МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОГО БИЗНЕСА

Направление подготовки (специальность)
09.04.03 Прикладная информатика

Направленность (профиль/специализация) программы
Прикладная информатика в экономике

Уровень высшего образования - магистратура

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Бизнес-информатики и информационных технологий
Курс	2
Семестр	3

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО - магистратура по направлению подготовки 09.04.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 916)

Рабочая программа рассмотрена и одобрена на заседании кафедры Бизнес-информатики и информационных технологий
11.02.2020, протокол № 6

Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
доцент кафедры БИиИТ, канд. пед. наук _____ Е.В. Чернова

Рецензент:
Генеральный директор ООО «Корпоративные системы Плюс» , _____ Ю.А. Чудинова

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Г.Н. Чусавитина

1 Цели освоения дисциплины (модуля)

Целью изучения дисциплины «Информационная безопасность цифрового бизнеса»: овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты информации ограниченного доступа от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения в условиях цифровой экономики России

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Информационная безопасность цифрового бизнеса входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Методология и практика консалтинга в сфере ИКТ

Архитектура предприятий и информационных систем

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Выполнение и защита выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

Производственная-преддипломная практика

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Информационная безопасность цифрового бизнеса» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-2 Способен формировать стратегию информатизации прикладных процессов и создания прикладных ИС в соответствии со стратегией развития предприятий	
ПК-2.1:	Осуществляет ИТ-аудит
ПК-2.2	Разрабатывает ИТ-стратегию в соответствии со стратегией развития предприятия, выбирает оптимальные решения в вопросах совершенствования ИТ-инфраструктуры и архитектуры предприятия
ПК-2.3:	Разрабатывает проектную документацию, проводит обучение пользователей, осуществляет ИТ-консалтинг

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 37 акад. часов:

– аудиторная – 36 акад. часов;

– внеаудиторная – 1 акад. часов

– самостоятельная работа – 107 акад. часов;

Форма аттестации - зачет с оценкой

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Информационная безопасность цифрового бизнеса: нормативно-правовые основы								
1.1 Понятия ИБ цифрового бизнеса. Основные понятия. Значение информационной безопасности для субъектов информационных отношений. Понятие и сущность защиты информации. Цели и концептуальные основы защиты информации. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой информации	3	4			8	Самостоятельное изучение учебной и научной литературы Работа с электронными библиотеками	Тестирование	ПК 2.1 ПК 2.2

1.2 Стандарты и спецификации в области информационной безопасности Международные и национальные стандарты и спецификации в области ИБ. Федеральные критерии безопасности информационных технологий. Профиль защиты. Назначение, структура и этапы разработки профиля защиты. Ядро безопасности. Современные стандарты в области управления рисками информационной безопасности		2			8	Самостоятельное изучение учебной и научной литературы Работа с электронными библиотеками	Тестирование	ПК 2.1
1.3 Стандарты и критерии проведения аудита информационной безопасности Стандарты в области управления информационной безопасностью. ISO 27005 (BS 7799 – 3:2006): Управление рисками информационной безопасности. Другие стандарты и критерии аудита		2			8	Самостоятельное изучение учебной и научной литературы Работа с электронными библиотеками	Тестирование	ПК 2.1 ПК 2.2
Итого по разделу		8			24			
2. Аудит информационной безопасности цифрового бизнеса								
2.1 Основные этапы и методы работ по проведению аудита безопасности Этапы проведения аудита. Стадии аудита: планирование; моделирование; тестирование; анализ; разработка предложений; документирование. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника («взлом» защиты информации)	3	4	2		18	Самостоятельное изучение учебной и научной литературы Работа с электронными библиотеками Разработка проекта (индивидуальная) Выполнение заданий практической работы	Тестирование ПР 1 «Разработка принципов и форм аудита ИБ предприятия (объект магистерской работы)»	ПК 2.1 ПК 2.3

