автономная некоммерческая образовательная организация
высшего образования
«Региональный финансово-экономический институт»

Кафедра экономики и управления

Утверждаю
Декан экономического факультета
_____ Ю.И. Петренко
«29» мая 2020 г.

Рабочая программа дисциплины

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки **38.03.05 Бизнес-информатика**
Профиль **Информационный бизнес**
Квалификация (степень) **Бакалавр**

Факультет экономический

Заочная форма обучения

Курск 2020

Рецензенты:

Бутова Вера Николаевна, кандидат педагогических наук, доцент кафедры экономики и управления ;

Аксенова Е.С., к.э.н., доцент кафедры экономики и управления.

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки 38.03.05 Бизнес-информатика, утвержденного приказом Министерства образования и науки Российской Федерации от от 11 августа 2016 г. N 1002.

Рабочая программа предназначена для методического обеспечения дисциплины образовательной программы 38.03.05 Бизнес-информатика.

«29» мая 2020 г.

Составитель: _____ Смецкой А.С., ст. преподаватель кафедры экономики и управления

Лист согласования рабочей программы
дисциплины «Информационная безопасность»

Направление подготовки 38.03.05: **Бизнес-информатика**
Профиль: **Информационный бизнес**

Квалификация (степень): **Бакалавр**

Факультет экономический

Заочная форма обучения

2020/2021 учебный год

Рабочая программа утверждена на заседании кафедры экономики и управления, протокол № 8 от «29» мая 2020 г.

Зав. кафедрой _____ С.Л. Аксенов

Составитель: _____ Смецкой А.С.

Согласовано:

Начальник УМУ
_____ О.И. Петренко, «29» мая 2020 г.

Библиотекарь
_____ Т.А. Котельникова, «29» мая 2020 г.

Председатель методической комиссии по профилю
_____ В.Н. Бутова, «29» мая 2020 г.

Изменения в рабочей программе
дисциплины «Информационная безопасность»
на 2021-2022 уч. год

Утверждаю
Декан экономического факультета
_____ Ю.И. Петренко
«25» августа 2021 г.

В рабочую программу вносятся следующие изменения:
1) внесены изменения в список основной литературы.

Рабочая программа утверждена на заседании кафедры экономики и управления, протокол № 1 от «25» августа 2021 г.

Зав. кафедрой _____ С.Л. Аксенов

Согласовано:

Начальник УМУ
_____ О.И. Петренко, «25» августа 2021 г.

Председатель методической комиссии по профилю
_____ В.Н. Бутова, «25» августа 2021 г.

Изменения в рабочей программе
дисциплины «Информационная безопасность»
на 2022-2023 уч. год

Утверждаю
Декан экономического факультета
_____ Ю.И. Петренко
«26» августа 2022 г.

В рабочую программу вносятся следующие изменения:

1) внесены изменения в список дополнительной литературы.

Рабочая программа утверждена на заседании кафедры экономики и управления, протокол № 1 от «26» августа 2022 г.

Зав. кафедрой _____ С.Л. Аксенов

Согласовано:

Начальник УМУ
_____ О.И. Петренко, «26» августа 2022 г.

Председатель методической комиссии по профилю
_____ В.Н. Бутова, «26» августа 2022 г.

Изменения в рабочей программе
дисциплины «Информационная безопасность»
на 2023-2024 уч. год

Утверждаю
Декан экономического факультета
_____ Ю.И. Петренко
«25» августа 2023 г.

В рабочую программу вносятся следующие изменения:

1) внесены изменения в перечень вопросов для самоконтроля по самостоятельно изученным темам.

Рабочая программа утверждена на заседании кафедры экономики и управления, протокол № 1 от «25» августа 2023 г.

Зав. кафедрой _____ С.Л. Аксенов

Согласовано:

Начальник УМУ
_____ О.И. Петренко, «25» августа 2023 г.

Председатель методической комиссии по профилю
_____ В.Н. Бутова, «25» августа 2023 г.

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Цель и задачи изучения дисциплины

Дисциплина включена в базовую часть профессионального цикла ООП.

Дисциплина «Информационная безопасность» базируется на знаниях полученных в процессе освоения школьной программы по предметам: «Математика», «Физика», «Информатика», а также на знаниях полученных студентами в процессе освоения дисциплин базовой части математического и естественнонаучного цикла бакалавриата.

Из дисциплин профессионального цикла «Информационная безопасность» имеет логическую и содержательно-методологическую взаимосвязи с дисциплинами: «Базы данных», «Управление разработкой информационных систем», «Менеджмент», «Электронный бизнес», «Экономика фирмы», «Системы электронного документооборота».

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих общекультурных и профессиональных компетенций:

- готов к ответственному и целеустремленному решению поставленных задач во взаимодействии с обществом, коллективом, партнерами (ОК-7);
- способен находить организационно-управленческие решения и готов нести за них ответственность (ОК-8);
- осознает сущность и значение информации в развитии современного общества; владеет основными методами, способами и средствами получения, хранения, переработки информации (ОК-12);
- использовать соответствующий математический аппарат и инструментальные средства для обработки, анализа и систематизации информации по теме исследования (ПК-20);
- управлять контентом предприятия и Интернет-ресурсов, управлять процессами создания и использования информационных сервисов (контент-сервисов) (ПК-7).

В результате изучения дисциплины обучающийся должен:

- знать основные понятия информационной безопасности(З-1); источники возникновения информационных угроз;(З-2) модели и принципы защиты информации от несанкционированного доступа;(З-3) методы антивирусной защиты информации(З-4); состав и методы организационно-правовой защиты

информации(З-5);

- уметь применять организационные, правовые, технические и программные средства защиты информации(У-1); создавать программные средства защиты информации(У-2);

- владеть навыками определения требований и состава средств, методов и мероприятий по организации комплекса средств защиты информации в компьютерных технологиях;(В-1) навыками практического применения технических, программных и программно-аппаратных средств и методов защиты информации в компьютерных технологиях(В-2).

Соотнесение результатов обучения по дисциплине с планируемыми результатами освоения образовательной программы представлено в таблице, Приложение 1.

3. Место дисциплины в структуре ООП

Дисциплина включена в базовую часть профессионального цикла ООП.

Дисциплина «Информационная безопасность» базируется на знаниях полученных в процессе освоения школьной программы по предметам: «Математика», «Физика», «Информатика», а также на знаниях полученных студентами в процессе освоения дисциплин базовой части математического и естественнонаучного цикла бакалавриата.

Из дисциплин профессионального цикла «Информационная безопасность» имеет логическую и содержательно-методологическую взаимосвязи с дисциплинами: «Базы данных», «Управление разработкой информационных систем», «Менеджмент», «Электронный бизнес», «Экономика фирмы», «Системы электронного документооборота».

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий

Схема распределения учебного времени по видам учебной работы

Общая трудоемкость дисциплины при заочной форме обучения – 2 зачетные единицы (72 академических часа)

Схема распределения учебного времени по семестрам

Виды учебной работы	**Трудоемкость, час**	
4 курс	**Всего:**	
Общая трудоемкость	72	72
Аудиторная работа	6	6
в том числе: лекции практические занятия лабораторные работы	2 2 2	2 2 **2**
Самостоятельная работа	62	62
Курсовая работа	+	+
Промежуточная аттестация	Зачет с оценкой	Зачет с оценкой

Тематический план

№ п/п	**Разделы и темы дисциплины**	**Общая трудоемкость, час**	**В том числе аудиторных**	**Самостоятельная работа**	**Промежуточная аттестация (зачет с оценкой)**
всего	**из них:**				
лекц	**лабор**	**практ**			
1	Средства защиты от несанкционированного доступа	4	1	4	
2	Системы анализа и моделирования информационн	8		6	1

	ых потоков				
3	Системы мониторинга сетей	12	1	6	
4	Антивирусные средства.	6	3	7	
5	Криптографические средства	16	2	18	1
6	Системы аутентификации	6	1	9	
7	Средства предотвращения взлома корпусов и краж оборудования.	4		4	
8	Средства контроля доступа в помещения.	8		6	
9	Инструментальные средства анализа систем защиты	8		4	
	Промежуточная аттестация (экзамен)	4			
	Итого	**72**	**8**	**62**	**4**

Структура и содержание дисциплины

Тема 1. Средства защиты от несанкционированного доступа

Средства авторизации. Мандатное управление доступом. Избирательное управление доступом. Управление доступом на основе ролей. Журналирование.
Литература:
Основная – 1; 5; 9.
Дополнительная – 1; 2, 10, 14.
Интернет-ресурс:
1.Интернет ресурсы из списка: 7, 9, 11
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-7; ОК-8; ПК-20.
Образовательные результаты: З-1; З-2; В-2.

Тема 2. Системы анализа и моделирования информационных потоков .
Системы анализа и моделирования информационных потоков (CASEсистемы). Системы мониторинга. Системы обнаружения и предотвращения вторжений (IDS/IPS). Системы предотвращения утечек конфиденциальной информации (DLP-системы).

Литература:
Основная – 1; 3,4.
Дополнительная – 1; 5; 8;.
Интернет-ресурс:

1.Википедия [Электронный ресурс]: [свобод. Интернет-энцикл.] – Электрон. дан. и прогр. – Режим доступа: http://ru.wikipedia.org, свободный. – Русскояз. часть междунар. проекта «Википедия».

1. Интернет ресурсы из списка: 4, 5, 16, 17, 8, 9.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-12; ПК-7.
Образовательные результаты: З-4; З-5; У-2; В-1.

Тема 3. Системы мониторинга сетей.
Анализаторы протоколов. Межсетевые экраны. Виды систем обнаружения вторжений. Пассивные и активные системы обнаружения вторжений. Сравнение СОВ и межсетевого экрана. История разработок СОВ. Свободно распространяемые СОВ. Коммерческие СОВ.
Литература:
Основная – 3; 4; 6.
Дополнительная – 2; 3;7;8;9.
Интернет-ресурс:
1.Интернет ресурсы из списка: 1,8, 9, 12, 13, 14,15, 16.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с

элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ПК-20; ОК-7; ОК-12.
Образовательные результаты: З-1; З-5; З-3; У-1; В-1.

Тема 4. Антивирусные средства.
Антивирусная программа. Хронология компьютерных вирусов и червей. Целевые платформы антивирусного ПО. Антивирусные продукты для ОС семейства Windows. Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.). Антивирусные продукты для ОС семейства MacOS.

Литература:
Основная – 1; 3, 6,7, 8, 9.
Дополнительная – 1; 6; 9;.
Интернет-ресурс:

1.Интернет ресурсы о из списка: 4, 6, 7, 8, 10, 13.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-7; ОК-8; ПК-20; ПК-7
Образовательные результаты: З-2; З-3; У-1; В-2.

Тема 5. Криптографические средства.
Шифрование; Цифровая подпись. Криптографические атаки. Криптографические хеш-функции. Криптографическое программное обеспечение. Стандарты криптографии
Литература:
Основная – 1; 3,11.
Дополнительная – 1; 2; 3,7;.
Интернет-ресурс:
1.Интернет ресурсы из списка: 4,8, 12, 13, 14,15, 17.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная

лекция, практическое занятие.
Формируемые компетенции: ОК-17; ОК-12; ПК-20
Образовательные результаты: З-1; З-2; З-3; У-1; В-1; В-2.

Тема 6. Системы аутентификации

Идентификация личности. Менеджеры паролей. Одноразовый пароль. Односторонняя функция с потайным входом. Бесконтактная карта Биометрические системы аутентификации.

Литература:
Основная – 3; 4,9.
Дополнительная – 3; 4; 11,17;.
Интернет-ресурс:
1.
2.Интернет ресурсы из списка: 1, 3, 7, 9, 11.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-12; ПК-7
Образовательные результаты: З-1; З-4; У-1; В-1.

Тема 7. Средства предотвращения взлома корпусов и краж оборудования

Кабины и шкафы модульные серверные. Оборудование для депозитариев. Системы противокражные. Средства предотвращения взлома корпусов. Устройства антивандальные. Литература:
Основная – 3; 4.
Дополнительная – 3; 4; 11;.
Интернет-ресурс:
Интернет ресурсы из списка: 1, 3, 7, 9, 11,14,18.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-8; ПК-20; ПК-7
Образовательные результаты: З-2; З-5; У-2; В-1.

