МАЭУ «МУРМАНСКАЯ АКАДЕМИЯ ЭКОНОМИКИ И УПРАВЛЕНИЯ»

ОДОБРЕНО
Решением
Ученого совета ЧОУ ВО «МАЭУ»
от «21» февраля 2018г.
Протокол № 10

УТВЕРЖДАЮ
Ректор ЧОУ ВО «МАЭУ»
О.И. Чиркова
«21» февраля 2018г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность
38.05.01 Экономическая безопасность

Специализация №1
«Экономико-правовое обеспечение экономической безопасности»

Мурманск
2018

Рабочая программа дисциплины / **Информационная безопасность**. – Мурманск: ЧОУ ВО «МАЭУ», 2018.

Информационная безопасность: Рабочая программа дисциплины по специальности 38.05.01 «Экономическая безопасность» для заочной формы обучения. Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ПООП ВО по специальности и направленности подготовки «Экономическая безопасность»

ОГЛАВЛЕНИЕ

1. Введение…….
2. Тематическое планирование……
3. Содержание дисциплины (модуля) курса……
4. Перечень учебно-методического обеспечения самостоятельной работы обучающихся……
5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)……
6. Перечень ресурсов информационно-телекоммуникационной сети «интернет», необходимых для освоения дисциплины (модуля)….
7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем……
8. Материально-техническое обеспечение дисциплины (модуля), необходимой для освоения дисциплины (модуля)……
9. Методические указания для обучающихся по освоению дисциплины (модуля)……

   Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)……..

I ВВЕДЕНИЕ

Рабочая программа дисциплины «**Информационная безопасность**» предназначена для реализации Федерального государственного стандарта высшего образования по направлению 38.05.01 «Экономическая безопасность» и является единой для всех форм обучения.

1 Указание места дисциплины в структуре образовательной программы

Дисциплины (модули), практики, предшествующие изучению данной дисциплины и формирующие аналогичные компетенции	**Код компетенции**	**Объект логической и содержательной взаимосвязи**		**Код компетенции**	**Дисциплины (модули), практики, изучаемые в последующих семестрах и формирующие аналогичные компетенции,** ИА
		Дисциплина	**Код компетенции**		
–	ПК-20	Информационная безопасность	ПК-20	ПК-20	Специализация "Экономико-правовое обеспечение экономической безопасности" Производственная (практика по получению профессиональных умений и опыта правоохранительной деятельности) Итоговая аттестация
-	ПСК-3		ПСК-3	ПСК-3	Специализация "Экономико-правовое обеспечение экономической безопасности" Итоговая аттестация

Дисциплина «Информационная безопасность» относится к базовой части профессионального цикла Б1.Б.35.03

2 Перечень планируемых результатов обучения по дисциплине соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 1− Перечень планируемых результатов обучения по дисциплине

Код компе-	**Наименование ком-**	**Вид деятельности и**	**Планируемые резуль-**	**Уровень осво-**

тенции	**петенции**	**проф. задачи**[1]	**таты**	**ения компетенции**[2]•
ПК-20	Способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Правоохранительная деятельность: реализация мер, обеспечивающих нейтрализацию факторов, способных дестабилизировать экономическую ситуацию; профилактика, предупреждение, пресечение, выявление и раскрытие преступлений и иных правонарушений в сфере экономики.	Знать: виды угроз ИС и методы обеспечения информационной безопасности Уметь: выявлять угрозы информационной безопасности в экономической отрасли	Пороговый
			Знать: виды угроз ИС и методы обеспечения информационной безопасности; модели безопасности и их применение. Уметь: выявлять угрозы информационной безопасности в экономической отрасли	Базовый
			Знать: виды угроз ИС и методы обеспечения информационной безопасности; модели безопасности и их применение. Уметь: выявлять угрозы информационной безопасности в экономической отрасли, обосновывать организационно-технические мероприятия по защите информации в ИС. Владеть: способами	Продвинутый

[1] Описываются задачи по видам деятельности, которые указываются в ФГОС по данному направлению (специальности) в соответствии с разделом IV «Характеристика профессиональной деятельности бакалавра (магистра / специалиста) ».

[2] Каждый преподаватель прописывает этот раздел самостоятельно

			выявления и защиты информации на предприятии.	
ПСК-3	Владение навыками организации системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	**Информационно-аналитическая деятельность:** поиск и оценка источников информации, анализ данных, необходимых для проведения экономических расчетов.	Знать: - общую теорию базы данных; - основные особенности создания и защиты реляционной базы данных; - создание, ведение и анализ структуры базы данных на основе форм, запросов и отчетов. - назначение, виды, характеристики и сферу применения систем и средств ведения внутреннего документооборота в экономике; Уметь: - обращаться с информационными системами и устройствами, подключаемыми к ним; - пользоваться устройствами и программами управления информационных систем и баз данных; - работать в локальных сетях и глобальной сети передачи данных. Владеть: - приемами эффективной работы с базами данных	Пороговый

			Знать: - общую теорию базы данных; - основные особенности создания и защиты реляционной базы данных; - создание, ведение и анализ структуры базы данных на основе форм, запросов и отчетов. - назначение, виды, характеристики и сферу применения систем и средств ведения внутреннего документооборота в экономике; - алгоритмы эффективного принятия оперативных решений; Уметь: - обращаться с информационными системами и устройствами, подключаемыми к ним; - пользоваться устройствами и программами управления информацией; - работать в локальных сетях и глобальной сети передачи данных; - использовать для поиска и сбора информации поисковые системы; - составлять алгоритмы для решения практических задач	Базовый

			Владеть: - приемами эффективной работы с базами данных	
			Знать: - общую теорию базы данных; - основные особенности создания и защиты реляционной базы данных; - создание, ведение и анализ структуры базы данных на основе форм, запросов и отчетов. - назначение, виды, характеристики и сферу применения систем и средств ведения внутреннего документооборота в экономике; - информационные потоки в экономических системах, их взаимосвязи с глобальной системой передачи, хранения и обработки информации Уметь: - обращаться с информационными системами и устройствами, подключаемыми к ним; - пользоваться устройствами и программами управления информацией; - работать в локальных сетях и глобальной сети пере-	Продвинутый

			дачи данных; - использовать для поиска и сбора информации поисковые системы; - составлять алгоритмы для решения практических задач; - пользоваться средствами компактного хранения и переноса информации. <u>Владеть:</u> - приемами эффективной работы с базами данных - навыками организации системы электронного документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	

Изучаемая дисциплина также дает частично знания и умения, которые позволят выпускнику по данному профилю выполнять частично обобщенные трудовые функции:

- организация и контроль текущей деятельности системы внутреннего контроля экономического субъекта, изложенные в профессиональном стандарте «Специалист по внутреннему контролю (внутренний контролер)» (утв. приказом Минтруда России от 22.04.2015)

II ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

1 Объем дисциплины и виды учебной работы

СРОК ОБУЧЕНИЯ: 5 лет 6 месяцев

ФОРМА ОБУЧЕНИЯ: заочная

Вид учебной работы	Всего час./зач.ед., форма контроля	Количество семестров
Контактная работа обучающихся с преподавателем:	**10**	**1**
В том числе:		
Лекции	4	
Практические занятия (ПЗ)	6	
Самостоятельная работа	**132**	
Вид промежуточной аттестации (зачет, экзамен)	Зачет с оценкой	
Общая трудоемкость	**144/4**	

III СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
3.1 Разделы дисциплины и виды занятий

СРОК ОБУЧЕНИЯ: 5 лет 6 месяцев

ФОРМА ОБУЧЕНИЯ: заочная

Наименование разделов и тем дисциплины	Контактная работа обучающихся с преподавателем			Самостоятельная работа, час.	Всего, час.
	Лекции, час.	Практические занятия, час.	Лабораторные занятия, час		
Тема 1. Введение в предмет. Угрозы информационной безопасности	1			22	**23**
Тема 2. Основные понятия теории информационной безопасности	1			22	**23**
Тема 3. Программно-технические методы защиты	1			22	**23**
Тема 4. Организационно правовые методы информационной безопасности	1	2		22	**25**
Тема 5. Роль стандартов в обеспечении информационной безопасности				22	**22**
Тема 6. Технологии построения защищенных систем и баз данных		4		22	**26**
Зачёт с оценкой					**2**
ВСЕГО	**4**	**6**	**0**	**132**	**144**

3.2 Содержание дисциплины, структурированное по темам

Тема 1. Введение в предмет. Угрозы информационной безопасности.