2.2 Сбор исходной информации для проведения аудита. Цель сбора исходных данных. Методы сбора исходных данных. Общие исходные данные. Исходные данные об обрабатываемой информации. Исходные данные о системе обеспечения безопасности информации. Исходные данные о персонале. Сбор дополнительных исходных данных. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности. Мониторинг событий безопасности		4	14		40	Самостоятельное изучение учебной и научной литературы Работа с электронными библиотеками Разработка проекта (индивидуальная) Выполнение заданий практической работы	ПР 2 «Анализ и инвентаризация ресурсов ИТ-инфраструктуры предприятия» ПР 3 «Внутренний аудит безопасности ИТ-инфраструктуры пред-приятия» ПР 4 «Разработка процесса обучения пользователей навыкам обеспечения информационной безопасности цифрового бизнеса» ПР 5 «Постановка задачи инструментальных проверок» ПР 6 «Использование сканера безопасности» ПР 7 «Построение карты сети» ПР 8 «Анализ защищенности веб-серверов» ПР 9 «Сканирование портов и идентификация ОС»	ПК 2.1 ПК 2.2 ПК 2.3
2.3 Управление аудитом информационной безопасности ИТ-инфраструктуры предприятия Планирование программы аудита ИБ. Реализация и поддержка программы аудита ИБ. Контроль и совершенствование программы аудита ИБ цифрового бизнеса		2	2		25	Самостоятельное изучение учебной и научной литературы Работа с электронными библиотеками Разработка проекта (индивидуальная) Выполнение заданий практической работы	ПР 9 «Планирование программы аудита безопасности (объект магистерской работы) и процесса обучения пользователей навыкам обеспечения информационной безопасности цифрового бизнеса»	ПК 2.1 ПК 2.2 ПК 2.3
Итого по разделу		10	18		83			
Итого за семестр		18	18		107		зао	
Итого по дисциплине		18	18		107		зачет с оценкой	

5 Образовательные технологии

Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы студентов, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию.

В ходе проведения всех самостоятельных занятий предусматривается использование средств вычислительной техники при выполнении индивидуальных заданий. Текущий, промежуточный и рубежный контроль проводится с помощью образовательного портала.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР: ИНФРА-М, 2019. – 400 с. – (Высшее образование). – DOI: https://doi.org/10.12737/1759-3 – Текст : электронный. – URL: https://znanium.com/read?id=339378

2. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. – Москва : ИНФРА-М, 2019.– 223 с. – (Высшее образование: Бакалавриат). – www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. – Текст : электронный. – URL: https://znanium.com/read?id=342244

б) Дополнительная литература:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-467356

2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2020. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — https://urait.ru/viewer/prestupleniya-v-sfere-informacionnoy-bezopasnosti-448295

в) Методические указания:

Методические рекомендации по дисциплине представлены в приложении 3

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Учебные аудитории для проведения занятий лекционного типа: специализированная (учебная) мебель (столы, стулья, доска аудиторная), мультимедийное оборудование (проектор, компьютер, экран) для презентации учебного материала по дисциплине;

Учебные аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: специализированная (учебная) мебель (столы, стулья, доска аудиторная), персональные компьютеры объединенные в локальные сети с выходом в Internet и с доступом в электронную информационно-образовательную среду университета, оснащенные современными программно-методическими комплексами

Аудитории для самостоятельной работы (компьютерные классы; читальные залы библиотеки): специализированная (учебная) мебель (столы, стулья, доска аудиторная), персональные компьютеры объединенные в локальные сети с выходом в Internet Internet и с доступом в электронную информационно-образовательную среду университета, оснащенные современными программно-методическими комплексами

Помещение для хранения и профилактического обслуживания учебного оборудования: мебель (столы, стулья, стеллажи для хранения учебно-наглядных пособий и учебно-методической документации), персональные компьютеры.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Информационная безопасность цифрового бизнеса» предусмотрена самостоятельная работа магистрантов.

Внеаудиторная самостоятельная работа магистрантов осуществляется в виде изучения учебной и научной литературы по соответствующему разделу с проработкой материала, участие в дистанционном курсе или изучении МООК, предложенном преподавателем и выполнения домашних заданий (подготовка к практическим работам) с консультациями преподавателя.

Самостоятельная работа студентов предполагает решение и оформление согласно заданным требованиям заданий практических работ. Требования к оформлению находятся в СМК-О-СМГТУ-42-09 Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления.