Тема 8. Средства контроля доступа в помещения

Преграждающие устройства. Идентификатор. Контроллер. Считыватель. Конверторы среды. Вспомогательное оборудование. Программное обеспечение.

Литература:

Основная – 3; 4,8.
Дополнительная – 3; 4; 11; 13.
Интернет-ресурс
1.Интернет ресурсы из списка: 1, 3, 7, 9, 11.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-7; ОК-8; ОК-12
Образовательные результаты: З-2; З-4; У-1; В-2.

Тема 9. Инструментальные средства анализа систем защиты

Организационная защита объектов информатизации.
Программыкаталогизаторы, или файловые оболочки ОС. Программы поиска файлов и текстовых и двоичных последовательностей в текстовых и двоичных файлах. Программы - мониторы активных задач, процессов, потоков и окон. Программы перехвата и протоколирования клавиатурного ввода (Keyboard Loggers)

Литература:
Основная – 3; 4, 9.
Дополнительная – 3; 4; 11;17.
Интернет-ресурс:
1.Интернет ресурсы из списка: 1, 3, 7, 9, 11.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-8; ПК-20; ПК-7
Образовательные результаты: З-2; З-3; У-1; В-1.

Практические занятия

Практическое занятие №1 «Средства защиты от несанкционированного доступа»

Цель: Ознакомить студента с основными Средства защиты от несанкционированного доступа, формирование общекультурных и профессиональных компетенций.

Вопросы для обсуждения:

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем

Литература:

Основная – 1; 2; 4.

Дополнительная – 1; 5,10.

Интернет-ресурс:

1. Интернет ресурсы из списка: 1, 3, 7, 9, 11,18

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.

Формируемые компетенции: ОК-12; ОК-9.

Образовательные результаты: З-1; З-2; В-1.

Форма контроля: групповая дискуссия, опрос.

Практическое занятие №2 « Системы анализа и моделирования информационных потоков»

Цель: Ознакомить студента с CASE системами, системами обнаружения и предотвращения вторжений (IDS/IPS); формирование общекультурных и профессиональных компетенций.

Вопросы для обсуждения:

1. Пассивные и активные системы обнаружения вторжений
2. Сравнение СОВ и межсетевого экрана
3. Обнаружение аномалий
4. Система предотвращения вторжений(IPS)
5. Защита серверов от несанкционированного доступа
6. Network intrusion detection system (NIDS)

7.Система обнаружения вторжений (IDS)
8.Предотвращение сетевых атак
9.Коммерческая тайна.
10. Правовая защита.
11. Организационная защита.
12. Методы и средства защиты информации от утечки по техническим каналам.

Литература:
Основная – 1; 4.
Дополнительная – 4; 5; 9;10;11;.
Интернет-ресурс:
1.Википедия [Электронный ресурс]: [свобод. Интернет-энцикл.] – Электрон. дан. и прогр. – Режим доступа: http://ru.wikipedia.org, свободный. – Русскояз. часть междунар. проекта «Википедия».
2.Интернет ресурсы из списка: 1, 5, 6, 7, 8, 9, 10, 11, 12, 16.

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-12; ПК-7.
Образовательные результаты: З-4; З-5; У-2; В-1.
Форма контроля: групповая дискуссия, опрос, сравнительный анализ.

Практическое задание №3 «Системы мониторинга сетей.»

Цель: Ознакомить студента с основами мониторинга сетей, протоколами и сетевыми экранами; формирование общекультурных и профессиональных компетенций.

Вопросы для обсуждения:
1.Средства обеспечения информационной безопасности в ОС Windows’2000. Разграничение доступа к данным.
2.Групповая политика.
3.Применение файловой системы NTFS для обеспечения информационной безопасности в Windows NT/2000/XP.
4.Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
5.Применение средств Windows 2000/XP для предотвращения угроз раскрытия конфиденциальности данных.
6.Разграничение доступа к данным в ОС семейства UNIX.
7.Пользователи и группы в ОС UNIX.
8.Пользователи и группы в ОС Windows’2000. Свободные межсетевые экраны
9.Межсетевой экран
10. Персональный файрвол

Литература:
Основная – 2; 3;4.

Дополнительная – 4; 7; 8;.
Интернет-ресурс:
1.Интернет ресурсы из списка: 1, 3, 5,8, 9, 10, 11, 12, 13.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ПК-20; ОК-7; ОК-12.
Образовательные результаты: З-1; З-5; З-3; У-1; В-1.
Форма контроля: групповая дискуссия, опрос.

Практическое занятие №4 «Антивирусные средства»

Цель: предоставление теоретических знаний и практических навыков студенту по работе с антивирусными средствами, формирование общекультурных и профессиональных компетенций.
Вопросы для обсуждения:
. Классификация антивирусных продуктов
. Антивирусные продукты для корпоративных пользователей
. Лжеантивирусы
. Базы антивирусов
. Антивирусные продукты для ОС семейства Windows
. Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.)
. Антивирусные продукты для ОС семейства MacOS
. Антивирусные продукты для мобильных платформ
. Антивирусные продукты для защиты рабочих станций
. Антивирусные продукты для защиты файловых и терминальных серверов
. Антивирусные продукты для защиты почтовых и Интернет-шлюзов
. Антивирусные продукты для защиты серверов виртуализации
Литература:
Основная – 1, 3, 4, 5, 6, 9.
Дополнительная – 1; 2; 3;.9
Интернет-ресурс:
1.Интернет ресурсы о из списка: 1, 3, 7, 8, 11.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-7; ОК-8; ПК-20; ПК-7
Образовательные результаты: З-2; З-3; У-1; В-2.
Форма контроля: групповая дискуссия, опрос, сравнительный анализ.
Практическое занятие №5 «Криптографические средства»
Цель: предоставление теоретических знаний и практических навыков студенту по криптографической защите информации, формирование общекультурных и

профессиональных компетенций.
Вопросы для обсуждения:
1. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах.
2. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
3. Функции и задачи защиты, механизмы защиты,
4. уровень защищенности,
5. управление защитой и другие базовые понятия, используемые при формировании КСЗИ.
6. Общетеоретическая постановка задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.
7. Основные технологические этапы разработки КСЗИ.
8. Средства моделирования, применяемые для оптимизации КСЗИ.
9. Организационно-технические мероприятия, проводимые в процессе эксплуатации КСЗИ.
10. Задачи, решаемые подсистемой аудита в составе защищенных КС.
11. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.

Литература:
Основная – 2; 3.
Дополнительная – 1; 2; 6;.
Интернет-ресурс:
1. Интернет ресурсы из списка: 4,8, 12, 13, 14,15, 17.

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-17; ОК-12; ПК-20
Образовательные результаты: З-1; З-2; З-3; У-1; В-1; В-2.
Форма контроля: групповая дискуссия, опрос, сравнительный анализ.
Практическое занятие №6 «Системы аутентификации »
Цель: предоставление теоретических знаний и практических навыков по работе с языком интегрированных запросов LINQ, формирование общекультурных и профессиональных компетенций.
Вопросы для обсуждения:
1. Современные системы идентификации и аутентификации.
2. Парольные системы.
3. Технология инфраструктуры открытых ключей.
4. Системы одноразовых паролей.
5. Биометрические характеристики.
6. Процедурный уровень обеспечения безопасности.

7.Авторизация пользователей в информационной системе.
8.Идентификация и аутентификация при входе в информационную систему.
9.Использование парольных схем.
10. Недостатки парольных схем.
11. Идентификация и аутентификация пользователей.
12. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
13. Биометрические средства идентификации и аутентификации пользователей.
14. Аутентификация субъектов в распределенных системах, проблемы и решения.
15. Схема Kerberos.

Литература:
Основная – 1; 3.
Дополнительная – 7; 8; 9;10.
Интернет-ресурс:
• Интернет ресурсы из списка: 1, 5, 6,7,9,12,18

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-1; ОК-4; ОК-8; ОК-12; ПК-3; ПК-4; ПК-8; ПК-11.
Образовательные результаты: З-1; З-2; З-3; У-1; В-1.
Форма контроля: групповая дискуссия, опрос, сравнительный анализ, выполнение практических заданий.

Практическое занятие №7 «Средства предотвращения взлома корпусов и краж оборудования.»

Цель: предоставление теоретических знаний и практических навыков по работе с средствами защиты, формирование общекультурных и профессиональных компетенций.
Вопросы для обсуждения:
◦ Правовая охрана программ и баз данных
◦ Защита от несанкционированного доступа к информации
◦ Причины несанкционированного доступа к информации
◦ Последствия несанкционированного доступа к информации
◦ Средства предотвращения взлома корпусов и краж оборудования.
◦ Средства контроля доступа в помещения.

Литература:
Основная – 1; 3.
Дополнительная – 7; 8; 9;10.
Интернет-ресурс:
• Интернет ресурсы из списка: 11-17.

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-8; ПК-20; ПК-7
Образовательные результаты: З-2; З-5; У-2; В-1.
Форма контроля: групповая дискуссия, опрос, сравнительный анализ, выполнение практических заданий.

Практическое занятие №8 «Средства контроля доступа в помещения»

Цель: предоставление теоретических знаний и практических навыков по с средствами контроля доступа в помещение, формирование общекультурных и профессиональных компетенций.
Вопросы для обсуждения:

- Контроль доступа
- Учёт рабочего времени
- Повышение качества охраны
- Контроль автономных объектов, на которых нет постоянно присутствующего охранного и обслуживающего персонала (АТС и энергоузлы)
- Снижение вероятности нанесения материального ущерба путём хищения.
- Документирование и возможность ретроспективы всех событий по входу/выходу в помещения
- Интеграция с текущей IT-инфраструктурой
- Интеграция с уже установленными системами охранной, пожарной сигнализации и видеонаблюдения.
- Исключение несанкционированного доступа к рабочим местам (АРМ).
- Разграниченный контроль для разных групп сотрудников
- Возможность неограниченного масштабирования системы контроля и управления доступом до межрегионального уровня

Литература:
Основная – 1; 3.
Дополнительная – 7; 8; 9;10.
Интернет-ресурс:

- Интернет ресурсы из списка: 1-11, 13

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-12; ПК-7.
Образовательные результаты: З-4; З-5; У-2; В-1.
Форма контроля: групповая дискуссия, опрос, сравнительный анализ, выполнение практических заданий.
Практическое занятие №9 «Инструментальные средства анализа систем защиты

»
Цель: предоставление теоретических знаний и практических навыков по работе с инструментальными средствами анализа систем защиты, формирование общекультурных и профессиональных компетенций.
Вопросы для обсуждения:
1.Программы - мониторы файловой системы
2.Программы - мониторы системных файлов ОС
3.Программы - мониторы вызовов подпрограмм ОС
4.Программы - мониторы обмена данными с системными устройствами
5.Программы - мониторы сетевого обмена данными
6.Программы - мониторы конвейеров данных
7.Программы перехвата и протоколирования клавиатурного ввода
8.Программы копирования областей ОЗУ в ВЗУ
9.Программы восстановления удаленных файлов
10. Программы побайтового копирования гибких магнитных дисков
11. Программы — распаковщики/дешифраторы
12. Средства дизассемблирования объектных модулей ПО
13. Средства декомпиляции объектных модулей ПО
14. Средства отладки объектных модулей
15. Средства поиска и замены текстовых и двоичных последовательностей в текстовых и двоичных файлах

Литература:
Основная – 1; 3.
Дополнительная – 7; 8; 9;10.
Интернет-ресурс:
1.Интернет ресурсы из списка: 1, 4, 5, 7, 11, 12, 14, 17.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-8; ПК-20; ПК-7
Образовательные результаты: З-2; З-3; У-1; В-1.
Форма контроля: групповая дискуссия, опрос, сравнительный анализ, выполнение практических заданий.

Лабораторные работы

Лабораторная работа №1-5 «Создание и проверка подлинности электронной цифровой подписи»

Цель: Ознакомиться со схемами цифровой подписи и получить навыки создания и проверки подлинности ЦП., формирование общекультурных и профессиональных компетенций.

Вопросы для обсуждения:

1. Для чего нужна цифровая подпись?
2. Назовите основные свойства цифровой подписи.
3. Какие схемы цифровой подписи существуют? Какая схема самая распространенная?
4. Как осуществляется подпись RSA? В чем отличие подписи RSA от шифра RSA?
5. Как осуществляется подпись Эль-Гамаля?
6. Как осуществляется проверка на подлинность подписи Эль-Гамаля?