Содержание темы: Понятие информационной безопасности и защищенной системы. Международные стандарты информационного обмена. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем. Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.

Тема 2. Основные понятия теории информационной безопасности.

Содержание темы: Основные положения теории информационной безопасности информационных систем. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления досту-

пом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Тема 3. Программно-технические методы защиты.

Содержание темы: Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности. Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

Тема 4. Организационно правовые методы информационной безопасности.

Содержание темы: Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Ос-

новные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

Тема 5. Роль стандартов в обеспечении информационной безопасности.

Содержание темы: Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем. Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев.

Тема 6. Технологии построения защищенных систем и баз данных

Содержание темы: Использование защищенных компьютерных систем и баз данных. Общие принципы построения защищенных систем и баз данных. Иерархический метод разработки защищенных систем и баз данных. Структурный принцип. Принцип модульного программирования. Исследование коррект-

ности реализации и верификации автоматизированных систем. Спецификация требований, предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

V ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Общий объем самостоятельной работы обучающихся по дисциплине включает аудиторную и внеаудиторную самостоятельную работу в течение семестра. Аудиторная самостоятельная работа осуществляется в форме тестирования, выполнение практических работ, внеаудиторная самостоятельная работа осуществляется в следующих формах:

- самостоятельная работа при подготовке к практическим занятиям;
- самостоятельная работа по подготовке ответов на вопросы и выполнение заданий;
- самостоятельное изучение теоретического материала;
- подготовка рефератов, эссе.

Перечень проверяемых компетенций

ПК-20 – способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности.

ПСК-3 – владение навыками организации системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов.

4.1 Перечень заданий для самостоятельной работы

ПК-20:

1. Определить место информационной безопасности в обеспечении системы экономической безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности в сфере экономики.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Охарактеризовать технические каналы несанкционированного доступа к информации.
14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
15. Проанализировать особенности угроз автоматизированным банковским системам.
16. Дать классификацию удаленных атак.
17. Проанализировать основные направления правовой защиты инфор-

мации.

18. Определить объекты защиты авторских прав.

19. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.

20. Дать определение государственной тайны и назвать грифы секретности.

21. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.

22. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.

23. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.

24. Назвать основные положения концепции информационной безопасности предприятия.

ПСК-3:

25. Изложить содержание регламента обеспечения информационной безопасности в базах данных.

26. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации в БД.

27. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

28. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.

29. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.

30. Сформулировать возможности, трудности и направления использования

электронной почты для передачи конфиденциальных документов и БД.

31. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.

32. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.

33. Назвать основные элементы физической защиты территории и помещений предприятия.

34. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов и БД.

4.2 Тематика рефератов

ПК-20

1. Политика информационной безопасности предприятия.

2. Нормативно-правовая база обеспечения информационной безопасности предприятия.

3. Содержание основных законов Российской Федерации в сфере компьютерного права.

4. Законодательная база РФ по вопросам защиты информации.

5. Комплексный подход к обеспечению информационной безопасности.

6. Законодательные и нормативные акты РФ о предпринимательской деятельности.

7. Машинное представление информации.

8. Виды и формы представления информации.

9. Информация как объект права собственности.

10. Информация как коммерческая тайна.

11. Информация как рыночный продукт.

12. Элементы и объекты защиты в АС.

13. Основные виды вирусов и схемы их функционирования.

14. Обнаружение вирусов и меры по защите и профилактике

15. Основные меры защиты от вирусов.

16. Программно-технические меры обеспечения информационной безопасности.

17. Обеспечение информационной безопасности средствами Windows 7.

ПСК-3:

18. Жизненный цикл, разработка, поддержка и сопровождение баз данных.

19. Сетевые, распределённые и параллельные базы данных.

20. Специализированные машины и системы баз данных.

21. Архитектура, технология разработки и защиты экспертных систем

22. Безопасное хранение данных на основе шифрования.

23. Американский стандарт шифрования данных DES.

24. Стандарт шифрования данных ГОСТ 28147-89.

25. Система цифровой телефонии.

26. Комплексный подход к обеспечению информационной безопасности в БД

4.3. Вопросы к контрольной работе:

1. Что такое информационная безопасность?
2. Перечислите важнейшие аспекты информационной безопасности.
3. Перечислите уровни решения проблемы информационной безопасности.
4. Перечислите уровни защиты информации.
5. Охарактеризуйте угрозы информационной безопасности: раскрытия целостности, отказ в обслуживании.
6. Объясните причины компьютерных преступлений.
7. Опишите, как обнаружить компьютерное преступление или уязвимые места в системе информационной безопасности.
8. Опишите основные технологии компьютерных преступлений.

9. Перечислите меры защиты информационной безопасности.

10. Перечислите меры предосторожности при работе с целью защиты информации.

11. Опишите, какими способами можно проверить вводимые данные на корректность.

12. Опишите основные меры защиты носителей информации.

13. Почему подключение к глобальной компьютерной сети Интернет представляет собой угрозу для информационной безопасности?

14. Опишите, как использование электронной почты создает угрозу информационной безопасности. Какие меры обеспечивают безопасное использование e-mail?

15. Охарактеризовать особенности экономической информации

16. Перечислить основные характеристики экономической информации

17. Что такое документ, документооборот?

18. Какова классификация документов?

19. Что такое реляционная БД? Ее особенности и защита.

V ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Основная литература:

Информационная безопасность [Электронный ресурс]: учебник / Т.Ю. Васильева, А.И. Куприянов, В.П. Мельников. – Электрон. текстовые данные. — Москва : КноРус, 2018. — 371 с. — ISBN 978-5-406-04906-8. - Режим доступа: https://www.book.ru/book/929884 - ЭБС BOOK.ru, по паролю

Дополнительная литература:

Информационная безопасность. Введение в специальность (для бакалавров) + еПриложение: Тесты. Учебник [Электронный ресурс]: учебник / В.А. Медведев. – Электрон. текстовые данные. — Москва : КноРус, 2019. —

144 с. — ISBN 978-5-406-06590-7. - Режим доступа: https://www.book.ru/book/930545 - ЭБС BOOK.ru, по паролю

Информационная безопасность. Лабораторный практикум (для бакалавров)+ Электронные приложения на сайте www.book.ru [Электронный ресурс]: учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – Электрон. текстовые данные. — Москва : КноРус, 2018. — 131 с. — ISBN 978-5-406-05990-6. - Режим доступа: https://www.book.ru/book/926191 - ЭБС BOOK.ru, по паролю

VI ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Справочно-поисковые системы информационно-правового обеспечения ГАРАНТ-Максимум и КОНСУЛЬТАНТ + http://www.garant.ru/, http://www.consultant.ru/
2. Центр проблем информационного права - http://www.medialaw.ru/
3. Институт развития информационного общества в России http://www.iis.ru/index.html
4. Единое окно доступа к образовательным ресурсам http://window.edu.ru.
5. ЭБС: http://www.iprbookshop.ru
6. https://www.lektorium.tv/ – Интернет-библиотека видеолекций от ведущих лекторов ВУЗов России
7. http://www.teachvideo.ru/catalog/ – Обучающие видеокурсы

VII ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧ-

НЫХ СИСТЕМ

При осуществлении образовательного процесса по дисциплине «Информационная безопасность» широко используются информационные технологии такие как:

1. Консультант плюс - Consultant.ru
2. Гарант - garant.ru
3. Microsoft Windows 7 Professional
4. Microsoft Office 2013 Professional plus
5. Интернет браузер Internet Explorer
6. Adobe Acrobat Reader

VIII ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ ДИСЦИПЛИНЫ, НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Центр (класс) деловых игр, учебная аудитория для проведения занятий лекционного типа

(183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 4 этаж, ауд. 407)

Комплект учебной мебели на 48 человек; оснащена электронным УМК по дисциплинам, электронные учебные пособия по дисциплинам в ЭБС, слайд-лекции, демонстрационный экран, мультимедийный видеопроектор,автоматизированное рабочее место преподавателя с программным обеспечением, доступ к сети Internet.

