



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Магнитогорский государственный технический университет им. Г.И. Носова»



**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОГО БИЗНЕСА**

Направление подготовки  
09.04.03 Прикладная информатика

Направленность программы  
Прикладная информатика в экономике

Уровень высшего образования – магистратура

Программа подготовки – академическая магистратура

Форма обучения  
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Бизнес-информатики и информационных технологий
Курс	2
Семестр	3

Магнитогорск  
2019 г.

Рабочая программа составлена на основе ФГОС ВО по направлению подготовки 09.04.03 Прикладная информатика, утвержденного приказом МОиН РФ от № 916 от 19.09.2017.


Рабочая программа рассмотрена и одобрена на заседании кафедры Бизнес информатики и информационных технологий «02» сентября 2019 г., протокол № 1.

Зав. кафедрой  / Г.Н. Чусавитина/


Рабочая программа одобрена методической комиссией института Энергетики и автоматизированных систем «25» сентября 2019 г., протокол № 1.

Председатель  / С.И. Лукьянов /

Рабочая программа составлена: доцентом кафедры БИ и ИТ, кандидатом педагогических наук, доцентом

 Е.В. Черновой

Рецензент: начальник бюро разработки тренажеров металлургии и машиностроения отдела обучающих систем SIKE. Корпоративные системы

 / А.Е. Соченко/

**Лист актуализации рабочей программы**

---

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от 31 августа 2020 г. № 1  
Зав. кафедрой \_\_\_\_\_ *Гусев* Г.Н. Чусавитина

---

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

---

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 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:

Структурный элемент компетенции	Планируемые результаты обучения
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	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	3	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	4		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

<p>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</p>	4	12		42	<p>Самостоятельное изучение учебной и научной литературы Работа с электронными библиотеками Разработка проекта (индивидуальная) Выполнение заданий практической работы</p>	<p>ПР 2 «Анализ и инвентаризация ресурсов ИТ-инфраструктуры предприятия» ПР 3 «Внутренний аудит безопасности ИТ-инфраструктуры предприятия» 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»</p>	<p>ПК 2.1 ПК 2.2 ПК 2.3</p>
<p>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</p>	2	2		23	<p>Самостоятельное изучение учебной и научной литературы Работа с электронными библиотеками Разработка проекта (индивидуальная) Выполнение заданий практической работы</p>	<p>ПР 9 «Планирование программы аудита безопасности (объект магистерской работы) и процесса обучения пользователей навыкам обеспечения информационной безопасности цифрового бизнеса»</p>	<p>ПК 2.1 ПК 2.2 ПК 2.3</p>
Итого по разделу	10	18					
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. Защита 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](http://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]. — URL: <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
FAR Manager	свободно распространяемое ПО	бессрочно
7Zip	свободно распространяемое ПО	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

### Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	<a href="https://elibrary.ru/project_risc.asp">https://elibrary.ru/project_risc.asp</a>
Поисковая система Академия Google (Google Scholar)	<a href="https://scholar.google.ru/">https://scholar.google.ru/</a>
Информационная система - Единое окно доступа к информационным ресурсам	<a href="http://window.edu.ru/">http://window.edu.ru/</a>

### 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 Интернет 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 Интернет 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 MOOK, 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.

**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	<p>Перечень теоретических вопросов</p> <ol style="list-style-type: none"> <li>1. Что представляют собой международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности?</li> <li>2. В чем заключается основная роль стандартов по аудиту информационной безопасности?</li> <li>3. Раскройте влияние международных стандартов на национальные стандарты и руководства по основам аудита информационной безопасности?</li> <li>4. Что представляет собой оценивание результатов аудита и самооценки информационной безопасности?</li> <li>5. Раскройте особенности развития средств и систем автоматизации.</li> <li>6. Раскройте основные направления обеспечения и оценки информационной безопасности.</li> <li>7. Что представляет собой аудит информационной безопасности информационных технологий?</li> <li>8. Что представляет собой комплексный аудит информационной безопасности ИТ?</li> <li>9. Что представляет собой аудит безопасности внешнего периметра корпоративной сети?</li> <li>10. Что включает собой обследование внешнего периметра корпоративной сети на предмет защищенности?</li> <li>11. Что представляет собой аудит безопасности отдельных объектов ИТ-инфраструктуры?</li> <li>12. Раскройте виды аудита информационной безопасности?</li> <li>13. Что представляет собой активный аудит?</li> <li>14. Что представляют собой результаты активного аудита?</li> <li>15. Что представляет собой экспертный аудит?</li> <li>16. Что представляет собой аудит на соответствие стандартам?</li> <li>17. Что представляют собой зарубежные и международные стандарты по аудиту ИБ?</li> <li>18. Раскройте этапы непосредственного проведения аудита.</li> </ol>