Задание

Реализовать приложение, позволяющие решить задачи в соответствии с вариантом. Все параметры (сообщение, параметры, ключи) должны вводиться пользователем или задавать в файле.

Указание к работе

На протяжении многих веков при ведении деловой переписки, заключении контрактов и оформлении любых других важных бумаг подпись ответственного лица или исполнителя была непременным условием признания его статуса или неоспоримым свидетельством его важности. Подобный акт преследовал две цели:

1. гарантирование истинности письма путем сличения подписи с имеющимся образцом;
2. гарантирование авторства документа (с юридической точки зрения).

Выполнение данных требований основывается на следующих свойствах подписи:

1. подпись аутентична, т.е. с ее помощью получателю документа можно доказать, что она принадлежит подписывающему;
2. подпись служит доказательством, что только тот человек, чей автограф стоит на документе, мог подписать данный документ, и никто другой не смог бы этого сделать;
3. подпись непереносима, т.е. является частью документа и поэтому перенести ее на другой документ невозможно;
4. документ с подписью является неизменяемым, т.е. после подписания его невозможно изменить, оставив данный факт незамеченным;

5. подпись неоспорима, т.е. человек, подписавший документ, в случае признания экспертизой, что именно он засвидетельствовал данный документ, не может оспорить факт подписания;
6. любое лицо, имеющее образец подписи, может удостовериться в том, что данный документ подписан владельцем подписи.

С переходом к безбумажным способам передачи и хранения данных, а также с развитием систем электронного перевода денежных средств, в основе которых – электронный аналог бумажного платежного поручения, проблема виртуального подтверждения аутентичности документа приобрела особую остроту. Развитие любых подобных систем теперь немыслимо без существования электронных подписей под электронными документами. Однако применение и широкое распространение *электронно-цифровых подписей* (ЭЦП) повлекло целый ряд правовых проблем. Так, ЭЦП может применяться на основе договоренностей внутри какой-либо группы пользователей системы передачи данных, и в соответствии с договоренностью внутри данной группы ЭЦП должно иметь юридическую силу. Но будет ли электронная подпись иметь доказательную силу в суде, например, при оспаривании факта передачи платежного поручения?

Схема 1

Данная схема предполагает шифрование электронного документа (ЭД) на основе симметричных алгоритмов и предусматривает наличие в системе третьего лица (арбитра), пользующегося доверием участников обмена подписанными подобным образом электронными документами. Взаимодействие пользователей данной системой производится по следующей схеме (см. рисунок 1)

Участник А зашифровывает сообщение своим секретном ключе K_A, знание которого разделено с арбитром (C на рисунке 1), затем шифрованное сообщение передается арбитру с указанием адресата данного сообщения (информация, идентифицирующая адресата, передается также в зашифрованном виде).

Арбитр расшифровывает полученное сообщение ключом K_A, производит необходимые проверки и затем зашифровывает его секретным ключом участника B (K_B). Далее зашифрованное сообщение посылается участнику B вместе с информацией, что оно пришло от участника A.

Участник B расшифровывает данное сообщение и убеждается в том, что отправителем является участник A.

Авторизацией документа в данной схеме считается сам факт шифрования электронного документа (ЭД) секретным ключом и передача зашифрованного ЭД арбитру. Основным преимуществом этой схемы является наличие третьей стороны, исключающей какие-либо спорные вопросы между участниками информационного обмена, то есть в данном случае не требуется дополнительной системы арбитража ЭЦП. Недостатком схемы является так же наличие третьей стороны и использование симметричных алгоритмов

шифрования. На практике эта схема не получила широкого распространения.

Схема 2

Фактом подписания документа в данной схеме является шифрование документа секретным ключом его отправителя. Здесь используются асимметричные алгоритмы шифрования.

Вторая схема используется довольно редко вследствие того, что длина ЭД может оказаться очень большой (шифрование асимметричным алгоритмом может оказаться неэффективным по времени), но в этом случае в принципе не требуется наличие третьей стороны, хотя она и может выступать в роли сертификационного органа открытых ключей пользователя.

Схема 3

Наиболее распространенная схема ЭЦП использует шифрование окончательного результата обработки ЭД хэш-функцией при помощи асимметричного алгоритма. Структурная схема такого варианта построения ЭЦП представлена на рисунке 3.

Литература:

Основная – 1; 2; 4.

Дополнительная – 1; 2.

Интернет-ресурс:

1. Учебный курс для студентов направления подготовки «Бизнес-информатика» РФЭИ - http://it.rfei.ru/~3b

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.

Формируемые компетенции: ОК-1; ОК-4; ПК-3; ПК-4.

Образовательные результаты: З-1; З-2; В-1.

Форма контроля: групповая дискуссия, опрос.

Лабораторная работа №5-9 «Перехват клавиатурного ввода»

Цель: Поиск и самостоятельное исследование любой программы из класса перехватачиков вводимой информации; формирование общекультурных и профессиональных компетенций.

Вопросы для обсуждения:

1. Существует ли необходимость в использовании данного вида ПО?
2. Предоставляют ли такие программы возможность осуществить незаконное получение ключа регистрации/пароля к ПО
3. Предназначен ли данный тип программных средств для сохранения информации, введенной в ЭВМ с клавиатуры в специальные файлы протокола?
4. Возможна ли фильтрация сохраняемых данных?
5. Возможна ли работа по дополнительно вводимым критериям?

Знания о том, как данное программное обеспечение может быть установлено и использовано смогут сформировать подход к защите от перехвата вводимой информации. Работу можно условно разделить на три части:

1. Исследование программы, работающей локально, например Skylogger.
2. Установка и настройка сетевого кейлогера KeySpider.
3. Поиск и самостоятельное исследование любой программы из класса кейлогеров.

В отчёте указать данные, которые Вы считаете необходимыми для того, чтобы я понял, что работа проделана, исследование выполнено, знания и умения приобретены.

Литература:

Основная – 1;4.

Дополнительная – 5; 8; 11;6.

Интернет-ресурс:

1. Википедия [Электронный ресурс] : [свобод. Интернет-энцикл.] – Электрон. дан. и прогр. – Режим доступа: http://ru.wikipedia.org, свободный. – Русскояз. часть междунар. проекта «Википедия».
2. Учебный курс для студентов направления подготовки «Бизнес-информатика» РФЭИ – .http://it.rfei.ru/~3b
3. Интернет ресурсы о PHP из списка: 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17.

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.

Формируемые компетенции: ОК-1; ОК-4; ПК-3; ПК-4; ПК 15.

Образовательные результаты: З-1; З-2; У-1; В-1.

Форма контроля: групповая дискуссия, опрос, сравнительный анализ, выполнение практических заданий.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа студентов нацелена на углубление практических навыков по способам и средствам обеспечения информационной безопасности.

Вопросы для самостоятельной работы:

1. Основные понятия и определения информационной безопасности. Задачи информационной безопасности.
2. Структуры, обеспечивающие информационную безопасность.
3. Этапы развития информационной безопасности.
4. Нормативно-правовые аспекты информационной безопасности.
5. Виды информационных угроз.
6. Хакерские атаки.
7. Фишинговые атаки.
8. Спам.
9. Вредоносные программы.
10. Компьютерные преступления.
11. Многоуровневая защита информации.
12. Антивирусная защита.
13. Современные системы идентификации и аутентификации.
14. Парольные системы.
15. Технология инфраструктуры открытых ключей.
16. Системы одноразовых паролей.
17. Биометрические характеристики.
18. Криптографическая защита данных.
19. Электронно-цифровая подпись.
20. Коммерческая тайна.
21. Правовая защита.
22. Организационная защита.
23. Методы и средства защиты информации от утечки по техническим каналам.
24. Аттестация информационных объектов.
25. Международная деятельность по обеспечению информационной безопасности. Международное сотрудничество.
26. Виды коммерческих международных операций.
27. Организация работы с зарубежными партнерами.
28. Порядок защиты конфиденциальной информации с зарубежными партнерами.

Литература:

Основная – 1; 3.

Дополнительная – 1; 2; 3;.

Интернет-ресурс:

1.Учебный курс для студентов направления подготовки «Бизнес-информатика»

РФЭИ - http://it.rfei.ru/~3b

Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-7; ОК-12; ПК-20.
Образовательные результаты: З-1; З-2; З-3; У-1; В-1.
Форма контроля: выполнение практических заданий.

Научно-исследовательская работа студентов

Темы: «Криптографическая защита данных»

Цель: формирование у студентов научного мышления, способности верно производить постановку проблемы исследования, самостоятельно осуществлять поиск информации, анализ проблем и формирование адекватных выводов, исходя из масштабов ее деятельности, целей и задач.

Тематика докладов:

1. Электронно-цифровая подпись.
2. Многоуровневая защита информации
3. Антивирусная защита.
4. Технология инфраструктуры открытых ключей.
5. Аттестация информационных объектов.
6. Парольные методы и оценка их эффективности.
7. Шифрование методом замены.
8. Шифрование методом перестановки.
9. Аналитические методы шифрования.
10. Системы шифрования с открытым ключом.
11. Отечественные и зарубежные стандарты шифрования.

Литература:
Основная – 1; 2; 4.
Дополнительная – 1; 2б9.
Интернет-ресурсы: 4; 5; 6;12.
Образовательные технологии, методы и формы обучения: дистанционные образовательные технологии, объяснительно-иллюстративного обучения с элементами проблемного изложения; развивающего обучения, проблемная лекция, практическое занятие.
Формируемые компетенции: ОК-16; ОК-15; ПК-18; ПК-26.
Образовательные результаты: З-1; З-2; В-1.
Форма контроля: групповая дискуссия, опрос.
Форма контроля: подготовка доклада.

Курсовая работа

Задача курсового проекта: использовать полученные знания на практике для обеспечения защиты передаваемой информации в корпоративных сетях, в сети интернет, выявления потенциальных угроз информационной безопасности и анализ методов борьбы с угрозами.

Ваша *задача* в ходе выполнения курсовой работы: описание теоретической базы рассматриваемой темы информационной безопасности и практическая реализация описанного алгоритма, основанная на теории.
Вам следует выбрать наиболее подходящую тему курсовой работы из представленного далее списка тем, а затем раскрыть данную тем. После описания теоретической базы, вас нужно реализовать один из алгоритмов криптографической защиты информации на любом из удобных для вас языков программирования. Курсовая работа присылается в виде файла с описанием теоретической части и листингом программы.

Перечень возможных тем:

1. Программная реализация асимметричных криптографических алгоритмов: Шифрование и расшифрование по алгоритму RSA
Опишите и дайте математическое обоснование алгоритма, а затем реализуйте программно алгоритм шифрования и дешифрования сообщения.
2. Симметричный алгоритм шифрования (DES).
Опишите и дайте математическое обоснование алгоритма, а затем реализуйте используя удобный для вас язык программирования алгоритм шифрования и дешифрования сообщения.
3. Обеспечение защиты информации при передачи по каналам связи
Данная тема предполагает теоретическое описание методов защиты информации в каналах связи и способов создания защищённых телекоммуникационных систем, а так же анализ и рекомендации по выбору наиболее оптимальных способов.
4. Системы криптографической защиты информации с функцией цифровой подписи.
Опишите и дайте математическое обоснование какого-либо выбранного вам алгоритма ЭЦП, а затем реализуйте программно данный алгоритм.
5. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.
Опишите особенности использования цифровой подписи в в электронном документообороте и реализуйте алгоритм ЭЦП для подписи документа.
6. Сетевые атаки
Данная тема предполагает теоретическое описание возможных сетевых атак, анализ способов обнаружения и защиты, а так же рекомендации по наиболее оптимальным методам действий.
7. Механизмы защиты информации в сети 3G

Предполагает подробное описание (математическое обоснование) и анализ одного из способов защиты информации в сетях 3G
8. Свой вариант

Написание курсовой работы

При работе с курсовым проектом Вам потребуется написать теоретическую часть работы, оформленную согласно общим требованиям к оформлению курсовых и дипломных работ, а так же выполнить практическую часть. Выполнение практической части различается в зависимости от выбранной темы. Если вы выберите темы 3, 6 или 7, то Вам необходимо провести сравнительный анализ и привести выводы в практической части вашей работы. Если же вы выбираете темы связанные с реализацией того или иного алгоритма, вам необходимо в практической части работы предоставить листинг программы.