Программное обеспечение: Лицензионное: операционная система Windows; офисные программы MicrosoftOffice; справочно-правовая система КонсультантПлюс; электронная библиотечная система.

Учебная аудитория для проведения занятий семинарского типа

(183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 4 этаж, ауд. 401)

Комплект учебной мебели на 24 человека; оснащен электронным УМК по

общепрофессиональным дисциплинам, электронные учебные пособия по дисциплинам в ЭБС, слайд-лекции, переносной демонстрационный экран, переносной мультимедийный проектор, автоматизированное рабочее место преподавателя с программным обеспечением, доступ к сети Internet.

Программное обеспечение: Лицензионное: операционная система Windows; офисные программы MicrosoftOffice; справочно-правовая система КонсультантПлюс; электронная библиотечная система.

Учебный зал судебных заседаний, центр (класс) деловых игр, учебная аудитория для проведения занятий семинарского типа (183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 4 этаж, ауд. 403)

Зал рассчитан на 26 посадочных мест, оборудован компьютером для секретаря судебного заседания, мультимедийной системой для представления аудио, видеодоказательств, трибуна для представления свидетельских показаний, место для представителей государственного обвинения, место судей, место адвоката, место для подсудимого, герб РФ, флаг РФ, мантия судьи,

Лицензионное программное обеспечение: операционная система Windows; офисные программы MicrosoftOffice; справочно-правовая система КонсультантПлюс; электронная библиотечная система.

Учебная аудитория для проведения индивидуальных консультаций по направлению подготовки 38.05.01 Экономическая безопасность

(183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 2 этаж, ауд. 204)

Комплект учебной мебели на 4 человека; оснащенные лицензионным программным обеспечением, с выходом в локальную сеть ЧОУ ВО «МАЭУ», глобальную сеть Интернет и обеспечением доступа в электронную информационно-образовательную среду ЧОУ ВО «МАЭУ»

Программное обеспечение: Лицензионное: операционная система Windows; офисные программы MicrosoftOffice; электронная библиотечная система.

Учебная аудитория для проведения групповых консультаций, текущего

контроля и промежуточной аттестации

(183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 4 этаж, ауд. 405)

Комплект учебной мебели на 98 человек; оснащена электронным УМК по дисуиплинам; электронные учебные пособия по дисциплинам в ЭБС, слайд-лекции, переносной демонстрационный экран, переносной мультимедийный видеопроектор, автоматизированное рабочее место преподавателя с программным обеспечением, доступ к сети Internet, программное обеспечение: Лицензионное: операционная система Windows; офисные программы MicrosoftOffice; справочно-правовая система КонсультантПлюс; электронная библиотечная система.

Лаборатория информатики и информационных технологий (183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 3 этаж, ауд. 305)

Автоматизированные рабочие места для обучающихся (20 мест), оснащенные лицензионным программным обеспечением, с выходом в локальную сеть ЧОУ ВО «МАЭУ», глобальную сеть Интернет и обеспечением доступа в электронную информационно-образовательную среду ЧОУ ВО «МАЭУ». Программное обеспечение: электронный УМК; слайд-лекции, демонстрационный экран, мультимедийный видеопроектор, автоматизированное рабочее место преподавателя с программным обеспечением, доступ к сети Internet.

Программное обеспечение:

Лицензионное: операционная система Windows; офисные программы MicrosoftOffice; Использование не в коммерческих целях: программа для тестирования MyTest.

Кабинет информатики (компьютерный класс) (183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 2 этаж, ауд. 211)

Комплект учебной мебели на 16 человек; оснащена электронными УМК по дисциплинам, электронные учебные пособия по дисциплинам в ЭБС, слайд-

лекции, лингафонное оборудование, переносной мультимедийный видеопроектор, переносной демонстрационный экран, автоматизированное рабочее место преподавателя с программным обеспечением, доступ к сети Internet.

Программное обеспечение: Лицензионное: операционная система Windows; офисные программы MicrosoftOffice; электронно-библиотечная система, Использование не в коммерческих целях: программа для тестирования MyTest.

Кабинет информатики (компьютерный класс) (183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 2 этаж, ауд. 212)

Комплект учебной мебели на 29 человек;

оснащена электронными УМК по дисциплинам, электронные учебники по дисциплинам в ЭБС, слайд-лекции, переносной мультимедийный видеопроектор, переносной демонстрационный экран, автоматизированное рабочее место преподавателя с программным обеспечением, доступ к сети Internet.

Программное обеспечение: Лицензионное: операционная система Windows; офисные программы MicrosoftOffice; электронная библиотечная система.

Использование не в коммерческих целях: программа для тестирования MyTest.

Помещение для самостоятельной работы

(183025, Российская Федерация, Северо-Западный федеральный округ, Мурманская область, г. Мурманск, ул. Полярной Правды, д.8, 2 этаж, ауд. 203)

Автоматизированные рабочие места для обучающихся (18 мест), оснащенные лицензионным программным обеспечением, с выходом в локальную сеть ЧОУ ВО «МАЭУ», глобальную сеть Интернет и обеспечением доступа в электронную информационно-образовательную среду ЧОУ ВО «МАЭУ». Программное обеспечение:

Лицензионное: операционная система Windows; офисные программы MicrosoftOffice; Использование не в коммерческих целях: программа для тестирования MyTest.

IX МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

9.1 План практических занятий

№ П/П	№ Модуля (раздела) дисциплины	Наименование практических занятий
1.	Введение в предмет. Угрозы информационной безопасности	-
2.	Основные понятия теории информационной безопасности	Изучение положений о государственном лицензировании деятельности в области защиты информации. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации.
3.	Программно-технические методы защиты	Система сертификации средств криптографической защиты информации. Изучение положения о сертификации средств вычислительной техники и связи.
4.	Организационно правовые методы информационной безопасности	Законодательство РФ в области информационной безопасности Изучение положения по аттестации объектов информатизации по требованиям безопасности информации. Изучение особенностей аттестации помещений по требованиям безопасности информации.
5.	Роль стандартов в обеспечении информационной безопасности	Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации. Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации.
6.	Технологии построения защищенных систем и баз данных	Парольная защита Архивирование с паролем Шифр простой замены. Таблица Вижинера Обмен ключами по Диффи-Хелману Шифр RSA Циклические коды Создание и защита баз данных на примере MS ACCESS.

9.2 План занятий в интерактивной форме

СРОК ОБУЧЕНИЯ: 5 лет 6 месяцев

ФОРМА ОБУЧЕНИЯ: заочная

Наименование тем дисциплины	Форма реализации интерак-	Контактная работа обучающихся с преподавателем	Самостоятельная	Всего час.