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		<p>19. Протоколирование и аудит</p> <p>Примерные варианты тестовых заданий Найдите лишнее, среди путей несанкционированного получения информации:</p> <ol style="list-style-type: none"> <li>a) хищение носителей информации и производственных отходов</li> <li>b) дистанционное фотографирование</li> <li>c) использование материалов СМИ</li> </ol> <p>Практические задания Разработать принципы и формы аудита ИБ предприятия</p>
ПК-2.2	<p>Разрабатывает ИТ-стратегию в соответствии со стратегией развития предприятия, выбирает оптимальные решения в вопросах совершенствования ИТ-инфраструктуры и архитектуры предприятия</p>	<p>Перечень теоретических вопросов</p> <ol style="list-style-type: none"> <li>1. Что представляет собой техническая экспертиза продуктов и решений по обеспечению информационной безопасности?</li> <li>2. Что представляет собой контроль защищенности информации ограниченного доступа?</li> <li>3. Шифрование</li> <li>4. Экранирование</li> <li>5. Классификация межсетевых экранов</li> <li>6. Анализ защищенности</li> <li>7. Доступность</li> <li>8. Отказоустойчивость и зона риска</li> <li>9. Криптография</li> <li>10. Вредоносные программы и способы защиты от них</li> <li>11. Место и роль аппаратно-программных средств защиты.</li> <li>12. Обнаружение сетевой атаки.</li> <li>13. Способы обеспечения безопасной работы в Интернет.</li> <li>14. Принципы функционирования брандмауэров.</li> <li>15. Перечень информационных ресурсов, подлежащих защите.</li> <li>16. Основы безопасности web-ресурсов.</li> <li>17. Способы защиты файлов от постороннего доступа.</li> <li>18. Вредоносное программное обеспечение.</li> <li>19. Пути проникновения вредоносного программного обеспечения.</li> <li>20. Способы защиты от вредоносного программного обеспечения</li> <li>21. Основные понятия программно-технического уровня информационной безопасности</li> <li>22. Особенности современных</li> </ol>

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		<p>информационных систем, существенные с точки зрения безопасности Примерные варианты тестовых заданий</p> <p>Что необходимо иметь персоналу в случае возникновения нештатной ситуации?</p> <p>а) план обеспечения непрерывности ведения бизнеса и порядок действий в нештатных ситуациях б) инструкция по рестарту системы и восстановительным процедурам, необходимым в случае ее сбоя в) список ответственных лиц и инструкция по связи с ними г) порядок действий в нештатных ситуациях и список лиц и способы связи с ними в нештатных ситуациях</p> <p>Конфиденциальность – это:</p> <p>а) актуальность и непротиворечивость информации, ее защищенность от правонарушителей и несанкционированных изменений б) возможность за разумное время получить требуемую информацию в) защита от несанкционированного доступа к информации</p> <p>Практические задания</p> <ol style="list-style-type: none"> <li>1. Провести анализ защищенности веб-серверов.</li> <li>2. Произвести сканирование портов и идентификацию ОС.</li> <li>3. Определить задачи инструментальных проверок.</li> <li>4. Произвести оценку результатов использования сканера безопасности.</li> <li>5. Построить карту сети.</li> </ol>
ПК-2.3	Разрабатывает проектную документацию, проводит обучение пользователей, осуществляет ИТ-консалтинг	<p>Перечень теоретических вопросов</p> <ol style="list-style-type: none"> <li>1. Подразделения технической защиты информации.</li> <li>2. Требования руководящих документов к средствам защиты информации от несанкционированного доступа.</li> <li>3. Эргономические и нормативные требования к организации рабочего места пользователя</li> <li>4. Поддержание работоспособности</li> <li>5. Реагирование на нарушения режима безопасности</li> <li>6. План обеспечения безопасности</li> </ol>

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

**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.

### 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)