Структура курсовой работы:

- титульный лист;
- оглавление;
- введение;
- теоретическая часть;
- практическая часть;
- заключение.

Оглавление должно быть расположено на 2-й странице. Заголовки оглавления должны точно повторять заголовки в тексте. В оглавление не включают титульный лист.

Во введении опишите и обоснуйте выбранную вами тему, опишите структуру вашего курсового проекта.

В теоретической части подробно опишите и проанализируйте выбранную вами тему. Приведите теоремы и утверждения, дайте кратко математическую базу на которой основывается выбранный вам алгоритм шифрования (если вами выбрана тема по криптографическим алгоритмам), либо (если тема не предполагает работ с алгоритмами шифрования) покажите на примерах и опишите и исследуйте особенности выбранной предметной области.

Практическая часть предполагает реализацию какого-либо криптографического алгоритма, основываясь на математической базе, показанной в теоретической части, с помощью удобного для вас языка программирования. Код должен быть структурирован, элементы кода расставлены в порядке иерархичности. В конце проекта должны быть приведены листинги программы. Для тем предполагающих анализ средств и методов защиты информации, практическая часть должна содержать детальный анализ, рекомендации по выбору наиболее оптимальных способов на примере конкретной предметной области (предприятия, компьютерной сети и т.п.) и выводы.

В заключении сделайте выводы о проделанной работе, представьте список литературы и используемых вами интернет-сервисов, которыми вы пользовались при разработке проекта.

Публикация результатов

Для сдачи курсовой работы Вы должны предоставить для проверки архив в формате *.zip, содержащий файл с курсовой работой, включающей листинг программы и проект с программной реализацией алгоритма (если это требуется по выбранной вами тематике).

Файл курсовой работы должен быть в формате .doc или .docx.

Листинг программы - это основная часть кода, отвечающая за реализацию, собственно требуемого алгоритма. В листинге программы не приводится полностью код проекта. Полный рабочий проект для проверки и тестирования находится отдельно от файла курсовой работы. Листинг находится в заключительной части работы, как правило, в приложении.

Проект представляет собой реализацию одного из алгоритмов криптографической защиты информации. На любом из изученных вами языков программирования, вы можете реализовать полный рабочий алгоритм шифрования и дешифрования сообщения. Полностью рабочий проект вы присылаете в архиве вместе с файлом курсовой работы.

Выгрузка работы в виде архива в формате *.*zip* производится на портал РФЭИ: my.rfei.ru. А затем, Вам следует дать обязательную оценку курсового проекта, написав эссе, в котором необходимо указать, что ваша курсовая работа выгружена на портал РФЭИ для проверки.

Вопросы к зачету

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности.

Основные законодательные акты РФ в области защиты информации.

10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
12. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
13. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
14. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
15. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
16. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
17. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
18. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
19. Биометрические средства идентификации и аутентификации пользователей.
20. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
21. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
22. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
23. Законодательный уровень применения цифровой подписи.
24. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
25. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

26. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
27. Средства обеспечения информационной безопасности в ОС Windows’2000. Разграничение доступа к данным. Групповая политика.
28. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows NT/2000/XP. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
29. Применение средств Windows 2000/XP для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
30. Разграничение доступа к данным в ОС семейства UNIX.
31. Пользователи и группы в ОС UNIX.
32. Пользователи и группы в ОС Windows’2000.
33. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
34. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
35. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
36. Распределенные информационные системы. Удаленные атаки на информационную систему.
37. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
38. Физические средства обеспечения информационной безопасности.
39. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
40. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
41. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
42. Виртуальные частные сети, их функции и назначение.

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

См. Приложение №2 к рабочей программе.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модулю).

Основная литература

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

2. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

3. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

Дополнительная литература

1. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008.— 176 с.— ISBN 978-985-463-258-2.

2. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008.— 272 с.— ISBN 978-5-388-00069-9.

3. Брандман Э. М. Глобализация и информационная безопасность общества/Э.М.Брандман //Философия и общество.-2006.-№1.-С.31-41.

4. Поляков В.П. Информационная безопасность в курсе информатики /В.П.Поляков //Информатика и образование.-2006.-№10.-С.116-119.

5. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008.— 272 с.— ISBN 978-5-388-00069-9.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины (модулю)

1. Электронная библиотека Регионального финансово-экономического института – http://students.rfei.ru/a/students/library.jspx
2. Википедия [Электронный ресурс] : [свобод. Интернет-энцикл.] – Электрон. дан. и прогр. – Режим доступа: http://ru.wikipedia.org, свободный. – Русскояз. часть междунар. проекта «Википедия».

9. Методические указания для обучающихся по освоению дисциплины (модулю)

Методические указания по изучению дисциплины представляют собой комплекс рекомендаций и объяснений, позволяющих бакалавру оптимальным образом организовать процесс изучения данной дисциплины. Известно, что в структуре учебного плана значительное время отводится на самостоятельное изучение дисциплины. В рабочих программах дисциплин размещается примерное распределение часов аудиторной и внеаудиторной нагрузки по различным темам данной дисциплины.

Для успешного освоения дисциплины бакалавр должен:

1. Прослушать курс лекций по дисциплине.

2. Выполнить все задания, рассматриваемые на практических занятиях, включая решение задач.

3. Выполнить все домашние задания, получаемые от преподавателя.

4. Решить все примерные практические задания, рассчитанные на подготовку к промежуточной аттестации.

При подготовке к промежуточной аттестации особое внимание следует обратить на следующие моменты:

1. Выучить определения всех основных понятий.

2. Повторить все задания, рассматриваемые в течение семестра.

3. Проверить свои знания с помощью тестовых заданий.

Рекомендации по работе на лекционном занятии

На лекциях преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на семинарское занятие и указания на самостоятельную работу. В ходе лекции бакалавр должен внимательно слушать и конспектировать лекционный материал.

Рекомендации для самостоятельной работы

Самостоятельная работа бакалавров – планируемая учебная, научно-исследовательская работа, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Цель самостоятельной работы бакалавра – научиться осмысленно и

самостоятельно работать сначала с учебным материалом, затем с научной информацией, изучить основы самоорганизации и самовоспитания с тем, чтобы в дальнейшем непрерывно повышать свою квалификацию.

Целью самостоятельной работы бакалавров по дисциплине является овладение фундаментальными знаниями, профессиональными умениями и навыками решения задач и теоретическим материалом по дисциплине. Самостоятельная работа способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению различных проблем.

В зависимости от конкретных видов самостоятельной работы, используемых в каждой конкретной рабочей программе, следует придерживаться следующих рекомендаций.

Одной из форм текущего контроля знаний студентов является контрольная работа. Контрольная работа подразумевает знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, требующихся для запоминания и являющихся основополагающими в этой теме.

Выполняя контрольную работу, необходимо внимательно ознакомиться с условиями заданий и написать развернутый и аргументированный ссылками на нормативные акты и литературу ответ. При написании контрольной работы необходимо проанализировать научную и учебную специальную литературу, действующие нормативно-правовые акты, публикации в периодической печати, судебную практику, статистические данные. В процессе выполнения работы необходимо подтверждать свои выводы цифровыми примерами, представленными в виде таблиц, диаграмм, графиков, а также примерами судебной практики. Как правило, контрольные работы проводятся на семинарском занятии.

Подготовка к написанию реферата предполагает поиск литературы и составление списка используемых источников, изложение мнения авторов и своего суждения по выбранному вопросу; формулирование основных аспектов проблемы.

Коллоквиум представляет собой одну из форм учебных занятий, ориентированную на определение качества работы с конспектом лекций, подготовки ответов к контрольным вопросам и др. Коллоквиумы, как правило, проводятся в форме мини-экзамена, имеющего целью уменьшить список тем, выносимых на основной экзамен, и оценить текущий уровень знаний бакалавров.

При подготовке к практикуму/лабораторной работе бакалаврам предлагается выполнить задания, подготовить проекты, составленные преподавателем по каждой учебной дисциплине.

Следует также учитывать краткие комментарии при написании курсовой работы, если она предусмотрена рабочей программой, и подготовке к итоговому контролю, проводимого в форме зачета и (или) экзамена. Так,

написание курсовой работы базируется на изучении научной, учебной, нормативной и другой литературы. Включает отбор необходимого материала, формирование выводов и разработку конкретных рекомендаций по решению поставленных цели и задач, проведение практических исследований по данной теме. Все необходимые требования к оформлению находится в методических указаниях по написанию курсовой работы.

Рекомендации по подготовке к практическому (семинарскому) занятию

Семинарское занятие представляет собой такую форму обучения в учреждениях высшего образования, которая предоставляет студентам возможности для обсуждения теоретических знаний с целью определения их практического применения, в том числе средствами моделирования профессиональной деятельности. Семинарские занятия служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности бакалавров по изучаемой дисциплине. При наличии практических заданий по изучаемой дисциплине бакалавр выполняет все упражнения и задачи, подготовленные преподавателем. Целью практического занятия является более углубленное изучение отдельных тем дисциплины и применение полученных теоретических навыков на практике.

Семинарское занятие не сводится к закреплению или копированию знаний, полученных на лекции. Его задачи значительно шире, сложнее и интереснее. Семинарское занятие одновременно реализует учебное, коммуникативное и профессиональное предназначение. Подготовка к практическому (семинарскому) занятию начинается с тщательного ознакомления с условиями предстоящей работы, т. е. с обращения к планам семинарских занятий.

Подготовка к практическим занятиям должна носить систематический характер. Это позволит бакалавру в полном объеме выполнить все требования преподавателя.

Тщательная подготовка к семинарским занятиям, как и к лекциям, имеет определяющее значение: семинар пройдёт так, как аудитория подготовилась к его проведению.

Самостоятельная работа – столп, на котором держится вся подготовка по изучаемому курсу. Готовясь к практическим занятиям, следует активно пользоваться справочной литературой: энциклопедиями, словарями, альбомами схем и др. Владение понятийным аппаратом изучаемого курса является необходимостью.

При подготовке к семинару бакалавры имеют возможность воспользоваться консультациями преподавателя. Кроме указанных тем бакалавры вправе, по согласованию с преподавателем, избирать и другие интересующие их темы.

Определившись с проблемой, привлекающей наибольшее внимание, следует обратиться к рекомендуемой литературе. Следует иметь ввиду, что в семинаре участвует вся группа, а потому задание к практическому занятию следует распределить на весь коллектив. Задание должно быть охвачено полностью и рекомендованная литература должна быть освоена группой в полном объёме.

Для полноценной подготовки к практическому занятию чтения учебника крайне недостаточно – в учебных пособиях излагаются только принципиальные основы, в то время как в монографиях и статьях на ту или иную тему поднимаемый вопрос рассматривается с разных ракурсов или ракурса одного, но в любом случае достаточно подробно и глубоко. Тем не менее, для того, чтобы должным образом сориентироваться в сути задания, сначала следует ознакомиться с соответствующим текстом учебника – вне зависимости от того, предусмотрена ли лекция в дополнение к данному семинару или нет. Оценив задание, выбрав тот или иной сюжет, и подобрав соответствующую литературу, можно приступать собственно к подготовке к семинару. Для получения более глубоких знаний бакалаврам рекомендуется изучать дополнительную литературу. Следует активно пользоваться справочной литературой: энциклопедиями, словарями, альбомами схем и др. Владение понятийным аппаратом изучаемого курса является необходимостью. В ходе работы студент должен применить приобретенные знания при обобщении теоретического и практического материала, продемонстрировать навыки грамотного изложения своих мыслей с использованием общеправовой и отраслевой терминологии.

Семинар (практическое занятие) предполагает свободный обмен мнениями по избранной тематике. Преподаватель формулирует цель занятия и характеризует его основную проблематику. Заслушиваются сообщения бакалавров. Обсуждение сообщения совмещается с рассмотрением намеченных вопросов. Кроме того заслушиваются сообщения, предполагающие анализ публикаций по отдельным вопросам семинара. Поощряется выдвижение и обсуждение альтернативных мнений. Преподаватель подводит итоги обсуждения и объявляет оценки выступавшим бакалаврами. В целях контроля подготовленности бакалавров и привития им навыков краткого письменного изложения своих мыслей преподаватель в ходе семинарских занятий может осуществлять текущий контроль знаний в виде тестовых заданий.