Вопросы для самостоятельного изучения:

1. Основные понятия. Значение информационной безопасности для субъектов информационных отношений.
2. Понятие и сущность защиты информации.
3. Цели и концептуальные основы защиты информации.
4. Критерии, условия и принципы отнесения информации к защищаемой.
5. Носители защищаемой информации.
6. Международные и национальные стандарты и спецификации в области ИБ.
7. Федеральные критерии безопасности информационных технологий.
8. Профиль защиты.
9. Назначение, структура и этапы разработки профиля защиты.
10. Ядро безопасности.
11. Современные стандарты в области управления рисками информационной безопасности.
12. Стандарты в области управления информационной безопасностью.
13. ISO 27005 (BS 7799 – 3:2006): Управление рисками информационной безопасности.
14. Другие стандарты и критерии аудита.
15. Этапы проведения аудита.
16. Стадии аудита: планирование; моделирование; тестирование; анализ; разработка предложений; документирование.
17. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника («взлом» защиты информации).
18. Цель сбора исходных данных.
19. Методы сбора исходных данных.
20. Общие исходные данные.
21. Исходные данные об обрабатываемой информации.
22. Исходные данные о системе обеспечения безопасности информации.
23. Исходные данные о персонале.
24. Сбор дополнительных исходных данных.
25. Обнаружение и устранение уязвимостей.
26. Возможности сканеров безопасности.
27. Мониторинг событий безопасности.
28. Планирование программы аудита ИБ.
29. Реализация и поддержка программы аудита ИБ.
30. Контроль и совершенствование программы аудита ИБ цифрового бизнеса.

Приложение 2

Оценочные средства для проведения промежуточной аттестации
а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-2 – способен формировать стратегию информатизации прикладных процессов и создания прикладных ИС в соответствии со стратегией развития предприятий		
ПК-2.1	Осуществляет ИТ-аудит	Перечень теоретических вопросов 1. Что представляют собой международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности? 2. В чем заключается основная роль стандартов по аудиту информационной безопасности? 3. Раскройте влияние международных стандартов на национальные стандарты и руководства по основам аудита информационной безопасности? 4. Что представляет собой оценивание результатов аудита и самооценки информационной безопасности? 5. Раскройте особенности развития средств и систем автоматизации. 6. Раскройте основные направления обеспечения и оценки информационной безопасности. 7. Что представляет собой аудит информационной безопасности информационных технологий? 8. Что представляет собой комплексный аудит информационной безопасности ИТ? 9. Что представляет собой аудит безопасности внешнего периметра корпоративной сети? 10. Что включает собой обследование внешнего периметра корпоративной сети на предмет защищенности? 11. Что представляет собой аудит безопасности отдельных объектов ИТ-инфраструктуры? 12. Раскройте виды аудита информационной безопасности? 13. Что представляет собой активный аудит? 14. Что представляют собой результаты активного аудита? 15. Что представляет собой экспертный аудит? 16. Что представляет собой аудит на соответствие стандартам? 17. Что представляют собой зарубежные и международные стандарты по аудиту ИБ? 18. Раскройте этапы непосредственного проведения аудита.

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		19. Протоколирование и аудит Примерные варианты тестовых заданий Найдите лишнее, среди путей несанкционированного получения информации: a) хищение носителей информации и производственных отходов b) дистанционное фотографирование c) использование материалов СМИ Практические задания Разработать принципы и формы аудита ИБ предприятия
ПК-2.2	Разрабатывает ИТ-стратегию в соответствии со стратегией развития предприятия, выбирает оптимальные решения в вопросах совершенствования ИТ-инфраструктуры и архитектуры предприятия	Перечень теоретических вопросов 1. Что представляет собой техническая экспертиза продуктов и решений по обеспечению информационной безопасности? 2. Что представляет собой контроль защищенности информации ограниченного доступа? 3. Шифрование 4. Экранирование 5. Классификация межсетевых экранов 6. Анализ защищенности 7. Доступность 8. Отказоустойчивость и зона риска 9. Криптография 10. Вредоносные программы и способы защиты от них 11. Место и роль аппаратно-программных средств защиты. 12. Обнаружение сетевой атаки. 13. Способы обеспечения безопасной работы в Интернет. 14. Принципы функционирования брандмауэров. 15. Перечень информационных ресурсов, подлежащих защите. 16. Основы безопасности web-ресурсов. 17. Способы защиты файлов от постороннего доступа. 18. Вредоносное программное обеспечение. 19. Пути проникновения вредоносного программного обеспечения. 20. Способы защиты от вредоносного программного обеспечения 21. Основные понятия программно-технического уровня информационной безопасности 22. Особенности современных

