеганография?</p> <p>2. Что такое криптография?</p> <p>3. Что называется криптосистемой?</p> <p>4. Что такое криптоанализ?</p> <p>5. Приведите классификацию методов шифрования.</p> <p>6. Перечислите требования, которым должны отвечать современные методы шифрования.</p> <p>7. Приведите процедуру использования открытого ключа.</p> <p>8. Приведите алгоритм зашифрования с помощью таблицы Виженера.</p> <p>9. Приведите алгоритм расшифрования с помощью таблицы (матрицы) Виженера.</p> <p>10. В чем заключается различие блочных и поточных шифров?</p> <p>11. Что устанавливает электронная подпись?</p> <p>12. Как создается электронная подпись?</p> <p>Рекомендуемые источники: Раздел 8: [6, 8 - 10] Раздел 9: [4, 6]</p>	Доклады, рефераты, групповые дискуссии, презентации

<p>Риски информационной безопасности и проблема построения комплексной системы защиты информации</p>	<ol style="list-style-type: none"> 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. <p>Рекомендуемые источники: Раздел 8: [6 - 9] Раздел 9: [4, 6]</p>	<p>Доклады, рефераты, групповые дискуссии, презентации</p>
<p>Особенности защиты информации в распределенных компьютерных системах</p>	<ol style="list-style-type: none"> 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. <p>Рекомендуемые источники: Раздел 8: [6 - 8] Раздел 9: [4, 6]</p>	<p>Доклады, рефераты, групповые дискуссии, презентации</p>
<p>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</p>	<ol style="list-style-type: none"> 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? <p>Рекомендуемые источники: Раздел 8: [6 - 10] Раздел 9: [4, 6]</p>	<p>Доклады, рефераты, групповые дискуссии, презентации.</p>

Защита компьютерных систем от вирусов и вредоносных программ	<ol style="list-style-type: none"> 1. 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 «тройанский 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. <p>Рекомендуемые источники: Раздел 8: [6 - 10] Раздел 9: [4, 6]</p>	Доклады, рефераты, групповые дискуссии, презентации.
--	---	--

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	<ol style="list-style-type: none"> 1. Изучение профессиональной терминологии в области информационной безопасности и информационного противоборства. 2. Системные связи информационной безопасности с другими видами национальной безопасности. 	Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
Правовое и организационное обеспечение	<ol style="list-style-type: none"> 1. Общая характеристика организационных методов защиты информации в ИС. 	Изучение материалов по теме из разделов основной и дополнительной литературы,

информационной безопасности	2. Задачи государства в области безопасности информации.	интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
Основы управления информационными рисками	1. Возможные стратегии управления информационными рисками 2. Принципы управления информационными рисками.	Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
Информационные уязвимости объектов	1. Классификация информационных уязвимостей 2. Антропогенные и техногенные информационные уязвимости.	Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
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.	Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
Методы и средства обеспечения информационной безопасности компьютерных систем	1. Способы противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности. 2. Классификация методов шифрования.	Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
Риски информационной безопасности и проблема построения комплексной	1. Методика оценки информационных рисков. 2. Задачи решаемые в процессе создания системы	Изучение материалов по теме из разделов основной и дополнительной литературы,

системы защиты информации	управления информационными рисками.	интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
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.	Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
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.	Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.
Защита компьютерных систем от вирусов и вредоносных программ	1. Классификация компьютерных вирусов. 2. Характеристика антивирусных программ. 3. Рекомендации по антивирусной защите.	Изучение материалов по теме из разделов основной и дополнительной литературы, интернет-источников, нормативно-правовых актов, подготовка докладов, рефератов и презентаций по теме, выполнение контрольной работы, подготовка к зачету.

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

Примерные темы контрольной работы

1. Используя таблицу Виженера, решить задачи зашифрования исходного текста и расшифрования шифртекста.

Таблица

Номер задачи	Исходный текст	Ключ зашифрования	Шифртекст (криптограмма)	Ключ расшифрования
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	ЛЭЗЦДЙУИ	луч
6	Информационный риск	знак	ЖЮХЧЮНАЪН	фон
7	Конфиденциальность информации	блок	ЙКЧПХТУСЙЗЧФЗ	звук
8	Внешние и внутренние угрозы	язык	ЪКТДГЩЦМВЕБДХ	цель
9	Каналы утечки звуковой информации	гост	ББТСЯИОУЪБТУС	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	ЪЫЦЫПИЖА	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 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	ЭГРАТЦЯРЙКВЮХ	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

Примерные темы дискуссий

1. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.
2. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
4. 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?
5. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?
6. 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.
7. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.
8. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?
9. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?
10. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?
11. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.
12. 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.
13. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.

14. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.
15. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.
16. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.
17. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.
18. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа.
19. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?
20. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.
21. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.
22. Рассмотрите основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.
23. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.
24. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?
25. Объясните, что представляет собой стеганография?
26. Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования.
27. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.

28. От каких основных свойств криптографических алгоритмов зависит, на ваш взгляд, стойкость криптосистемы?
29. В чем принципиальное различие оценки стойкости криптосистемы с использованием теории информации и теории вычислительной сложности?
30. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?
31. Опишите наиболее известный алгоритм шифрования DES. Какие из основных методов шифрования использованы в этом алгоритме?
32. Каковы основные особенности криптосистем с общедоступным ключом?
33. Раскройте основное содержание алгоритма электронной подписи.
34. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.
35. Опишите последовательность установления связи и передачи сообщений в централизованных системах распределения ключей шифрования с центром трансляции ключей и с центром распределения ключей.
36. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?
37. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.
38. Попробуйте изобразить структуру компьютерного вируса в виде программы, написанной на псевдоязыке.
39. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.
40. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?
41. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?
42. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.
43. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.

44. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?
45. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.
46. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.
47. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.
48. Дайте классификацию источников утечки информации по техническим каналам.
49. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.
50. Назовите известные вам методы и средства контроля акустической информации.
51. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.
52. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.
53. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.
54. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».
55. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.
56. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.
57. 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?

58. Охарактеризуйте задачи, решаемые организационно-правовым обеспечением защиты информации в АС. Выделите особенности, связанные с «электронной» формой представления информации в АС.
59. Сформулируйте основные направления развития организационно-правового обеспечения защиты информации в зарубежных странах. Назовите известные вам законодательные акты зарубежных стран в области регулирования процессов информатизации и обеспечения безопасности информации.
60. Что вы знаете из истории развития организационно-правового обеспечения защиты информации в СССР и Российской Федерации? Охарактеризуйте современное состояние отечественной законодательной базы в области информатизации и защиты информации.
61. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?
62. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.
63. 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.
64. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.
65. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.
66. 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?
67. Сформулируйте основные концептуальные положения теории защиты информации.

68. Раскройте содержание функции защиты информации. Какие из функций образуют полное множество функций защиты?
69. Сформулируйте определение задачи защиты информации и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.
70. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?
71. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.
72. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?

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 обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

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 должнавключать...

- 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 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	Индикаторы достижения компетенций	Типовые задания
ПКН-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Задание 1 Провести анализ рынка вычислительного оборудования, коммуникационного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных по критериям ИБ - шифрование данных,

		отказоустойчивость и отсутствие незадекларированных возможностей.
	2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Задание 1 Рекомендовать заказчику вычислительное оборудование, СХД и инфраструктурные решения ЦОД с учетом требования заказчика по ИБ - отсутствие незадекларированных возможностей.
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий	1. Выявляет и устраняет проблемы, связанные с нарушением техники безопасности на рабочем месте, обеспечивая безопасные условия труда.	Задание 1 Для защиты информации в компьютерных сетях от искажения, несанкционированного доступа и уничтожения, на рабочих местах (компьютерах) должен быть проведен комплекс мероприятий. Перечислите их.
	2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях.	Задание 1 Перечислите мероприятия, которые необходимо провести для защиты информации от: - технических сбоев компьютерных компонентов, электропитания; - от действий инсайдеров, вторжения хакеров и компьютерных вирусов.
	3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей.	Задание 1 Организация имеет территориально разнесенные офисы ЦОД с СХД в столице. Все компьютеры организации соединены в корпоративную сеть. Для этого используется сеть INTRANET и INTERNET. Какие мероприятия необходимо провести для защиты данных?
	4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания.	Задание 1 Какие мероприятия необходимо провести для обеспечения сохранности информации и баз данных в условиях ЧС и природных катаклизмов. Ответ обоснуйте.

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>

Основная литература

6. Информационная безопасность и защита информации: Учебное пособие / Е. К. Баранова, А. В. Бабаш 4е изд., перераб. и доп. – М.: РИОР: ИНФРА-М, 2019. – 336 с. – Режим доступа: <https://znanium.com/read?id=359537>
7. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина – М.: ИНФРА-М, 2019. – 216 с. – (Высшее образование: Бакалавриат). Режим доступа: <https://znanium.com/read?id=343811>

Дополнительная литература

8. Внуков, А.А. Защита информации в банковской системе: учеб. пособие для бакалавриата и магистратуры / А.А. Внуков. – 2-е изд., исп. И доп. – М.: Изд-во

- Юрайт, 2019. – 246 с. (Серия: Бакалавр и магистр) – Режим доступа: <https://ez.el.fa.ru:2428/viewer/zaschita-informacii-v-bankovskih-sistemah-414083#page/1>
9. Бирюков А.А. Информационная безопасность: защита и нападение. – 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с. Режим доступа: <https://znanium.com/catalog/document?id=341187>;
<https://znanium.com/read?id=341187> (Доступ по логину и паролю через ИОП)
10. Хорев П.Б. Программно-аппаратная защита информации: учеб. пособие / П.Б. Хорев. – 2-е изд., испр. и доп. – М.: ФОРУМ : ИНФРА-М, 2019. – 352 с. – Режим доступа: <https://znanium.com/read?id=340852>;
<https://znanium.com/catalog/document?pid=1025261> (Доступ по логину и паролю через ИОП)

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

1. Справочная правовая система «КонсультантПлюс». <http://www.consultant.ru/>
2. Справочная правовая система «Гарант». [Электронный ресурс]. Режим доступа: <http://www.garant.ru/iv/>
3. Информационная безопасность для профессионалов. – URL: <http://anti-malware.ru/>
4. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
5. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
6. Электронно-библиотечная система Znanium <http://www.znanium.com>
7. Электронно-библиотечная система издательства «ЮРАЙТ»
8. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
9. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
10. Национальная электронная библиотека <http://нэб.рф/>

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 организуется на основе целей и задач программы дисциплины, является основным методом обучения и неотъемлемым элементом изучения дисциплины.

Целями самостоятельной работы 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;
- 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.

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» 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 домашних заданий;
- подготовку к семинарским занятиям в соответствии с темой занятия;
- индивидуальные и групповые консультации по наиболее сложным вопросам дисциплины;
- подготовку к зачету.

При подготовке к занятиям студент должен, 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 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.

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

Рекомендации по подготовке к лекционным занятиям (теоретический курс). Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры. Студентам необходимо перед очередной лекцией 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 практическим (семинарским) занятиям. Студентам следует:

- 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.

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.

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.