На семинаре идёт не проверка вашей подготовки к занятию (подготовка есть необходимое условие), но степень проникновения в суть материала, обсуждаемой проблемы. Поэтому беседа будет идти не по содержанию прочитанных работ; преподаватель будет ставить проблемные вопросы, не все из которых могут прямо относиться к обработанной вами литературе.

В ходе практических занятий бакалавры под руководством преподавателя могут рассмотреть различные методы решения задач по дисциплине. Продолжительность подготовки к практическому занятию должна составлять не менее того объема, что определено тематическим планированием в рабочей

программе. Практические занятия по дисциплине могут проводиться в различных формах:

1) устные ответы на вопросы преподавателя по теме занятия; 2) письменные ответы на вопросы преподавателя; 3) групповое обсуждение той или иной проблемы под руководством и контролем преподавателя; 4) заслушивания и обсуждение контрольной работы; 5) решение задач.

При работе необходимо не только привлечь наиболее широкий круг литературы, но и суметь на ее основе разобраться в степени изученности темы. Стоит выявить дискуссионные вопросы, нерешенные проблемы, попытаться высказать свое отношение к ним, привести и аргументировать свою точку зрения или отметить, какой из имеющихся в литературе точек зрения по данной проблематике придерживается автор и почему.

Рекомендации по работе с литературой

Изучение литературы очень трудоемкая и ответственная часть подготовки к семинарскому занятию, написанию эссе, реферата, доклада и т.п. Работа над литературой, статья ли это или монография, состоит из трёх этапов – чтения работы, её конспектирования, заключительного обобщения сути изучаемой работы.

Работа с литературой, как правило, сопровождается записями в следующих формах:

- конспект – краткая схематическая запись основного содержания научной работы. Целью конспектирования является выявление логики, схемы доказательств, основных выводов произведения;
- план – краткая форма записи прочитанного, перечень вопросов, рассматриваемых в книге, статье, составление плана раскрывает логику произведения, способствует ориентации в его содержании;
- выписки – либо цитаты из произведения, либо дословное изложение мест из источника, способствуют более глубокому пониманию читаемого текста;
- тезисы – сжатое изложение основных мыслей и положений прочитанного материала;
- аннотация – очень краткое изложение содержания прочитанной работы, составляется после полного прочтения и осмысливания работы;
- резюме – краткая оценка прочитанного произведения, отражает наиболее общие выводы и положения работы, ее концептуальные итоги.

Прежде, чем браться за конспектирование, скажем, статьи, следует её хотя бы однажды прочитать, чтобы составить о ней предварительное мнение, постараться выделить основную мысль или несколько базовых точек, опираясь на которые можно будет в дальнейшем работать с текстом.

Конспектирование – дело очень тонкое и трудоёмкое, в общем виде может

быть определено как фиксация основных положений и отличительных черт рассматриваемого труда вкупе с творческой переработкой идей, в нём содержащихся. Конспектирование – один из эффективных способов усвоения письменного текста. Хотя само конспектирование уже может рассматриваться как обобщение, тем не менее есть смысл выделить последнее особицей, поскольку в ходе заключительного обобщения идеи изучаемой работы окончательно утверждаются в сознании изучающего. Достоинством заключительного обобщения как самостоятельного этапа работы с текстом является то, что здесь читатель, будучи автором обобщений, отделяет себя от статьи, что является гарантией независимости читателя от текста.

Если программа занятия предусматривает работу с источником, то этой стороне подготовки к семинару следует уделить пристальное внимание. В сущности, разбор источника не отличается от работы с литературой – то же чтение, конспектирование, обобщение.

Рекомендации к написанию реферата

Использование реферата в качестве промежуточного или итогового отчета студента о самостоятельном изучении какой-либо темы учебного курса предполагает, прежде всего, установление целей и задач данной работы, а также его функциональной нагрузки в процессе обучения.

Реферат – это композиционно-организованное, обобщенное изложение содержания источника информации (в учебной ситуации – статей, монографий, материалов конференции, официальных документов и др., но не учебника по данной дисциплине). Тема реферата может быть предложена преподавателем или выбрана студентом из рабочей программы соответствующей дисциплины.

Возможно, после консультации с преподавателем, обоснование и формулирование собственной темы.

Тема реферата должна отражать проблему, которая достаточно хорошо исследована в науке. Как правило, внутри такой проблемы выбирается для анализа какой-либо единичный аспект.

Тематика может носить различный характер:

- межпредметный,
- внутрипредметный,
- интегративный,
- быть в рамках программы дисциплины или расширять ее содержание (рассмотрение истории проблемы, новых теорий, новых аспектов проблемы).

Целью реферата является изложение какого-либо вопроса на основе обобщения, анализа и синтеза одного или нескольких первоисточников. Другими словами, реферат отвечает на вопрос «какая информация содержится в первоисточнике, что излагается в нем?».

Принимая во внимание, что реферат – одна из форм интерпретации исходного текста одного или нескольких первоисточников, следует

сформулировать задачу, стоящую перед студентами: создать новый текст на основе имеющихся текстов, т.е. текст о тексте. Новизна в данном случае подразумевает собственную систематизацию материала при сопоставлении различных точек зрения авторов и изложении наиболее существенных положений и выводов реферируемых источников.

1. Требования к рефератам.

Прежде всего, следует помнить, что реферат не должен отражать субъективных взглядов референта (студента) на излагаемый вопрос, а также давать оценку тексту.

Основными требованиями к реферату считаются:

1. информативность и полнота изложения основных идей первоисточника;
2. точность изложения взглядов автора – неискаженное фиксирование всех положений первичного текста,
3. объективность – реферат должен раскрывать концепции первоисточников с точки зрения их авторов;
4. изложение всего существенного – «чтобы уметь схватить новое и существенное в сочинениях» (М.В. Ломоносов);
5. изложение в логической последовательности в соответствии с обозначенной темой и составленным планом;
6. соблюдение единого стиля – использование литературного языка в его научно-стилевой разновидности;
7. корректность в характеристике авторского изложения материала.

2. Виды рефератов.

По характеру воспроизведения информации различают рефераты репродуктивные и продуктивные.

Репродуктивные рефераты воспроизводят содержание первичного текста:

- реферат-конспект содержит в обобщенном виде фактографическую информацию, иллюстративный материал, сведения о методах исследования, о полученных результатах и возможностях их применения;
- реферат-резюме приводит только основные положения, тесно связанные с темой текста.

Продуктивные рефераты предполагают критическое или творческое осмысление литературы:

- реферат-обзор охватывает несколько первичных текстов, дает сопоставление разных точек зрения по конкретному вопросу;
- реферат-доклад дает анализ информации, приведенной в первоисточниках, и объективную оценку состояния проблемы.

По количеству реферируемых источников:

- монографические – один первоисточник;
- обзорные – несколько первичных текстов одной тематики.

По читательскому назначению:

- общие – характеристика содержания в целом; ориентация на широкую аудиторию;
- специализированные – ориентация на специалистов.

3. Этапы работы над рефератом.

1. Выбор темы.
2. Изучение основных источников по теме.
3. Составление библиографии.
4. Конспектирование необходимого материала или составление тезисов.
5. Систематизация зафиксированной и отобранной информации.
6. Определение основных понятий темы и анализируемых проблем.
7. Разработка логики исследования проблемы, составление плана.
8. Реализация плана, написание реферата.
9. Самоанализ, предполагающий оценку новизны, степени раскрытия сущности проблемы, обоснованности выбора источников и оценку объема реферата.
10. Проверка оформления списка литературы.
11. Редакторская правка текста.
12. Оформление реферата и проверка текста с точки зрения грамотности и стилистики.

4. Структура реферата.

В структуре реферата выделяются три основных компонента: библиографическое описание, собственно реферативный текст, справочный аппарат.

Библиографическое описание предполагает характеристику имеющихся на эту тему работ, теорий; историографию вопроса; выделение конкретного вопроса (предмета исследования); обоснование использования избранных первоисточников.

Собственно реферативный текст:

Введение – обоснование актуальности темы, проблемы; предмет, цели и задачи реферируемой работы, предварительное формулирование выводов.

Основная часть – содержание, представляющее собой осмысление текста, аналитико-синтетическое преобразование информации, соответствующей теме реферата.

Основную часть рекомендуется разделить на два-три вопроса. В зависимости от сложности и многогранности темы, вопросы можно разделить на параграфы. Чрезмерное дробление вопросов или, наоборот, их отсутствие приводят к поверхностному изложению материала. Каждый вопрос должен заканчиваться промежуточным выводом и указывать на связь с последующим вопросом.

Заключение – обобщение выводов автора, область применения результатов работы.

Справочный аппарат:

Список литературы – список использованных автором реферата работ (может состоят из одного и более изданий).

Приложения (необязательная часть) – таблицы, схемы, графики, фотографии и т.д.

Реферат как образец письменной научной речи

1. Качества научной речи.

Функциональные стили различаются:

- характером предаваемой информации;
- сферой функционирования;
- адресатом;
- использованием языковых средств различных уровней.

Главной коммуникативной задачей реферата является выражение научных понятий и умозаключений.

Реферат должен быть написан научным стилем, что предполагает:

- передачу информации научного характера;
- функционирование в образовательной среде;
- в качестве адресата преподавателя, т.е. специалиста, или студентов,
- заинтересованных в получении данной информации;
- демонстрацию характерных языковых особенностей письменной разновидности научно-учебного подстиля литературного языка.

Научный стиль обладает рядом экстралингвистических характеристик, или качеств:

- точность – строгое соответствие слов обозначаемым предметам и явлениям действительности (знание предмета и умение выбирать необходимую лексику);
- понятность – доступность речи для тех, кому она адресована (правильное использование терминов, иностранных слов, профессионализмов);
- логичность, последовательность – четкое следование в изложении логике и порядку связей в действительности (первоисточнике);
- объективность – отсутствие субъективных суждений и оценок в изложении информации;
- абстрактность и обобщенность – отвлеченность от частных, несущественных признаков;
- преобладание рассуждения как типа речи над описанием и повествованием;
- графическая информация наличие схем, графиков, таблиц, формул и т.п.

2. Особенности письменной научной речи

Письменная речь, в отличие от устной, подразумевает:

- определенную степень подготовленности к работе;
- возможность исправления и доработки текста;
- наличие композиции строения, соотношения и взаимного расположения частей реферата;
- выдержанность стиля изложения; строгое следование лексическим и грамматическим нормам.

Доминирующим фактором организации языковых средств в научном стиле является их обобщенно-отвлеченный характер на лексическом и грамматическом уровнях языковой системы.

Лексический уровень предполагает:

- использование абстрактной лексики, преобладающей над конкретной: мышление, отражение, изменяемость, преобразование, демократизация и т.п.;
- отсутствие единичных понятий и конкретных образов, что подчеркивается употреблением слов обычно, постоянно, регулярно, систематически, каждый и т.п.;
- преобладание терминов различных отраслей науки: лексикология, коммуникация, эмпиризм, гносеология, адаптация и т.п.;
- использование слов общенаучного употребления: функция, качество, значение, элемент, процесс, анализ, доказательство и т.п.;
- употребление многозначных слов в одном (реже двух) значениях: предполагать (считать, допускать); окончание (завершение), рассмотреть (разобрать, обдумать, обсудить) и т.п.;
- наличие специфических фразеологизмов: рациональное зерно, демографический взрыв, магнитная буря и т.п.;
- клиширование: представляет собой..., включает в себя..., относится к..., заключается в... и т.п.;
- преобладание отвлеченных существительных над однокоренными глаголами: взаимодействие, зависимость, классификация, систематизация и т.п.

Грамматический уровень:

- использование аналитической степени сравнения: более сложный, наиболее простой, менее известный и т.п. в отличие от эмоционально окрашенных: наиважнейший, сложнейший, ближайший и т.п.;

- преимущественное употребление глаголов 3 лица ед. и мн.ч. настоящего времени (реже 1 лица будущего времени сравним, рассмотрим): исследуются, просматривается, подразумевается, доказывает и т.п.;
- активность союзов, предлогов, предложных сочетаний: в связи..., в соответствии..., в качестве..., в отношении..., сравнительно с ... и т.п.;
- преобладание пассивных (страдательных) конструкций: рассмотрены вопросы,
- описаны явления, сделаны выводы, отражены проблемы и т.п.;
- выражение четкой связи между частями сложного предложения: следует сказать, что...; наблюдения показывают, что..., необходимо подчеркнуть, что... и т.п.;
- усиленная связующая функция наречий и наречных выражений: поэтому, итак, таким образом, наконец... и т.п.;
- осложнение предложений обособленными конструкциями: «Стремлением к смысловой точности и информативности обусловлено употребление в научной речи конструкций с несколькими вставками и пояснениями, уточняющими содержание высказывания, ограничивающими его объем, указывающими источник информации и т.д.».