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		информационных систем, существенные с точки зрения безопасности Примерные варианты тестовых заданий Что необходимо иметь персоналу в случае возникновения нештатной ситуации? a) план обеспечения непрерывности ведения бизнеса и порядок действий в нештатных ситуациях b) инструкция по рестарту системы и восстановительным процедурам, необходимым в случае ее сбоя c) список ответственных лиц и инструкция по связи с ними d) порядок действий в нештатных ситуациях и список лиц и способы связи с ними в нештатных ситуациях Конфиденциальность – это: a) актуальность и непротиворечивость информации, ее защищенность от правонарушителей и несанкционированных изменений b) возможность за разумное время получить требуемую информацию c) защита от несанкционированного доступа к информации Практические задания 1. Провести анализ защищенности веб-серверов. 2. Произвести сканирование портов и идентификацию ОС. 3. Определить задачи инструментальных проверок. 4. Произвести оценку результатов использования сканера безопасности. 5. Построить карту сети.
ПК-2.3	Разрабатывает проектную документацию, проводит обучение пользователей, осуществляет ИТ-консалтинг	Перечень теоретических вопросов 1. Подразделения технической защиты информации. 2. Требования руководящих документов к средствам защиты информации от несанкционированного доступа. 3. Эргономические и нормативные требования к организации рабочего места пользователя 4. Поддержание работоспособности 5. Реагирование на нарушения режима безопасности 6. План обеспечения безопасности

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		Примерные варианты тестовых заданий Политика безопасности: a) Фиксирует правила разграничения доступа b) Отражает подход организации к защите своих информационных активов c) Описывает способы защиты руководства организации Практическое задание Разработать проект обеспечения безопасности цифрового бизнеса по теме индивидуального проекта.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Информационная безопасность цифрового бизнеса» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета с оценкой.

Зачет по данной дисциплине проводится в устной форме по зачетным билетам, каждый из которых включает один теоретический вопрос и одно практическое задание.

Показатели и критерии оценивания зачета с оценкой:

«Отлично» – оценка знаний студента, который свободно владеет:

1) понятийно-терминологической базой дисциплины и знает значение наиболее часто используемых аббревиатур;

2) четко увязывает теоретическое познание дисциплины с реальной практикой;

3) знаком с широким кругом литературных источников, знает, где их достать, хорошо разбирается в истории становления дисциплины, в оценке ее текущего состояния и перспектив ее развития;

4) полностью владеет материалом практического задания, четко и аргументировано защищает ее положительные результаты, обосновано комментирует и объясняет допущенные недочеты.

«Хорошо» – оценка знаний студента, который владеет понятийно-терминологической базой дисциплины, может увязать теоретическое познание дисциплины с реальной практикой. Владеет материалом практической работы, показал способность к объяснению смысла основных положений;

«Удовлетворительно» – оценка знаний студента, который в большей части владеет, с небольшими изъянами, понятийно-терминологической базой дисциплины, имеет представление о внутренней логике дисциплины, представленной в виде учебной программы, Владеет, но неуверенно, материалом практического задания.

«Неудовлетворительно» – оценка знаний студента, который не владеет понятийно-терминологической базой дисциплины и материалом практического задания.

Приложение 3

Методические рекомендации для студентов

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Осваивая курс, магистранту необходимо научиться организовывать самостоятельную внеаудиторную деятельность.

По ходу изучения теоретического материала важно подчеркивать новые термины, устанавливать их взаимосвязь с понятиями, научиться использовать новые понятия в учебной деятельности. Необходимо очень тщательно делать рисунки, графики, схемы, подчеркнуть наиболее важные моменты, составить словарь новых терминов.

В процессе подготовки к занятиям необходимо воспользоваться материалами учебно-методического комплекса дисциплины, материалами, рекомендованными преподавателем и самостоятельно найденными материалами.