	тивной работы	Лекции	Практические занятия	Лабораторные занятие	работа	
Раздел 1. Технологии создания и преобразования информационных объектов						
Тема 1. Введение в предмет. Угрозы информационной безопасности.	Дискуссия, работа в малых группах					
Тема 2. Основные понятия теории информационной безопасности.	Дискуссия, работа в малых группах					
Тема 3. Программно-технические методы защиты.	Дискуссия, работа в малых группах					
Тема 4. Организационно правовые методы информационной безопасности	Дискуссия, работа в малых группах		2			2
Тема 5. Роль стандартов в обеспечении информационной безопасности	Дискуссия, работа в малых группах					
Тема 6. Технологии построения защищенных систем и баз данных	Дискуссия, работа в малых группах		2			2
Всего			**4**			**4**

9.3 Описание показателей и критерии оценивания компетенций по текущему контролю

Код компетенции	Наименование компетенции	Наименование темы	Виды текущего контроля успеваемости	Средства оценки по теме	Критерии оценки в зависимости от уровня освоения компетенции
ПК-20	способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности.	Угрозы информационной безопасности Основные понятия теории информационной безопасности Программно-технические методы защиты	Лекции, практические занятия, интерактивные занятия, дискуссия в малых группах	Тестовые задания, реферат	Пороговый от 60 до 73 баллов Базовый от 74 до 87 баллов Продвинутый от 88 до 100 баллов

ПСК-3	владение навыками организации системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов.	Организационно правовые методы информационной безопасности Роль стандартов в обеспечении информационной безопасности Технологии построения защищенных систем	Лекции, практические занятия, интерактивные занятия. дискуссия в малых группах	Тестовые задания, контрольная работа, реферат	Пороговый от 60 до 73 баллов
					Базовый от 74 до 87 баллов
					Продвинутый от 88 до 100 баллов

9.5 Типовые задания для текущего контроля

Перечень проверяемых компетенций

ПК-20 – способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности.

ПСК-3 – владение навыками организации системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов.

9.5 Типовые задания для текущего контроля

1) какая цель не является основной целью Информационной безопасности

А) доступность

Б) целостность

В) конфиденциальность

Г) открытость

2) назовите несуществующий способ обеспечения безопасности компьютерных систем

А) логический

Б) административный

В) физический

Г) правовой

3) на flash-носителе обнаружен вирус, подобный вирус обнаружен на сервере в профиле пользователя. Кто будет нести ответственность за нарушение ИБ

А) пользователь

Б) начальник

В) системный администратор

Г) начальник службы безопасности

4) контроль за соблюдением инструкции по работе с компьютерной техникой осуществляет

А) пользователь

Б) начальник

В) системный администратор

Г) начальник службы безопасности

6) по условию начала осуществления воздействие не существует атаки

А) после запроса от атакуемого объекта

Б) после наступления ожидаемого события на атакуемом объекте

В) безусловная

Г) после выполнения программы пользователя

7) к случайным не относится угроза?

А) ошибка персонала

Б) форс-мажор

В) ошибка автоматизированных систем

Г) программы закладки

8) за соблюдением ИБ на сетевой инфраструктуре отвечает

А) начальник службы информационной безопасности

Б) начальник

В) системный администратор

Г) начальник службы безопасности

9) безусловной атакой является атака когда

А) пользователь принес вирус на дискете

Б) пользователь открыл зараженное письмо которое парализовало работу на компьютере

В) злоумышленник открыто похитил диск с информацией оставленный без присмотра

Г) на ПК обнаружен вирус, передающий информацию в интернет

10) недокументированная возможность, содержащаяся в полезной программе называется

А) троянец

Б) червь

В) программа-шутка

Г) программа закладка

11) удаление вируса при помощи антивируса, запущенного с локальной машины - это способ защиты

А) комплексный

Б) фрагментальный

В) целостный

Г) административный

12) определите порядок действий при проведения атаки

А) 1234

Б) 4231

В) 1243

Г) 3421

13) угроза ИБ с обратной связью

А) пользователь принес вирус на дискет

Б) пользователь получил зараженное письмо, которое парализовало работу ПК

В) злоумышленник открыто похитил диск с информацией оставленный без присмотра, получил доступ к системе которым воспользовался

Г) на ПК обнаружен вирус

14) программой - закладной называют вирус

А) размножающий себя на ПК

Б) приводящий к временному изменению ссылок на программы

В) выдающий себя за какую-либо полезную программу

Г) активируется при нажатии сочетании клавиш

15) удаленная проверка компьютеров на вирусы.... защиты

А) часть фрагментального способа

Б) часть комплексного способа

В) часть целостного способа

Г) комплексный способ

16). Какая наименьшая единица хранения данных е БД?

а. хранимое поле

b. хранимый файл

c. ничего из вышеперечисленного

d. хранимая запись

e. хранимый байт

17). Что обязательно должно входить в СУБД?

a. процессор языка запросов

b. командный интерфейс

c. визуальная оболочка

d. система помощи

18). Перечислите преимущества централизованного подхода к хранению и управлению данными.

a. возможность общего доступа к данным

b. поддержка целостности данных

c. соглашение избыточности

d. сокращение противоречивости

19). Предположим, что некоторая база данных описывается следующим перечнем записей:

1 Иванов, 1956, 2400

2 Сидоров, 1957, 5300

3 Петров, 1956, 3600

4 Козлов, 1952, 1200

20). Какие из записей этой БД поменяются местами при сортировке по возрастанию, произведенной по первому полю:

a. 3 и 4;

b. 2 и 3;

c. 2 и 4;

d. 1 и 4

e. 1 и 3;

21). Структура файла реляционной базы данным (БД) меняется:

a. при изменении любой записи;

b. при уничтожении всех записей;

c. при удалении любого поля.

d. при добавлении одной или нескольких записей;

e. при удалении диапазона записей;

23) Как называется набор хранимых записей одного типа?

a. хранимый файл

b. представление базы данных

c. ничего из вышеперечисленного

d. логическая таблица базы данных

e. физическая таблица базы данных

24.Утечка информации

Выберите один из 3 вариантов ответа:

1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу

2) ознакомление постороннего лица с содержанием секретной информации

3) потеря, хищение, разрушение или неполучение переданных данных

25. Под изоляцией и разделением (требование к обеспечению ИБ) понимают
Выберите один из 2 вариантов ответа:
1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)
2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

26. К аспектам ИБ относятся
Выберите несколько из 5 вариантов ответа:
1) дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность

27. Линейное шифрование -
Выберите один из 3 вариантов ответа:
1) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
3) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами

28. Угроза - это
Выберите один из 2 вариантов ответа:
1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов
2) событие, действие, процесс или явление, которое приводит к ущербу чьих-

либо интересов

29. Под ИБ понимают

Выберите один из 3 вариантов ответа:

1) защиту от несанкционированного доступа

2) защиту информации от случайных и преднамеренных воздействий естественного и исскуственного характера

3) защиту информации от компьютерных вирусов

30. Что такое криптография?

Выберите один из 3 вариантов ответа:

1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

2) область доступной информации

3) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом

31. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется

Выберите один из 4 вариантов ответа:

1) кодируемой

2) шифруемой

3) недостоверной

4) защищаемой

32. Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это

Выберите один из 4 вариантов ответа:

1) текст

2) данные

3) информация

4) пароль

33. Организационные угрозы подразделяются на

Выберите несколько из 4 вариантов ответа:

1) угрозы воздействия на персонал

2) физические угрозы

3) действия персонала

4) несанкционированный доступ

34. Виды технической разведки (по месту размещения аппаратуры)

Выберите несколько из 7 вариантов ответа:

1) космическая

2) оптическая

3) наземная

4) фотографическая

5) морская

6) воздушная

7) магнитометрическая

35. Основные группы технических средств ведения разведки

Выберите несколько из 5 вариантов ответа:

1) радиомикрофоны

2) фотоаппараты

3) электронные "уши"

4) дистанционное прослушивание разговоров

5) системы определения местоположения контролируемого объекта

36. Разновидности угроз безопасности

Выберите несколько из 6 вариантов ответа:

1) техническая разведка

2) программные

3) программно-математичекие

4) организационные

5) технические

6) физические

37. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

Выберите один из 4 вариантов ответа:

1) угрозой;

2) опасностью;

3) намерением;

4) предостережением.

38. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

Выберите один из 4 вариантов ответа:

1) операционной системы, сетевого программного обеспечения

2) операционной системы, сетевого программного обеспечения и системы управления базами данных;

3) операционной системы, системы управления базами данных;

4) сетевого программного обеспечения и системы управления базами данных.

39. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

Выберите один из 4 вариантов ответа:

1) системой угроз;

2) системой защиты;

3) системой безопасности;

4) системой уничтожения.

40. К видам защиты информации относятся:

Выберите несколько из 4 вариантов ответа:

1) правовые и законодательные:

2) морально-этические;

3) юридические;

4) административно-организационные;

9.6 Особенности организации и содержания учебного процесса по дисциплине

Проведение учебных занятий в форме лекционных, лабораторных занятий в интерактивной форме, работы в малых группах обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 1− Результаты освоения компетенции

Код компетенции	Наименование компетенции	Дисциплины, практики, при изучении которых формируется данная компетенция•	Этапы формирования компетенции в рамках данной дисциплины (наименование разделов)
ПК-20	способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	1, 2, 3, 4, 5, 6	1, 2, 3, 4, 5, 6
ПСК-3	владение навыками организации системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	6	6

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 2 – Шкала оценивания

Код компетенции	**Планируемые результаты освоения дисциплины (модуля)**	**Уровень освоения компетенции**	**Показатели оценивания компетенции (перечень необходимых заданий)**[3]		**Критерии оценивания компетенции**
			Теоретические	**Практические**	**Зачет с оценкой**[4]

• Указываются дисциплины (модули), практики, читаемые в предыдущих семестрах (см. учебный план)

[3] Если задание одинаковое для всех уровней освоения компетенций, то критерием оценивания является качество выполнения задания.

[4] Итоговая оценка за экзамен, дифференцированный зачет выставляется по среднему баллу, отражающему уровень освоения компетенций

			вопросы (№ или от … до)	**задания (№ или от … до)**	
ПК-20	Знать: виды угроз ИС и методы обеспечения информационной безопасности Уметь: выявлять угрозы информационной безопасности в экномической отрасли	Пороговый уровень	1-9	Контрольная работа	Пороговый уровень «3» − от 10 до 18 б.
	Знать: виды угроз ИС и методы обеспечения информационной безопасности; модели безопасности и их применение. Уметь: выявлять угрозы информационной безопасности в экномической отрасли	Базовый уровень	10-20		Базовый уровень «4» − от 21 до 24 б.
	Знать: виды угроз ИС и методы обеспечения информационной безопасности; модели безопасности и их применение. Уметь: выявлять угрозы информационной безопасности в экономической отрасли, обосновывать организационно-технические мероприятия по защите информации в ИС. Владеть: способами	Продвинутый уровень	10-20		Продвинутый уровень «5» − от 25 до 30 б.

	выявления и защиты информации на предприятии.				
ПСК-3	Знать: - информационное обеспечение экономического процесса предприятия; - назначение, виды, характеристики и сферу применения систем и средств связи; - информационные потоки в экономических системах, их взаимосвязи с глобальной системой передачи, хранения и обработки информации Уметь: - обращаться с информационными системами и устройствами, подключаемыми к ним; - пользоваться устройствами и программами управления информацией; - работать в локальных сетях и глобальной сети передачи данных; Знать: - роль в организации информационной безопасности предприятия; - информационное обеспечение эконо-	Пороговый уровень Базовый уровень	30-37 30-37	Контрольная работа Контрольная работа	Пороговый уровень «3» − от 10 до 18 б. Базовый уровень «4» − от 21 до 24 б.

	мического процесса предприятия; - назначение, виды, характеристики и сферу применения систем и средств связи; - информационные потоки в экономических системах, их взаимосвязи с глобальной системой передачи, хранения и обработки информации; - автоматизированную систему управления (АСУ), как инструмента оптимизации процессов управления в экономических системах; - структуру, уровни построения и функции АСУ в экономике - алгоритмы эффективного принятия оперативных решений <u>Уметь:</u> - обращаться с информационными системами и устройствами, подключаемыми к ним; - пользоваться устройствами и программами управления информацией; - работать в локальных сетях и гло-				

	бальной сети передачи данных; - использовать для поиска и сбора информации поисковые системы; - составлять алгоритмы для решения практических задач; <u>Знать:</u> - роль организации информационной безопасности предприятия; - информационное обеспечение экономического процесса предприятия; - назначение, виды, характеристики и сферу применения систем и средств связи; - информационные потоки в экномических системах, их взаимосвязи с глобальной системой передачи, хранения и обработки информации; - автоматизированную систему управления (АСУ), как инструмента оптимизации процессов управления в экономических системах; - структуру, уровни построения и функции АСУ; - алгоритмы эффективного принятия	Продвинутый уровень	30-37	5	Продвинутый уровень «5» − от 25 до 30 б.

	оперативных решений; - техническое и информационное обеспечение АСУ; основы передачи данных; базы и банки данных. <u>Уметь:</u> - обращаться с информационными системами и устройствами, подключаемыми к ним; - пользоваться устройствами и программами управления информацией; - работать в локальных сетях и глобальной сети передачи данных; - использовать для поиска и сбора информации поисковые системы; - составлять алгоритмы для решения практических задач; - пользоваться средствами компактного хранения и переноса информации. <u>Владеть</u>: - навыками организации системы электронного документооборота организации, ведения баз данных по различным показате-				

	лям и формирования информационного обеспечения участников организационных проектов				

Перечень вопросов к зачету с оценкой

1. Основные угрозы безопасности России. Информационная безопасность. Определение. Аспекты информационной безопасности. Направления обеспечения ИБ

2. Жизненно важные интересы и угрозы в информационной сфере. Уровни угроз ИБ и их классификация.

3. Защита информации. Определение. Формы и способы защиты. Политика безопасности и гарантированности.

4. Основные предметные направления защиты информации. Правовые основы защиты информации. Структура законодательства России в области защиты информации.

5. Предмет и объекты защиты информации в автоматизированных системах обработки информации (АСОД). Надежность информации. Уязвимость информации.

6. Элементы и объекты защиты в АСОД. Основные элементы АСОД и типовые структурные компоненты.

7. Дестабилизирующие факторы АСОД. Причины нарушения целостности информации. Каналы несанкционированного получения информации в АСОД.

8. Преднамеренные угрозы безопасности АСОД. Атаки. Классификация угроз безопасности.

9. Функции и задачи защиты информации в АСОД. Механизм защиты.

10. Методы и системы защиты информации в АСОД. Целостность и конфиденциальность информации.

11. Аутентификация и идентификация. Подтверждение подлинности

пользователей и разграничение их доступа к компьютерным ресурсам. Контроль доступа к аппаратуре.

12. Процедура опознавания с использование простого пароля. Методы проверки подлинности на основе динамически изменяющегося пароля.

13. Методы идентификации и установления подлинности субъектов и различных объектов. Функциональные методы.

14. Контроль информационной целостности. Организация контроля. Способы модификаций информации.

15. Защита информации от утечки по техническим каналам. Определения, понятия и виды каналов утечки.

16. Защита информации от утечки по визуально-оптическим и акустическим каналам.

17. Защита информации от утечки по электромагнитным и материально-вещественным каналам.

18. Технические средства защиты. Классификация технических средств. Функции защиты и степень сложности устройства.

19. Механические системы защиты. Системы оповещения. Системы опознавания. Оборонительные системы. Охранное освещение.

20. Физические средства защиты. Средства контроля доступа. Автоматизированные системы контроля доступа.

21. Биометрические системы идентификации. Основные методы. Охранные системы.

22. Защита информации в персональных ЭВМ. Особенности защиты.

23. Угрозы информации в персональных ЭВМ. Классификация угроз. Виды каналов утечки.

24. Обеспечение целостности информации в персональных компьютерах (ПК). Защита ПК от несанкционированного доступа.

25. Физическая защита ПК и носителей информации. Опознавание (аутентификация) пользователей и используемых компонентов обработки информации.

26. Разграничение доступа к элементам защищаемой информации. Виды и характеристика способов доступа.

27. Регистрация обращений к защищаемой информации. Подсистема управления доступом. Подсистема регистрации и учета. Криптографическая система.

28. Защита информации от копирования. Основные функции систем защиты программ от копирования.