Обобщая отличительные языковые особенности письменного научного стиля, можно сказать, что он характеризуется:

- употреблением книжной, нейтральной и терминологической лексики;
- преобладанием абстрактной лексики над конкретной;
- увеличением доли интернационализмов в терминологии;
- относительной однородностью, замкнутостью лексического состава;
- неупотребительностью разговорных и просторечных слов; слов с эмоционально-экспрессивной и оценочной окраской;
- наличием синтаксических конструкций, подчеркивающих логическую связь и последовательность мыслей.

Оформление реферата. Критерии оценки.

Правила оформления реферата регламентированы. Объем – не более 10-15 стр. машинописного текста, напечатанного в формате Word 7,0, 8,0; размер шрифта – 14; интервал – 1,5, формат бумаги А 4, сноски постраничные, сплошные; поле (верхнее, нижнее, левое, правое) 2 мм; выравнивание – по ширине; ориентация книжная; шрифт Times New Roman Cyr.

Работа должна иметь поля; каждый раздел оформляется с новой страницы.

Титульный лист оформляется в соответствии с установленной формой.

На первой странице печатается план реферата, включающий в себя библиографическое описание; введение, разделы и параграфы основной части,

раскрывающие суть работы, заключение; список литературы; приложения.

В конце реферата представляется список использованной литературы с точным указанием авторов, названия, места и года ее издания.

Критерии оценки реферата.

1. Степень раскрытия темы предполагает:

- соответствие плана теме реферата;
- соответствие содержания теме и плану реферата;
- полноту и глубину раскрытия основных понятий;
- обоснованность способов и методов работы с материалом;
- умение работать с литературой, систематизировать и структурировать материал;
- умение обобщать, делать выводы, сопоставлять различные
- точки зрения по рассматриваемому вопросу.

2. Обоснованность выбора источников оценивается:

- полнотой использования работ по проблеме;
- привлечением наиболее известных и новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).

3. Соблюдение требований к оформлению определяется:

- правильным оформлением ссылок на используемую литературу;
- оценкой грамотности и культуры изложения;
- владением терминологией и понятийным аппаратом проблемы;
- соблюдением требований к объему реферата;
- культурой оформления.

Защита реферата

Рефераты обычно представляются на заключительном этапе изучения дисциплины как результат итоговой самостоятельной работы студента. Защита реферата осуществляется или на аудиторных занятиях, предусмотренных учебным планом, или на зачете как один из вопросов билета (последнее определяется преподавателем).

Если реферат подразумевает публичную защиту, то выступающему следует заранее подготовиться к реферативному сообщению, а преподавателю и возможным оппонентам – ознакомиться с работой.

Реферативное сообщение отличается от самого реферата прежде всего объемом и стилем изложения, т.к. учитываются особенности устной научной речи и публичного выступления в целом. В реферативном сообщении содержание реферата представляется подробно (или кратко) и, как правило, вне оценки, т.е. изложение приобретает обзорный характер и решает коммуникативную задачу (передать в устной форме информацию, которая должна быть воспринята слушателями). Учитывая публичный характер высказываний, выступающий должен:

- составить план и тезисы выступления;
- кратко представить проблематику, цель, структуру и т.п.;
- обеспечить порционную подачу материала не в соответствии с частями, разделами и параграфами, а сегментировать в зависимости от новизны информации;
- соблюдать четкость и точность выражений, их произнесение; обращать внимание на интонацию, темп, громкость и т.п. особенности публичного выступления;
- демонстрировать подготовленный характер высказываний, допуская, как в любой другой устной речи, словесную импровизацию.

Рекомендации по написанию эссе

Эссе – средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием концепций и аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.

Цель эссе состоит в развитии таких навыков, как самостоятельное творческое мышление и письменное изложение собственных мыслей.

Структура эссе определяется предъявляемыми требованиями:

- мысли автора по проблеме излагаются в форме кратких тезисов.
- мысль должна быть подкреплена доказательствами – поэтому за тезисом следуют аргументы.

Аргументы – это факты, явления общественной жизни, события, жизненные ситуации и жизненный опыт, научные доказательства, ссылки на мнение ученых и др.

Эссе обычно имеет кольцевую структуру (количество тезисов и аргументов зависит от темы, избранного плана, логики развития мысли):

- вступление
- тезис, аргументы
- тезис, аргументы
- тезис, аргументы
- заключение.

При написании эссе надо учитывать следующее:

Вступление и заключение должны фокусировать внимание на проблеме (во вступлении она ставится, в заключении – резюмируется мнение автора).

Необходимо выделение абзацев, красных строк, установление логической связи абзацев: так достигается целостность работы.

Стиль изложения: эмоциональность, экспрессивность, художественность.

Правила написания эссе:

- из формальных правил можно назвать только одно – наличие заголовка;
- внутренняя структура может быть произвольной. Поскольку это малая форма письменной работы, то не требуется обязательное повторение выводов в конце, они могут быть включены в основной текст или в заголовок;
- аргументация может предшествовать формулировке проблемы. Формулировка проблемы может совпадать с окончательным выводом.

В качестве примера можете познакомиться с широко известными эссе И.А. Бунина («Недостатки современной поэзии»), Д.С. Мережковского («О причинах упадка и новых течениях современной русской литературы»), К.Д. Бальмонта («Элементарные слова о символической поэзии»), В.Я. Брюсова («Ключи тайн»), Вяч. Иванова («Символизм как миропонимание»), А.А. Блока («О лирике»).

Учебно-методические указания к выполнению тестовых заданий

Тестовый контроль отличается от других методов контроля (устные и письменные экзамены, зачеты, контрольные работы и т.п.) тем, что он представляет собой специально подготовленный контрольный набор заданий, позволяющий надежно и адекватно количественно оценить знания обучающихся посредством статистических методов.

Все вышеуказанные преимущества тестового контроля могут быть достигнуты лишь при использовании теории педагогических тестов, которая сложилась на стыке педагогики, психологии и математической статистики. Основными достоинствами применения тестового контроля являются:

- объективность результатов проверки, так как наличие заранее определенного эталона ответа (ответов) каждый раз приводит к одному и тому же результату;
- повышение эффективности контролирующей деятельности со стороны преподавателя за счет увеличения её частоты и регулярности;
- возможность автоматизации проверки знаний учащихся, в том числе с использованием компьютеров;
- возможность использования в системах дистанционного образования.

Тест – инструмент, состоящий из системы тестовых заданий с описанными системами обработки и оценки результата, стандартной процедуры проведения и процедуры для измерения качеств и свойств личности, изменение которых возможно в процессе систематического обучения.

Преимущество тестового контроля состоит в том, что он является научно обоснованным методом эмпирического исследования и в определенной сфере позволяет преодолеть умозрительные оценки знаний студентов. Следует отметить, что задания, используемые многими преподавателями и называемые ими тестовыми, на самом деле таковыми вовсе не являются. В отличие от

обычных задач тестовые задания имеют четкий однозначный ответ и оцениваются стандартно на основе ценника. В самом простом случае оценка студента есть сумма баллов за правильно выполненные задания. Тестовые задания должны быть краткими, ясными и корректными, не допускающими двусмысленности. Сам же тест представляет собой систему заданий возрастающей трудности. Тестовый контроль может применяться как средство текущего, тематического и рубежного контроля, а в некоторых случаях и итогового.

Текущее тестирование осуществляется после изучения отдельной темы или группы тем. Текущее тестирование, прежде всего, является одним из элементов самоконтроля и закрепления слушателем пройденного учебного материала.

Виды тестовых заданий

Тестовое задание (ТЗ) может быть представлено в одной из следующих стандартизированных форм:

- закрытое ТЗ, предполагающее выбор ответов (испытуемый выбирает правильный ответ (ответы) из числа готовых, предлагаемых в задании теста);
- открытое ТЗ (испытуемый сам формулирует краткий или развернутый ответ);
- ТЗ на установление правильной последовательности;
- ТЗ на установление соответствия между элементами двух множеств.

Закрытое тестовое задание

Закрытое ТЗ состоит из неполного тестового утверждения с одним ключевым элементом и множеством допустимых вариантов ответов, один или несколько из которых являются правильными. Тестируемый студент определяет правильные ответы из данного множества. Рекомендуется пять или шесть вариантов ответов, из которых два или три являются правильными.

Открытое тестовое задание

Открытое ТЗ имеет вид неполного утверждения, в котором отсутствует один или несколько ключевых элементов и требует самостоятельной формулировки ответа тестируемого. В качестве отсутствующих ключевых элементов могут быть: число, буква, слово или словосочетание. При формулировке задания на месте ключевого элемента необходимо поставить прочерк или многоточие.

Тестовое задание на установление правильной последовательности

ТЗ на установление правильной последовательности состоит из однородных элементов некоторой группы и четкой формулировки критерия упорядочения этих элементов.

Тестовое задание на установление соответствия

ТЗ на установление соответствия состоит из двух групп элементов и четкой формулировки критерия выбора соответствия между ними. Внутри

каждой группы элементы должны быть однородными. Количество элементов во второй группе должно превышать количество элементов первой группы, но не более чем в 2 раза. Максимально допустимое количество элементов во второй группе не должно превышать 10. Количество же элементов в первой группе должно быть не менее двух.

Требования к тестовым заданиям

Для обеспечения адекватности оценки знаний тесты должны обладать следующими свойствами:

- тест должен быть **репрезентативным** с точки зрения изучаемого материала (ответы на вопросы, поставленные в тесте, не должны выходить за пределы данной учебной дисциплины);
- тест должен быть **уместным**: формулировка и состав вопросов должны соответствовать основной цели дисциплины (при тестировании по определенной теме вопросы должны соответствовать одной из основных задач дисциплины, упомянутых в программе курса);
- тест должен быть **объективным**, что заключается в неизбежности выбора правильного варианта ответа различными экспертами, а не только преподавателем, оставившим тест;
- тест должен быть **специфичным**, т.е. в тесте не должно быть таких вопросов, на которые мог бы ответить человек, не знающий данной дисциплины, но обладающий достаточной эрудицией;
- тест должен быть **оперативным**, что предусматривает возможность быстрого ответа на отдельный вопрос, поэтому вопросы формулируются коротко и просто и не должны включать редко используемые слова, конечно, если эти слова не являются понятиями, знание которых предусмотрено в учебной дисциплине.

Перечисленные свойства тестовых заданий обеспечивают необходимый качественный уровень проведения итогового контроля, к которому предъявляются следующие требования.

Процесс тестирования должен быть **валидным** (значимым), когда результаты подтверждают конкретные навыки и знания, которые экзамен подразумевает проверить.

Тестирование является **объективным**, если результаты не отражают мнения или снисходительность проверяющего.

Убедиться в **надежности** тестирования можно, если результаты повторно подтверждены последующими контрольными мероприятиями.

Эффективность тестирования определяется, если его выполнение и оценивание не занимает больше времени или денег, чем необходимо.

Тестирование можно считать **приемлемым**, если студенты и преподаватели воспринимают контрольное мероприятие адекватно его

значимости.

Изучение динамики процесса проверки знаний с помощью тестов позволяет установить индивидуальное время тестирования для каждого конкретного набора тестовых заданий. Нередко время тестирования для различных дисциплин устанавливается одинаковым на основании некоторого стандарта, не принимая во внимание специфику конкретной дисциплины и ее раздела.

Указания по подготовке к зачету/экзамену

Формой итогового контроля знаний и умений, полученных в процессе изучения дисциплины является зачет и экзамен.

Экзамен (зачет) дает возможность преподавателю:

- выяснить уровень освоения студентами учебной программы дисциплины;
- оценить формирование у студентов определенных знаний и навыков их использования, необходимых и достаточных для будущей профессиональной деятельности;
- оценить умение студентов творчески мыслить и логически правильно излагать ответы на поставленные вопросы.

