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
В.Р. Храмшин

10.02.2023 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

# *ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОГО БИЗНЕСА*

Направление подготовки (специальность)
09.04.03 Прикладная информатика

Направленность (профиль/специализация) программы
Прикладная информатика в цифровой 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
2023 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
08.02.2023, протокол № 5

Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа одобрена методической комиссией ИЭиАС
10.02.2023 г. протокол № 7

Председатель _____ В.Р. Храмшин

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

Рецензент:
главный специалист службы бизнес-решений
ЗАО «КОНСОМ СКС», канд. техн. наук _____ В.А. Ошурков

**Лист актуализации рабочей программы**

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 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 2025 - 2026 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:

Управление информационный инфраструктурой предприятия

Управление сервисами ИТ

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 управлять внедрением, использованием и развитием цифровых технологий | |
| ПК-2.1 | Разрабатывает ИТ-стратегию в соответствии со стратегией развития предприятия, выбирает оптимальные решения в вопросах совершенствования ИТ-инфраструктуры и архитектуры предприятия |
| ПК-2.2 | Осуществляет управление ИТ-проектами, организует деятельность по непрерывному улучшению управления ИТ-проектами |
| ПК-2.3 | Осуществляет совершенствование ИТ-сервисов в соответствии со стратегией бизнеса и стратегией организации в области ИТ; моделирует, оценивает и контролирует эффективность ИТ |
| ПК-2.4 | Осуществлять мониторинг и контроль управления информационной безопасностью, н управление непрерывностью ИТ-сервисов |

## 4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 37 акад. часов:

– аудиторная – 36 акад. часов;

– внеаудиторная – 1 акад. часов;

– самостоятельная работа – 71 акад. часов;

– в форме практической подготовки – 0 акад. час;

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-2.4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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-2.4 |
| 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-2.4 |
| 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 | | | 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-2.4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2 Сбор исходной информации для проведения аудита.<br>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 | | 22 | Самостоятельное изучение учебной и научной литературы<br>Работа с электронными библиотеками<br>Разработка проекта (индивидуальная)<br>Выполнение заданий практической работы | ПР 2 «Анализ и инвентаризация ресурсов ИТ-инфраструктуры предприятия»<br>ПР 3 «Внутренний аудит безопасности ИТ-инфраструктуры пред-приятия»<br>ПР 4 «Разработка процесса обучения пользователей навыкам обеспечения информационной безопасности цифрового бизнеса»<br>ПР 5 «Постановка задачи инструментальных проверок»<br>ПР 6 «Использование сканера безопасности»<br>ПР 7 «Построение карты сети»<br>ПР 8 «Анализ защищенности веб-серверов»<br>ПР 9 «Сканирование портов и идентификация ОС» | ПК-2.4 |
| 2.3 Управление аудитом информационной безопасности ИТ-инфраструктуры предприятия<br>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<br>Работа с электронными библиотеками<br>Разработка проекта (индивидуальная)<br>Выполнение заданий практической работы | ПР 9 «Планирование программы аудита безопасности (объект магистерской работы) и процесса обучения пользователей навыкам обеспечения информационной безопасности цифрового бизнеса» | ПК-2.4 |
| Итого по разделу | | 10 | 18 | | 47 | | | |
| Итого за семестр | | 18 | 18 | | 71 | | зао | |
| Итого по дисциплине | | 18 | 18 | | 71 | | зачет с оценкой | |

**5 Образовательные технологии**

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

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://new.znanium.com/catalog/product/1018901

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239

**б) Дополнительная литература:**

1. Илякова, И. Е. Конкурентная разведка : учебное пособие для вузов / И. Е. Илякова, С. Э. Майкова. — 2-е изд. — Москва : Издательство Юрайт, 2023. — 185 с. — (Высшее образование). — ISBN 978-5-534-14708-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520280

2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519079

3. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651

**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 Office 2007 Professional | № 135 от 17.09.2007 | бессрочно |
| 7Zip | свободно | бессрочно |
| MS Office 2003 Professional | № 135 от 17.09.2007 | бессрочно |
| FAR Manager | свободно | бессрочно |

**Профессиональные базы данных и информационные справочные системы**

| Название курса | Ссылка |
|---|---|
| Национальная информационно-аналитическая система – Российский индекс научного | 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 | URL: http://window.edu.ru/ |
| Российская Государственная библиотека. Каталоги | https://www.rsl.ru/ru/4readers/catalogues/ |
| Электронные ресурсы библиотеки МГТУ им. Г.И. Носова | https://magtu.informsystema.ru/Marc.html?locale=ru |
| 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

Персональный компьютер (или ноутбук) с пакетом MS Office с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Мультимедийный проектор, экран.