Важнейшей особенностью обучения в высшей школе является высокий уровень самостоятельности студентов в ходе образовательного процесса. Эффективность самостоятельной работы зависит от таких факторов как:

- уровень мотивации магистрантов к овладению конкретными знаниями и умениями;
- наличие навыка самостоятельной работы, сформированного на предыдущих этапах обучения;
- наличие четких ориентиров самостоятельной работы.

Приступая к самостоятельной работе, необходимо получить следующую информацию:

- цель изучения конкретного учебного материала;
- место изучаемого материала в системе знаний, необходимых для формирования специалиста;
- перечень знаний и умений, которыми должен овладеть студент;
- порядок изучения учебного материала;
- источники информации;
- форма и способ фиксации результатов выполнения учебных заданий;
- сроки выполнения самостоятельной работы.

Эта информация представлена в учебно-методическом комплексе дисциплины на портале.

При выполнении самостоятельной работы рекомендуется:

- записывать ключевые слова и основные термины,
- составлять словарь основных понятий,
- составлять таблицы, схемы, графики и т.д.
- писать краткие рефераты по изучаемой теме.

Следует выполнять рекомендуемые упражнения и задания.

Результатом самостоятельной работы должна быть систематизация и структурирование учебного материала по изучаемой теме, включение его в уже имеющуюся у студента систему знаний.

После изучения учебного материала необходимо проверить усвоение учебного материала с помощью предлагаемых контрольных вопросов и при необходимости повторить учебный материал.

В процессе подготовки к зачету необходимо систематизировать, запомнить учебный материал, научиться применять его на практике.

Основными способами приобретения знаний, как известно, являются: чтение учебника и дополнительной литературы, рассказ и объяснение преподавателя, поиск ответа на контрольные вопросы.

Приобретение новых знаний требует от учащегося определенных усилий и активной работы на каждом этапе формирования знаний. Знания, приобретенные учащимся в ходе активной самостоятельной работы, являются более глубокими и прочными.

Изучая данную дисциплину, магистрант сталкивается с необходимостью понять и запомнить большой по объему учебный материал. Запомнить его очень важно, так как даже интеллектуальные и операционные умения и навыки для своей реализации требуют определенных теоретических знаний.

Важнейшим условием для успешного формирования прочных знаний является их упорядочивание, приведение их в единую систему. Это осуществляется в ходе выполнения учащимся следующих видов работ по самостоятельному структурированию учебного материала:

- запись ключевых терминов,
- составление словаря терминов,
- составление словаря ГОСТов,

- составление таблиц,
- составление схем,
- составление классификаций,
- выявление причинно-следственных связей,
- составление опорных схем и конспектов.

Информация, организованная в систему, где учебные элементы связаны друг с другом различного рода связями (функциональными, логическими и др.), лучше запоминается.

В качестве контрольных точек по дисциплине предусмотрена защита 10 практических работ на протяжении всего семестра, выполнение прикладного исследования и тест по теоретическому материалу, а также сдача зачета с оценкой в конце семестра. Все практические работы выполняются в предметной области магистерского исследования, либо для организации, предложенной преподавателем.

Практическая работа 1 «Разработка принципов и форм аудита ИБ предприятия (объект магистерской работы)»

Практическая работа 2 «Анализ и инвентаризация ресурсов ИТ-инфраструктуры предприятия»

Практическая работа 3 «Внутренний аудит безопасности ИТ-инфраструктуры предприятия»

Практическая работа 4 «Разработка процесса обучения пользователей навыкам обеспечения информационной безопасности цифрового бизнеса»

Практическая работа 5 «Постановка задачи инструментальных проверок»

Практическая работа 6 «Использование сканера безопасности»

Практическая работа 7 «Построение карты сети»

Практическая работа 8 «Анализ защищенности веб-серверов»

Практическая работа 9 «Сканирование портов и идентификация ОС»

Практическая работа 10 «Планирование программы аудита безопасности (объект магистерской работы) и процесса обучения пользователей навыкам обеспечения информационной безопасности цифрового бизнеса»

Проект обеспечения безопасности цифрового бизнеса (объект магистерской работы)