При подготовке к экзамену (зачету) необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др. Сдача экзамена и (или) зачета предполагает полное понимание, запоминание и применение изученного материала на практике. Для успешной подготовки к промежуточной аттестации студентам необходимо вновь обратиться к пройденному материалу. Литература для подготовки к экзамену (зачету) рекомендуется преподавателем, либо указана в рабочей программе по дисциплине.

При подготовке к промежуточной аттестации в качестве ориентира студент может использовать перечень контрольных вопросов для самопроверки. Подготовка ответов на эти вопросы позволит:

- выяснить уровень освоения студентами учебных программ;
- оценить формирование у студентов определенных знаний и навыков их использования, необходимых и достаточных для будущей профессиональной деятельности;
- оценить умение студентов творчески мыслить и логически правильно излагать ответы на поставленные вопросы.

Оценка знаний студентов должна опираться на строго объективные критерии, научно обоснованные педагогикой и обязательные для выполнения всех преподавателей.

Среди таких критериев важнейшими являются принципы подхода к оценке. В наиболее общем виде эти принципы можно представить следующим образом:

- глубокие знания и понимание существа вопроса, но не всех его деталей, а лишь основных;

- степень сознательного и творческого усвоения изучаемых наук как базы личных убеждений и полезных обществу действий;
- понимание сущности науки, места каждой темы в общем курсе и её связи с предыдущими и последующими темами;
- выделение коренных проблем науки и умение правильно использовать это знание в самостоятельной научной деятельности или практической работе по специальности.

Экзамен (зачет) может проводиться в устной, письменной форме и с применением тестов. Экзамен (зачет) проводится по вопросам, охватывающим весь пройденный материал. По окончанию экзамена (зачета) преподаватель может задать студенту дополнительные и уточняющие вопросы.

Студентам необходимо тщательно готовиться к итоговому экзамену. Процесс подготовки к итоговому экзамену начинается, по существу, с самого первого этапа изучения предмета. Он включает в себя самостоятельную работу над рекомендованной литературой. Как правило, он начинается за полтора-два месяца до экзаменационной сессии. Изучив и законспектировав рекомендованные источники, выполнив предусмотренные учебным планом письменные работы и имея рецензии на них, студент начинает непосредственную подготовку к экзамену с тщательной отработки курса в соответствии с требованиями учебной программы и выполнения рекомендаций преподавателя, данных в рецензии. На этом этапе студент должен повторить изученное по учебникам и учебным пособиям, личным конспектам, записям лекций и другим материалам. При этом особое внимание должно быть обращено на тщательную отработку тех конкретных вопросов и тем учебной программы, которые слабо усвоены.

При повторении материала перед итоговым экзаменом необходима самопроверка или взаимная проверка знаний. В этом случае по каждой теме надо еще раз хорошо продумать материал, найти соответствующие статьи из нормативных актов, подобрать примеры. Вполне себя оправдывает групповая взаимная проверка. Для этого рекомендуется собираться по 3-4 человека и проводить разбор вопросов по курсу. Экзамен проводится по билетам. Если какой-либо из поставленных в билете вопросов студенту кажется неясным, он может обратиться к преподавателю за разъяснением. Пользоваться наглядными пособиями, словарями или справочниками можно только с разрешения преподавателя. При подготовке к ответу, а также при ответе не обязательно придерживаться той последовательности вопросов, которая дана в билетах. Записи ответов лучше делать в виде развернутого плана, их можно дополнить цифрами, примерами, фактами, а также сослаться на необходимые нормативные акты и другие источники.

Ответ должен быть построен в форме свободного рассказа. Важно не только верно изложить соответствующее положение, но и дать его глубокое теоретическое обоснование. При ответах надо избегать больших выступлений,

отклонений от существа вопросов, но не следует вдаваться и в такую крайность, как погоня за краткостью. Такой ответ не раскроет содержания вопроса и не даст возможности преподавателю правильно судить о знаниях студента. После ответов на вопросы билета преподаватель может задать дополнительные вопросы, на которые студент обязан ответить.

Экзаменатор оценивает знания по четырехбалльной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Все положительные оценки записываются в экзаменационную ведомость и зачетную книжку. Неудовлетворительные оценки проставляются в экзаменационную ведомость.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При осуществлении образовательного процесса используется ряд информационных технологий обеспечения дистанционного обучения, включающий, но не исчерпывающийся, технологиями онлайн и оффлайн распространения образовательной информации (почтовая рассылка печатных материалов и бланков тестирования или электронных версий образовательных материалов на физических носителях, либо интерактивный доступ к материалам через интернет, доступ к электронно-библиотечным системам института и сторонних поставщиков), технологиями взаимодействия студентов с преподавателем (видео-лекции и семинары, групповые и индивидуальные консультации через интернет, индивидуальные консультации по телефону), технологиями образовательного контроля (интерактивные онлайн тесты в интернет, оффлайн тесты с использованием персональных печатных бланков).

Для реализации указанных технологий используется набор программного обеспечения и информационных систем, включающий, но не ограничивающийся, следующим списком.

1. операционные системы Microsoft Windows (различных версий);
2. операционная система GNU/Linux;
3. свободный фисный пакет LibreOffice;
4. система управления процессом обучения «Lete e-Learning Suite» (собственная разработка);
5. система электронного обучения студентов направления подготовки «Бизнес-информатика» EduTerra.pro
6. система интерактивного онлайн тестирования (собственная разработка);
7. система телефонной поддержки и консультаций сотрудниками колл-центра «Центральная служба поддержки» (собственная разработка);
8. система онлайн видео конференций Adobe Connect;

9. электронно-библиотечная система «Айбукс»;
10. электронно-библиотечная система «Издательства «Лань»;
11. интернет-версия справочника «КонсультантПлюс»;
12. приложение для мобильных устройств «КонсультантПлюс: Студент»;
13. справочная правовая система «Гарант»;
14. иные ИСС.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

2. Аудиторная база (лекционная аудитория, аудитория для проведения практических занятий, виртуальные классные комнаты на портале РФЭИ)
3. Организационно-технические средства и аудиовизуальный фондовый материал, мультимедийное оборудование.
4. Комплекты видеофильмов, аудиокниг, CD-дисков по проблемам дисциплины.
5. Интернет.

ПРИЛОЖЕНИЯ

Приложение 1

Таблица. Результаты обучения по дисциплине «Информационная безопасность», соотнесенные с планируемыми результатами освоения образовательной программы

Название дисциплины	Планируемые результаты обучения		Компетенции											
	код	описание	ОК-1	ОК-5	ОК-11	ОК-12	ОК-13	ОК-16	ОК-17	ПК-2	ПК-5	ПК-19	ПК-20	ПК-28
Информационная безопасность	З-1	знает основные понятия информационной безопасности	x	x	x	x	x	x	x	x	x	x	x	x
	З-2	знает источники возникновения информационных угроз												
	З-3	понимает модели и принципы защиты информации от несанкционированного доступа												
	З-4	знает методы антивирусной защиты информации												
	З-5	демонстрирует знания состава и методов организационно-правовой защиты информации												
	У-1	умеет применять организационные, правовые, технические и программные средства защиты информации												
	У-2	создает программные средства защиты информации												
	В-1	владеет навыками определения требований и состава средств, методов и мероприятий по организации комплекса средств защиты информации в компьютерных технологиях												
	В-2	владеет навыками практического применения технических, программных и программно-аппаратных средств и методов защиты информации в компьютерных технологиях												

Приложение 2

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине, входящей в состав рабочей программы дисциплины **Информационная безопасность**

Направление подготовки **38.03.05 (080500) Бизнес-информатика**
Профиль **Информационный бизнес**
Квалификация (степень) **Бакалавр**
Утверждена **21 декабря 2015 г.**

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

Региональный финансово-экономический институт при формировании компетенций студентов направления подготовки 38.03.05 (080500) «Бизнес-информатика» выделяет три этапа формирования компетенции:

- **начальный**. На этом этапе формируются знаниевые и инструментальные основы компетенции, осваиваются основные категории, формируются базовые умения. В целом, знания и умения носят репродуктивный характер. Студент воспроизводит термины, факты, методы, понятия, принципы и правила. На этом этапе он решает задачи, преимущественно, по образцу. Если студент удовлетворительно отвечает этим требованиям, можно говорить об освоении им базового (начального) уровня компетенции;
- **основной** этап – знания, умения, навыки, обеспечивающие формирование компетенции, значительно возрастают, но ещё не достигают целевых (итоговых) значений. На этом этапе студент осваивает действия с предметными знаниями в конкретной дисциплине и, часто, в междисциплинарном характере действий. Способен самостоятельно решать учебные задачи, внося коррективы в алгоритм своих действий, осуществлять саморегуляцию в ходе работы, переносить знания и умения на новые, возникающие в ходе выполнения работ, условия. Успешное прохождение этого этапа позволяет достичь удовлетворительного уровня сформированности компетенции;
- **завершающий** этап – на этом этапе студент достигает итоговых (целевых) показателей по заявленной компетенции. Он осваивает весь необходимый объём знаний, овладевает всеми умениями и навыками в сфере заявленной компетенции. Он способен использовать эти знания, умения и навыки при решении реальных задач и в нестандартных учебных условиях.

Дисциплина имеет целью участие в формировании следующих компетенций (список в соответствии с РУП направления подготовки, составленным в соответствии с государственным стандартом на направление подготовки 080500, утверждён ПРИКАЗОМ от 14 января 2010 г. N 27 «ОБ УТВЕРЖДЕНИИ И ВВЕДЕНИИ В ДЕЙСТВИЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 080500 БИЗНЕС-ИНФОРМАТИКА (КВАЛИФИКАЦИЯ (СТЕПЕНЬ) "БАКАЛАВР"», зарегистрировано в Минюсте РФ 27 февраля 2010 г. N 16524):

1. ОК-1
2. ОК-5
3. ОК-11
4. ОК-12
5. ОК-13
6. ОК-16
7. ОК-17
8. ПК-2
9. ПК-5
10. ПК-19
11. ПК-20
12. ПК-28

Этапы формирования компетенций обычно распределены следующим образом:

13. **Начальный** – формируется в процессе изучения отдельных разделов дисциплины, а успешность его освоения определяется с помощью критериев оценивания компетенции, подробно описанной в разделе [2] этого документа.
14. **Основной** – формируется на этапе успешного завершения всех дисциплин, участвующих в процессе формирования компетенции.
15. **Завершающий** – достигается на основании комплексной междисциплинарной работы, в ходе итоговых практик, экзаменов, выполнении дипломной работы и подтверждении успешного овладения компетенцией.

Завершение дисциплины с точки зрения показателей раздела [2] означает успешное освоение как минимум начального уровня овладения компетенцией.

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

Контроль достижения целевых критериев на этапе текущего формирования компетенции при изучении любых дисциплин направления подготовки

осуществляется на основании следующих инструментов (средств оценивания):

1. индивидуальные задания расчётного типа;
2. индивидуальные задания графического типа;
3. индивидуальные задания вербального типа;
4. индивидуальные задания расчётно-графического типа;
5. индивидуальные темы рефератов по заданной теме;
6. индивидуальные темы эссе по заданной теме;
7. индивидуальные задания для выполнения контрольных работ;
8. тесты в ЭИОС по темам дисциплины:
    a. базовый уровень
    b. высокий уровень
    c. повышенный уровень
9. задания для выполнения лабораторных работ;
10. вопросы для защиты лабораторных работ;
11. задания для подготовки и защиты докладов;
12. сценарии ролевых игр;
13. сценарии мастер-классов;
14. задания для выполнения курсовых работ (проектов);
15. задания для выполнения научно-исследовательских работ;
16. задания для прохождения практик;
17. вопросы к экзамену;
18. вопросы к государственному экзамену;
19. задания для выполнения выпускных квалификационных работ.

Основными типами промежуточного контроля являются тестирования вербального и невербального типов в ЭИОС РФЭИ.

Эти тесты различаются по характеру стимульного материала.