Мультимедийные презентации к лекциям, учебно-наглядные пособия

Учебные аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Персональные компьютеры с пакетом MSOffice, операционной системой MS Windows 7 или MS Windows 10 и выходом в Интернет

Требуемое ПО, приведенное в таблице «Лицензионное программное обеспечение»

Аудитории для самостоятельной работы: компьютерные классы; читальные залы библиотеки

Персональные компьютеры с пакетом MS Office, операционной системой MS Windows 7, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

Аудитория для хранения и профилактического обслуживания учебного оборудования № 086

Мебель для хранения и обслуживания оборудования (шкафы, столы), учебно-методические материалы, стеллажи для хранения учебно-наглядных пособий и учебно-методической документации

**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 управлять внедрением, использованием и развитием цифровых технологий | | |
| ПК-2.4 | Осуществлять мониторинг и контроль управления информационной безопасностью, н управление непрерывностью ИТ-сервисов | Перечень теоретических вопросов<br>1. Что представляют собой международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности?<br>2. В чем заключается основная роль стандартов по аудиту информационной безопасности?<br>3. Раскройте влияние международных стандартов на национальные стандарты и руководства по основам аудита информационной безопасности?<br>4. Что представляет собой оценивание результатов аудита и самооценки информационной безопасности?<br>5. Раскройте особенности развития средств и систем автоматизации.<br>6. Раскройте основные направления обеспечения и оценки информационной безопасности.<br>7. Что представляет собой аудит информационной безопасности информационных технологий?<br>8. Что представляет собой комплексный аудит информационной безопасности ИТ?<br>9. Что представляет собой аудит безопасности внешнего периметра корпоративной сети?<br>10. Что включает собой обследование внешнего периметра корпоративной сети на предмет защищенности?<br>11. Что представляет собой аудит безопасности отдельных объектов ИТ-инфраструктуры?<br>12. Раскройте виды аудита информационной безопасности?<br>13. Что представляет собой активный аудит?<br>14. Что представляют собой результаты активного аудита?<br>15. Что представляет собой экспертный аудит?<br>16. Что представляет собой аудит на соответствие стандартам?<br>17. Что представляют собой зарубежные и международные стандарты по аудиту ИБ?<br>18. Раскройте этапы непосредственного проведения аудита.<br>19. Протоколирование и аудит |

| Код индикатора | Индикатор достижения компетенции | Оценочные средства |
|---|---|---|
| | | 20. Что представляет собой техническая экспертиза продуктов и решений по обеспечению информационной безопасности?<br>21. Что представляет собой контроль защищенности информации ограниченного доступа?<br>22. Шифрование<br>23. Экранирование<br>24. Классификация межсетевых экранов<br>25. Анализ защищенности<br>26. Доступность<br>27. Отказоустойчивость и зона риска<br>28. Криптография<br>29. Вредоносные программы и способы защиты от них<br>30. Место и роль аппаратно-программных средств защиты.<br>31. Обнаружение сетевой атаки.<br>32. Способы обеспечения безопасной работы в Интернет.<br>33. Принципы функционирования брандмауэров.<br>34. Перечень информационных ресурсов, подлежащих защите.<br>35. Основы безопасности web-ресурсов.<br>36. Способы защиты файлов от постороннего доступа.<br>37. Вредоносное программное обеспечение.<br>38. Пути проникновения вредоносного программного обеспечения.<br>39. Способы защиты от вредоносного программного обеспечения<br>40. Основные понятия программно-технического уровня информационной безопасности<br>41. Особенности современных информационных систем, существенные с точки зрения безопасности<br>42. Подразделения технической защиты информации.<br>43. Требования руководящих документов к средствам защиты информации от несанкционированного доступа.<br>44. Эргономические и нормативные требования к организации рабочего места пользователя<br>45. Поддержание работоспособности<br>46. Реагирование на нарушения режима безопасности<br>47. План обеспечения безопасности |

| Код индикатора | Индикатор достижения компетенции | Оценочные средства |
|---|---|---|
| | | Практические задания<br>1. Провести анализ защищенности веб-серверов.<br>2. Произвести сканирование портов и идентификацию ОС.<br>3. Определить задачи инструментальных проверок.<br>4. Произвести оценку результатов использования сканера безопасности.<br>5. Построить карту сети.<br><br>Комплексное задание<br>1. Разработать принципы и формы аудита ИБ предприятия<br>2. 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)