29. Защита от несанкционированного доступа к персональным компьютерам. Защита в среде MS DOS. Защита в средах Windows.

30. Классификация информации, баз данных и их общие характеристики.

31. Средства борьбы с вирусами и вредоносными закладками: юридические, организационно-административные, аппаратные и программные. Основные функции и мероприятия по защите баз данных.

32. Компьютерные вирусы. Классификация. Виды и характеристики вирусов, ориентированных на электронный документооборот и базы данных

33. Способы заражения программ компьютерными вирусами. Схема функционирования загрузочного вируса в БД.

34. Цели, функции и задачи защиты информации в сетях ЭВМ. Виды угроз в базах данных.

35. Основные угрозы безопасности России. Информационная безопасность. Определение. Аспекты информационной безопасности. Направления обеспечения ИБ в БД

36. Защита информации. Определение. Формы и способы защиты. Политика безопасности и гарантированности в БД.

37. Основные средства защиты. Средства контроля доступа. Автоматизированные системы контроля доступа в БД.

Вопросы к контрольной работе:

1. Защита информации в локальных вычислительных сетях на предприятии

2. Программные средства защиты информации от преднамеренных угроз под управлением WINDOWS

3. Разработка АС обеспечения информационной безопасности при сборе информации с экспресс-офисов компании

4. Разработка политики безопасности высшего учебного заведения

5. Разработка комплекса защитных мер по обеспечению информационной безопасности баз данных

6. Разработка предложений по защите телефонных каналов связи коммерческого банка

7. Внедрение системы контроля и управления доступом (СКУД) на предприятии

8. Разработка комплексной системы безопасности браузерной онлайн-игры

9. Организация защиты и функционирование электронной почты в сетях

10. Разработка системы контроля и управления доступом в Интернет-компании

11. Разработка мероприятий по резервному копированию данных серверов для обеспечения их максимальной отказоустойчивости

12. Внедрение и обеспечение системы информационной безопасности автоматизированной банковской системы

13. Внедрение системы межсетевого экранизирования ЛВС компании

14. Защита персональных данных в компании-партнере 1С

15. Модернизация комплекса антивирусный защиты в производственной компании

16. Разработка мероприятий по защите от несанкционированного доступа к информации в ЛВС медийной компании

17. Разработка политики безопасности рекламного агентства

18. Организация защиты информации в локальных вычислительных сетях, построенных на базе оборудования фирмы CISCO

19. Разработка специализированных мероприятий по защите IP-телефонии в компании

20. Разработка алгоритмов принятия решений по управлению информационной безопасностью

21. Исследование методов защиты конфиденциальной информации в системах интернет-банкинга

22. Сравнительный анализ современных антивирусных пакетов.

23. Сравнительный анализ межсетевых экранов.

24. Сравнение анализаторов безопасности автоматизированных систем.

25. Сравнительный анализ средств защиты электронной почты.

26. Анализ методов перехвата паролей пользователей автоматизированных систем и методов противодействия им.

27. Анализ методов гарантированного удаления конфиденциальной информации на электронных носителях.

28. Оценка защиты локальной вычислительной сети организации с внешним доступом в сеть Интернет.

29. Оценка защиты локальной вычислительной сети организации без доступа к внешним сетям.

30. Оценка безопасности информационного портала в образовательной среде.

31. Оценка безопасности автоматизированной системы при работе с облачными продуктами.

32. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.

33. Виды информации и основные методы её защиты.

34. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.

35. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.

36. Источники угроз информационной безопасности Российской Федерации.

37. Анализ информационной инфраструктуры государства.

38. Формальная постановка и решение задачи обеспечения информационной безопасности компьютерных систем.

39. Информационное оружие, его классификация и возможности.

40. Методы нарушения конфиденциальности, целостности и доступности информации.

41. Причины, виды, каналы утечки и искажения информации

42. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

43. Методы и средства обеспечения информационной безопасности объектов информационной сферы государства.

44. Анализ современных подходов к построению систем защиты информации.

45. Критерии оценки защищённости компьютерных систем, методы и средства обеспечения их информационной безопасности.

46. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.

47. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства.

48. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности.

49. Проблемы региональной информационной безопасности.

50. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности в БД

51. Защита различных видов информации в Интернете

52. Защита авторских прав в Интернете

53. Защита информации от несанкционированного доступа методом криптопреобразования

54. Защита конфиденциальной информации при проведении переговоров и совещаний

55. Международный опыт защиты информации и БД.

56. Развитие материально-технической базы защиты информации в БД

4 Методические материалы, определяющие процедуры оценивания уровней освоения компетенций у обучающихся в процессе обучения

В качестве условных уровней сформированности компетентности обучающихся по программам высшего образования выделяются следующие:

1. Допороговый уровень

2. Пороговый уровень

3. Базовый уровень

4. Продвинутый уровень

Общий бюджет оценки уровня сформированности по одной компетенции по дисциплине составляет 100 баллов.

Таблица 1 – Соответствие уровней освоения компетенций оценкам освоения

Уровень освоения компетенций	Кол-во баллов	Оценка уровня подготовки	Вербальный аналог
Допороговый уровень	От 0 до 59 баллов	2	Неудовлетворительно
Пороговый уровень	От 60 до 75 баллов	3	Удовлетворительно
Базовый уровень	От 76 до 85 баллов	4	Хорошо
Продвинутый уровень	От 86 до 100 баллов	5	Отлично

Результаты освоения компетенции при текущем контроле успеваемости определяются по балльно-рейтинговой системе.

Таблица 2 – Шкала оценок при текущем контроле успеваемости по балльно-рейтинговой системе:

Показатели оценивания компетенции дисциплины (модуля), практики:	***Шкала***
1. Посещение учебный занятий:	100% – 20 б 70% – 15 б Ниже – 0 б
2. Выполнение практических заданий 5. Участие в процессе учебного занятия: - доклад - сообщения - эссе - презентация	«5» – 5 б «4» – 4 б «3» – 3 б
6. Выполнение индивидуальных заданий: - контрольная работа - отчет по практике и его защита - реферат - освоение дополнительной квалификации с получением документа	«5» – 30 б «4» – 20 б «3» – 10 б «5» − 40 б «4» – 30 б. «3» - 20 б. 30 − б
7.Активность обучающегося при изучении дисциплины - участие в конкурсах, конференциях по дисциплине - участие в выставках - участие в олимпиадах по дисциплине	 20 б – «5» 10 – «4» 5б – «4»

При выставлении итогового балла учитываются результаты освоения каждой компетенции. Итоговый балл рассчитывается как среднее арифметическое значение. Оценка выставляется в соответствии с таблицей 1.

Итоговый текущий контроль успеваемости оценивается по 5-балльной шкале:

«отлично» − обучающийся приобрел знания, умения и владеет компетенциями в полном объеме, закрепленном рабочей программой дисциплины); 100% заданий, подлежащих текущему контролю, выполнено самостоятельно; обучающийся проявляет умение обобщать, систематизировать и научно классифицировать материал, анализировать показатели с подробными пояснениями и аргументированными выводами;

«хорошо» − обучающийся приобрел знания, умения; все компетенции, закрепленные рабочей программой дисциплины, сформированы полностью или не более 50% компетенций сформированы частично; обучающимся выполнено 75% заданий, подлежащих текущему контролю, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала; проявил умение обобщать, систематизировать и научно классифицировать материал; задания выполнены по стандартной методике без ошибок; сделаны выводы по анализу показателей, но даны недостаточно полные пояснения;

«удовлетворительно» − обучающийся приобрел знания, умения; более 50% компетенций, закрепленных рабочей программой дисциплины, сформированы частично; не менее 50% задания, подлежащего текущему контролю, выполнено по стандартной методике без существенных ошибок; сделаны выводы по анализу показателей, но даны недостаточно полные пояснения;

«неудовлетворительно» − обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; задания не выполнены, или выполнены менее чем на 50% с грубыми ошибками.

Соответствие критериев оценивания уровню освоения компетенций по итоговому текущему контролю успеваемости:

Оценка	Уровень освоения компетенции	Показатель
«3» - удовлетворительно	Пороговый Уровень	обучающийся приобрел знания, умения; более 50% компетенций, закрепленных рабочей программой дисциплины, сформированы частично; не менее 50% задания, подлежащего текущему контролю, выполнено

		по стандартной методике без существенных ошибок; сделаны выводы по анализу показателей, но даны недостаточно полные пояснения.
«4» - хорошо	Базовый уровень	обучающийся приобрел знания, умения; все компетенции, закрепленные рабочей программой дисциплины, сформированы полностью или не более 50% компетенций сформированы частично; обучающимся выполнено 75% задания, подлежащих текущему контролю, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала; проявил умение обобщать, систематизировать и научно классифицировать материал; задания выполнены по стандартной методике без ошибок; сделаны выводы по анализу показателей, но даны недостаточно полные пояснения.
«5» - отлично	Продвинутый уровень	обучающийся приобрел знания, умения и владеет компетенциями в полном объеме, закрепленном рабочей программой дисциплины; 100% задания, подлежащего текущему контролю, выполнено самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать и научно классифицировать материал, анализировать показатели с подробными пояснениями и аргументированными выводами.

Обучающийся, получивший от 60 до 75 баллов за семестр по дисциплине, получает оценку «удовлетворительно» или «зачтено», от 76 до 85 баллов получает оценку «хорошо», от 86 до 100 баллов получает оценку «отлично». При отказе от получения оценки «удовлетворительно», «хорошо» по итогам семестра обучающийся должен проходить промежуточную аттестацию, причем баллы, заработанные в процессе текущего контроля успеваемости в ходе промежуточной аттестации не учитываются.

Если обучающийся не набрал необходимое количество баллов при текущем контроле успеваемости, то преподаватель на свое усмотрение может начислить бонусные баллы за участие в олимпиадах по данной дисциплине или смежной с ней и в профессиональных конкурсах.

Шкала оценок по промежуточной аттестации по балльно-рейтинговой системе

Наименование формы промежуточной аттестации	*Шкала (критерии и показатель оценки)*
Зачет с оценкой	*«3» − 70 баллов «4» − 85 баллов «5» − 100 баллов*

«отлично» *− обучающийся приобрел знания, умения и владеет компетенциями в полном объеме, закрепленном рабочей программой дисциплины; все задания выполнены обучающимся полностью и самостоятельно; представлены позиции разных авторов, их анализ и оценка; терминологический аппарат использован правильно, аргументировано; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать и научно классифицировать материал; знает основные операции, приемы и методы решения задач; осознанно владеет всей структурой процесса решения задачи.*

Ответы экзаменующегося на вопросы экзаменационного билета и дополнительные вопросы полные, обстоятельные, аргументированные. Высказываемые положения подтверждены конкретными примерами; практические задания выполнены по стандартной или самостоятельно разработанной методике в полном объеме: без ошибок в расчетах, с подробными пояснениями по ходу решения, сделаны полные аргументированные выводы.

«хорошо» *− обучающийся приобрел знания, умения; все компетенции, закрепленные рабочей программой дисциплины, сформированы полностью или не более 50% компетенций сформированы частично; обучающийся ответил на все вопросы задания, точно дал определения и понятия. Затрудняется подтвердить теоретически положения практическими примерами. Практические задания выполнены по стандартной методике без ошибок в расчетах. Даны недостаточно полные пояснения, сделаны выводы по анализу показателей. Обучающимся выполнено 75% заданий или при выполнении 100% заданий допущены незначительные ошибки; обучающийся показал хорошие*

знания по предмету и владение навыками систематизации материала; ответы полные, обстоятельные, но неподтвержденные примерами.

«удовлетворительно» *− обучающийся приобрел знания, умения; более 50% компетенций, закрепленных рабочей программой дисциплины, сформированы частично; обучающимся выполнено от 50% до 75% заданий, допущены ошибки в расчетах или аргументации ответов; показал удовлетворительные знания по предмету; знает основные операции, приемы и методы, из которых складывается процесс решения задачи, умеет производить разрозненные операции этого процесса. Обучающийся правильно ответил на все вопросы, но с недостаточно полной аргументацией и не решил в билете практическое задание, или выполнил не менее 50% практических заданий.*

«неудовлетворительно» *− обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на теоретические вопросы; не справился с заданием или выполнено менее 50% заданий.*

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации:

Оценка	Уровень освоения компетенции	Показатель
«3» - удовлетворительно	Пороговый Уровень	обучающийся приобрел знания, умения; более 50% компетенций, закрепленных рабочей программой дисциплины (практики), сформированы частично; обучающимся выполнено от 50% до 75% заданий, допущены ошибки в расчетах или аргументации ответов; показал удовлетворительные знания по предмету; знает основные операции, приемы и методы, из которых складывается процесс решения задачи, умеет производить разрозненные операции этого процесса. Обучающийся правильно ответил на все вопросы, но с недостаточно полной аргументацией и не решил в билете практическое задание, или выполнил не менее 50% практических заданий.
«4» - хорошо	Базовый уровень	обучающийся приобрел знания, умения; все компетенции, закрепленные рабочей программой дисциплины (практики), сформированы полностью или не более 50% компетенций сформированы частично; обучающийся ответил на все вопросы задания, точно

		дал определения и понятия. Затрудняется подтвердить теоретически положения практическими примерами. Практические задания выполнены по стандартной методике без ошибок в расчетах. Даны недостаточно полные пояснения, сделаны выводы по анализу показателей. Обучающимся выполнено 75% заданий или при выполнении 100% заданий допущены незначительные ошибки; обучающийся показал хорошие знания по предмету и владение навыками систематизации материала; ответы полные, обстоятельные, но неподтвержденные примерами.
«5» - отлично	Продвинутый уровень	обучающийся приобрел знания, умения и владеет компетенциями в полном объеме, закрепленном рабочей программой дисциплины (практики); все задания выполнены обучающимся полностью и самостоятельно; представлены позиции разных авторов, их анализ и оценка; терминологический аппарат использован правильно, аргументировано; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать и научно классифицировать материал; знает основные операции, приемы и методы решения задач; осознанно владеет всей структурой процесса решения задачи. Ответы экзаменующегося на вопросы экзаменационного билета и дополнительные вопросы полные, обстоятельные, аргументированные. Высказываемые положения подтверждены конкретными примерами; практические задания выполнены по стандартной или самостоятельно разработанной методике в полном объеме: без ошибок в расчетах, с подробными пояснениями по ходу решения, сделаны полные аргументированные выводы.

Требования к реферату и критерии оценивания

Реферат отличает особая логичность подачи материала и изъяснения мысли, объективность изложения материала. Как правило, реферат отражает различные точки зрения на исследуемый вопрос, выражая в то же время и мнение самого автора.

Реферат имеет определённую композицию:

1. Введение. Во вступлении обосновывается выбор темы, могут быть даны исходные данные реферируемого текста;

2. Основная часть. Содержание реферируемого текста, приводятся и аргументируются основные тезисы;

3. Вывод. Заключение. Делается общий вывод по проблеме, заявленной в реферате.

Реферат имеет следующие признаки:

- содержание реферата полностью зависит от выбранной темы;
- содержит точное изложение основной информации без искажений и субъективных оценок.

Ниже приведены критерии выставления оценок по реферату и эссе.

Выполнение и защита реферата оценивается по пятибалльной системе:

Оценка **«отлично»** ставится, если:

Содержание работы:

– полностью соответствует теме;

– представлены позиции разных авторов, их анализ и оценка;

– терминологический аппарат использован правильно, аргументировано;

– используются новые источники, законодательные акты, эмпирические материалы;

– обучающийся показывает глубокую общетеоретическую подготовку;

– демонстрирует умение работать с различными видами источников;

– проявляет умение обобщать, систематизировать и научно классифицировать материал, являющийся предметом исследования.

Защита реферата

– обучающийся в устном выступлении на защите адекватно представляет результаты исследования;

– владеет понятийным аппаратом;

– владеет научным стилем изложения;

– аргументировано отвечает на вопросы и участвует в дискуссии.

Оценка **«хорошо»** ставится, если:

Содержание реферата:

– обучающийся показал хорошие знания по предмету и владеет навыками систематизации материала;

– обучающийся не в полном объеме изучил историю вопроса;

– допустил 1-2 ошибки в теории (аргументации);

– был некорректен в использовании терминологии.

Защита реферата:

– обучающийся не вполне адекватно представил результаты работы в устном выступлении на защите, но при этом обнаружил хорошие знания по дисциплине и владение навыками систематизации материала.

Оценка **«удовлетворительно»** ставится, если*:*

Содержание реферата

– обучающийся обнаружил удовлетворительные знания по предмету;

– имеются замечания по трем−четырем параметрам реферата, указанным в общих требованиях;

Защита реферата:

– в устном выступлении на защите обучающийся поверхностно представляет результаты исследования;

– отступает от научного стиля изложения;

– затрудняется в аргументации, отвечая на вопросы по теме работы.

Оценка **«неудовлетворительно»** ставится, если:

– установлен факт плагиата;

– имеются принципиальные замечания по реферату;

– обучающийся допустил грубые теоретические ошибки.

Билет № 1
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Компьютерные вирусы. Классификация. Виды и характеристики.
2. Методы и системы защиты информации в АСОД. Целостность и конфиденциальность информации.

Билет № 2
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Способы заражения программ компьютерными вирусами. Схема функционирования загрузочного вируса.
2. Защита информации от утечки по электромагнитным и материально-вещественным каналам.

Билет № 3
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Цели, функции и задачи защиты информации в сетях ЭВМ. Виды угроз.
2. Средства борьбы с вирусами и вредоносными закладками: юридические, организационно-административные, аппаратные и программные. Основные функции и мероприятия по защите.

Билет № 4
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Основные угрозы безопасности России. Информационная безопасность. Определение. Аспекты информационной безопасности. Направления обеспечения ИБ
2. Преднамеренные угрозы безопасности АСОД. Атаки. Классификация угроз безопасности.

Билет № 5
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Жизненно важные интересы и угрозы в информационной сфере. Уровни угроз ИБ и их классификация.
2. Технические средства защиты. Классификация технических средств. Функции защиты и степень сложности устройства.

Билет № 6
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Защита информации. Определение. Формы и способы защиты. Политика безопасности и гарантированности.
2. Защита информации от копирования. Основные функции систем защиты программ от копирования.

Билет № 7
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Основные предметные направления защиты информации. Правовые основы защиты информации. Структура законодательства России в области защиты информации.
2. Биометрические системы идентификации. Основные методы. Охранные системы.

Билет № 8
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Предмет и объекты защиты информации в автоматизированных системах обработки информации (АСОД). Надежность информации. Уязвимость информации.
2. Механические системы защиты. Системы оповещения. Системы опознавания. Оборонительные системы. Охранное освещение.

Билет № 9
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Элементы и объекты защиты в АСОД. Основные элементы АСОД и типовые структурные компоненты.
2. Компьютерные вирусы. Классификация. Виды и характеристики.

Билет № 10
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Дестабилизирующие факторы АСОД. Причины нарушения целостности информации. Каналы несанкционированного получения информации в АСОД.
2. Цели, функции и задачи защиты информации в сетях ЭВМ. Виды угроз.

Билет № 11
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Функции и задачи защиты информации в АСОД. Механизм защиты.
2. Защита от несанкционированного доступа к персональным компьютерам. Защита в среде MS DOS. Защита в средах Windows.

Билет № 12
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Методы и системы защиты информации в АСОД. Целостность и конфиденциальность информации.
2. Физические средства защиты. Средства контроля доступа. Автоматизированные системы контроля доступа.

Билет № 13
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Аутентификация и идентификация. Подтверждение подлинности пользователей и разграничение их доступа к компьютерным ресурсам. Контроль доступа к аппаратуре.
2. Компьютерные вирусы. Классификация. Виды и характеристики.

Билет № 14
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Процедура опознавания с использование простого пароля. Методы проверки подлинности на основе динамически изменяющегося пароля.
2. Способы заражения программ компьютерными вирусами. Схема функционирования загрузочного вируса.

Билет № 15
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Методы идентификации и установления подлинности субъектов и различных объектов. Функциональные методы.
2. Цели, функции и задачи защиты информации в сетях ЭВМ. Виды угроз.

Билет № 16
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Контроль информационной целостности. Организация контроля. Способы модификаций информации.
2. Основные угрозы безопасности России. Информационная безопасность. Определение. Аспекты информационной безопасности. Направления обеспечения ИБ

Билет № 17
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Защита информации от утечки по техническим каналам. Определения, понятия и виды каналов утечки.
2. Жизненно важные интересы и угрозы в информационной сфере. Уровни угроз ИБ и их классификация.

Билет № 18
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Способы заражения программ компьютерными вирусами. Схема функционирования загрузочного вируса.
2. Защита информации. Определение. Формы и способы защиты. Политика безопасности и гарантированности.

Билет № 19
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Основные предметные направления защиты информации. Правовые основы защиты информации. Структура законодательства России в области защиты информации.
2. Регистрация обращений к защищаемой информации. Подсистема управления доступом. Подсистема регистрации и учета. Криптографическая система.

Билет № 20
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Предмет и объекты защиты информации в автоматизированных системах обработки информации (АСОД). Надежность информации. Уязвимость информации.
2. Защита информации от утечки по визуально-оптическим и акустическим каналам.

Билет № 21
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Функции и задачи защиты информации в АСОД. Механизм защиты.
2. Защита от несанкционированного доступа к персональным компьютерам. Защита в среде MS DOS. Защита в средах Windows.

Билет № 22
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Методы и системы защиты информации в АСОД. Целостность и конфиденциальность информации.
2. Физические средства защиты. Средства контроля доступа. Автоматизированные системы контроля доступа.

Билет № 23
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Аутентификация и идентификация. Подтверждение подлинности пользователей и разграничение их доступа к компьютерным ресурсам. Контроль доступа к аппаратуре.
2. Компьютерные вирусы. Классификация. Виды и характеристики.

Билет № 24
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Процедура опознавания с использование простого пароля. Методы проверки подлинности на основе динамически изменяющегося пароля.
2. Способы заражения программ компьютерными вирусами. Схема функционирования загрузочного вируса.

Билет № 25
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Методы идентификации и установления подлинности субъектов и различных объектов. Функциональные методы.
2. Цели, функции и задачи защиты информации в сетях ЭВМ. Виды угроз.

Билет № 26
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Контроль информационной целостности. Организация контроля. Способы модификаций информации.
2. Основные угрозы безопасности России. Информационная безопасность. Определение. Аспекты информационной безопасности. Направления обеспечения ИБ

Билет № 27
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Защита информации от утечки по техническим каналам. Определения, понятия и виды каналов утечки.
2. Жизненно важные интересы и угрозы в информационной сфере. Уровни угроз ИБ и их классификация.

Билет № 28
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Способы заражения программ компьютерными вирусами. Схема функционирования загрузочного вируса.
2. Защита информации. Определение. Формы и способы защиты. Политика безопасности и гарантированности.

Билет № 29
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Основные предметные направления защиты информации. Правовые основы защиты информации. Структура законодательства России в области защиты информации.
2. Регистрация обращений к защищаемой информации. Подсистема управления доступом. Подсистема регистрации и учета. Криптографическая система.

Билет № 30
Наименование дисциплины: Информационная безопасность
Направление: 38.05.01 Экономическая безопасность

1. Предмет и объекты защиты информации в автоматизированных системах обработки информации (АСОД). Надежность информации. Уязвимость информации.
2. Защита информации от утечки по визуально-оптическим и акустическим каналам.