В вербальных типах заданий основным содержанием работы испытуемых являются операции с понятиями, мыслительные действия, осуществляемые в словеснологической форме. Составляющие эти методики задания апеллируют к памяти, воображению, мышлению в их опосредованной языковой форме. Они очень чувствительны к различиям в языковой культуре, уровню образования, профессиональным особенностям. Вербальный тип заданий наиболее распространён в компетентностных тестах, тестах достижений, при оценке специальных способностей. Невербальные тесты — это такой тип методик, в которых тестовый материал представлен в наглядной форме (в виде картинок, чертежей, графических изображений и т. п.). От испытуемых требуется понимание вербальных инструкций, само же выполнение заданий опирается на перцептивные и моторные функции.

Невербальные тесты уменьшают влияние языковых различий на результат испытания. Они также облегчают процедуру тестирования испытуемых с нарушением речи, слуха или с умеренным уровнем подготовки. Невербальные

тесты широко используются при оценке начального этапа формирования компетенции.

Программа изучения дисциплины составлена таким образом, что успешное её освоение возможно с различными результатами. Все задания разделены на обязательные и необязательные. Успешное выполнение всех обязательных заданий означает достижение удовлетворительного уровня по освоению дисциплины.

Количество обязательных заданий текущего контроля не менее 65% от общего количества заданий. Все обязательные задания предполагают возможность повторного выполнения (как автоматически, так и в ряде случаев по согласованию/дополнительному разрешению). Успешное выполнение всех обязательных заданий гарантирует студенту оценку «удовлетворительно» в зачётной книжке, если изучение этой дисциплины предполагает выставление оценки.

Необязательный уровень включает задания высокой и повышенной (относительно высокой) сложности. Их успешное выполнение необязательно для студента, однако их выполнение непосредственно влияет на оценку по дисциплине, а также более глубокий уровень освоения предметной областью дисциплины. Успешное завершение всех заданий высокой сложности предполагает получение оценки «хорошо», а повышенной сложности «отлично» при оценивании результатов освоения дисциплины.

Текущий подход является формализованным для всех дисциплин направления подготовки «Бизнес-информатика» и **обязателен к применению в рамках текущей дисциплины**.

В связи с различиями в части применения дисциплины на разных формах обучения и конкретных профилях здесь приводится полные сведения о способе формирования оценки.

1. Если по дисциплине в РУПе не предусмотрен промежуточный контроль (в РУПе по дисциплине указан только ОДИН итоговый экзамен)

Накопленная оценка по дисциплине рассчитывается с помощью взвешенной суммы оценок за отдельные формы текущего контроля знаний следующим образом:

$О_{накопленная}=n_1 О_{текущий1} + n_2 \cdot О_{текущий\ 2} + n_3 \cdot О_{текущий\ 3} + \ldots + n_i \cdot О_{текущий\ i,}$ где

$О_{текущий1}$ – оценка за текущее компьютерное тестирование (базовый, минимальный уровень)

$О_{текущий2}$ – оценка за текущее компьютерное тестирование (высокий уровень освоения)

$О_{текущий3}$ – оценка за текущее компьютерное тестирование (повышенной сложности)

$О_{текущий4}$ – оценка за эссе

…

$О_{текущий\ i}$ – оценка за реферат, доклад и т.п.

$n_1, n_2, n_3 \ldots n_i$ - веса оценок за отдельные формы текущего контроля ($О_{текущий1,}$

$O_{текущий2}$, $O_{текущий3}$.... $O_{текущий\ i}$)
n_1=**0.6**, n_2=**0.2**, n_3=**0.1** n_4=**0.1**
Сумма весов оценок за отдельные формы текущего контроля, которые учитываются в накопленной оценке, должна быть равна единице (нормализуются):
$\sum n_i = 1$
Способ округления накопленной оценки текущего контроля: **в пользу студента.**
Результирующая оценка по дисциплине (которая пойдёт в диплом и является критерием оц) рассчитывается следующим образом:
$O_{результ} = k_1 \cdot O_{накопл} + k_2 \cdot O_{экз}$, где
$O_{накопл}$ – накопленная оценка по дисциплине
$O_{экз}$ – оценка за экзамен
k_1 – вес накопленной оценки по дисциплине
k_2 – вес экзаменационной оценки по дисциплине
Сумма весов ($k_1 + k_2$) должна быть равна единице: $\sum k_i = 1$, при этом, $0{,}2 \le k_1 \le 0{,}8$. Вес итоговой аттестации не может быть менее 20% от всей дисцпилины.
Для текущей дисциплины $\boldsymbol{k_1 = 0{,}8}$
Способ округления экзаменационной и результирующей оценок: среднее арифметическое.
2. Если по дисциплине в РУПе предусмотрен промежуточный контроль (в РУПе по дисциплине указано БОЛЕЕ одного экзамена)
Итоговая накопленная оценка по дисциплине рассчитывается следующим образом:

$O_{накопленная\ Итоговая} = (O_{промежуточная\ 1} + O_{промежуточная\ 2} + \ldots + O_{накопленная\ i})$:на число этапов,

$O_{промежуточная\ 1}$ – промежуточная оценка 1 этапа/модуля
$O_{промежуточная\ 1} = m_1 \cdot O_{накопленная\ 1\ этапа} + m_2 \cdot O_{промежуточный\ экзамен\ 1\ этапа}$
Сумма весов ($m_1 + m_2$) должна быть равна единице, при этом, $0{,}2 \le m_1 \le 0{,}8$
$O_{промежуточная\ 2}$ – промежуточная оценка 2 этапа/модуля
$O_{промежуточная\ 2} = m_3 \cdot O_{накопленная\ 2\ этапа} + m_4 \cdot O_{промежуточный\ экзамен\ 2\ этапа}$
Сумма весов ($m_3 + m_4$) должна быть равна единице, при этом, $0{,}2 \le m_3 \le 0{,}8$
$O_{накопленная\ 1\ этапа}$, $O_{накопленная\ 2\ этапа}$ рассчитываются по приведенной выше формуле расчета накопленной оценки (за каждый этап)

$O_{накопленная\ i}$ – накопленная оценка последнего этапа/модуля перед итоговым экзаменом

$O_{накопленная\ i}$ рассчитывается по приведённой выше формуле расчёта накопленной оценки **(для последнего этапа/модуля перед итоговым экзаменом)**
Результирующая оценка по дисциплине (которая идёт в диплом и является одним из критериев оценивания достижения основного этапа освоения компетенции) рассчитывается следующим образом:
$O_{результ} = k_1 \cdot O_{накопленная\ Итоговая} + k_2 \cdot O_{Итоговый\ экз}$

$O_{Итоговый\ экз}$ – оценка за **итоговый** экзамен
Сумма весов ($k_1 + k_2$) должна быть равна единице: $\sum k_i = 1$, при этом, $0{,}2 \leq k_1 \leq 0{,}8$
Способ округления накопленных, промежуточных, экзаменационных и результирующей оценок: **среднее арифметическое**

3. Типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной деятельности.

В соответствии с описанием показателей и критериев оценивания, подробно описанные в пункте 2 этого документа, здесь приводится неполный список **примеров** тестовых заданий.
См. приложение 3.1 «Типовые контрольные задания», являющееся частью рабочей программы дисциплины.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующие этапы формирования компетенций

Система текущего контроля успеваемости и промежуточной аттестации студентов предусматривает решение следующих задач:

- оценка качества освоения студентами основной профессиональной образовательной программы (оцениваются знания, умения и навыки);
- аттестация студентов на соответствие их персональных достижений поэтапным требованиям соответствующей основной профессиональной образовательной программы;
- поддержание постоянной обратной связи и принятие оптимальных решений в управлении качеством обучения студентов на уровне преподавателя, кафедры, факультета и института целиком.

Текущий контроль успеваемости и промежуточная аттестация является основным механизмом оценки качества подготовки студентов (согласно требованиям ФГОС) и формой контроля учебной работы студентов.
Оценка качества подготовки студентов осуществляется в двух основных направлениях: оценка уровня освоения дисциплины и оценка компетенций студентов. Предметом оценивания являются знания, умения, компетенции обучающихся.
Промежуточная аттестация студентов проводится по учебной дисциплине в сроки, предусмотренные учебными планами и годовыми календарными учебными графиками в порядке, утверждённом в вузе.
Каждая компетенция формируется на всех этапах обучения студента в процессе изучения ряда дисциплин, а после, использования междисциплинарных знания для выполнения дипломной работы и практик.

Знания, умения и навыки постепенно формируют целевую компетенцию. Поэтому существенно отличаются и методы контроля промежуточной и итоговой оценки достижения компетенций.

Промежуточные методы контроля включают в себя автоматические и неавтоматические методы контроля, такие как тестирование или аттестация/не аттестация по выполнению требуемых видов работ.

С целью определения уровня овладения компетенциями, в заданные логикой преподавания дисциплины сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося. Все виды текущего контроля осуществляются в соответствии с формой задания (см. п.2 «описание показателей и критериев оценивания…»).

Процедура оценивания компетенций обучающихся основана на следующих условиях:

1. Периодичность проведения оценки (минимум 1 раз на каждую рассматриваемую тему в дисциплине).
2. Многоступенчатость: оценка (как автоматически с помощью ЭИОС или преподавателем) и самооценка обучающегося, обсуждение результатов и комплекс мер по устранению недостатков.
3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.

5. Показатели и критерии оценивания сформированности компетенций

Основным критерием итоговой сформированности любой компетенции является успешное завершение обучения студентом, выполнение и защита дипломной работы и государственного экзамена, прохождение и защита практик.

Успешное завершение дисциплины означает достижение очередного шага в формировании компетенции. Критерием успешного завершения дисциплины является как минимум выполнение всех обязательных требований (заданий) из перечня в пункте 2 этого документа. Критерии успешного завершения каждого из заданий определяются в самих заданиях. Примеры заданий можно посмотреть в п.3 этого документа.

Шкалы оценивания предусматривают детальный ответ на вопрос об уровне освоения дисциплины и, посредством оценивания процедур знаний, умений и навыков, показателей оценивания сформированности компетенции.

Общие понятия и определения.

Проверка знаний. Общие понятия и определения.

Общая группа

Ценность информации определяется

- коммерческой тайной
- степенью скретности
- степенью ее полезности для владельца

Как регулируется порядок защиты государственной тайны в РФ?

- Федеральным законом “О коммерческой тайне”
- Уровнем защиты информации и прав субъектов в области информационных процессов и информатизации
- Законом РФ «О государственной тайне» и законом «Об информации, информатизации и защите информации»
- Не регулируется вообще

Что понимают под безопасностью информации в компьютерной системе?

- ○ Разделение привилегий на доступ к информации из числа допущенных к ней должностных лиц
- ○ состояние устойчивости данных к случайным или преднамеренным воздействиям, исключающее недопустимые риски их уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя
- ○ некоторую физически замкнутую преграду вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
- ○ установление подлинности, заключающееся в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает

Какие из перечисленных пунктов не являются средствами обеспечения информационной безопасности?

- ☐ антивирусные системы
- ☐ системы шифрования информации
- ☐ системы журналирования и мониторинга трафика
- ☐ системы контроля доступа
- ☐ системы электронно-цифровой подписи

Способ преобразования текстового сообщения в защищенную форму называется

- ○ шифром
- ○ шифрованием
- ○ криптограммой

Используя Шифр Виженера и русский алфавит (А-Я строчными буквами без пробелов) зашифруйте сообщение `ОБУЧЕНИЕ` с ключом `СТУДЕНТ`. Получится криптограмма вида:

- ○ АУЧЬТАЪЧ
- ○ АУЖЫЙЫЫЦ
- ○ СУЖЫЙЫЫЦ
- ○ Нет верного ответа

Дана следующая криптограмма, полученная с помощью шифра Виженера: `ТЙЪКБЕДЙАЦЕШ` и ключ `СЕТЬ`. Расшифруйте криптограмму используя русский алфавит А-Я, без пробелов.

- ○ БЕЗВРЕМЕННЫЙ
- ○ БЕЗОПАСНОСТЬ
- ○ БЫСТРОТЕЧНЫЙ

Выберите верные утверждения:

- ☐ числа 32 и −10 сравнимы по модулю 7
- ☐ если числа сравнимы по модулю m, то каждое из них делится на m без остатка
- ☐ числа 32 и −10 сравнимы по модулю 5
- ☐ если разность двух чисел делится на m, по эти числа сравнимы по модулю m.
- ☐ если числа сравнимы по модулю m, то их разность делится на модуль m
- ☐ числа 32 и 39 сравнимы по модулю 7

Верно ли утверждение о том, что шифр Вернама не раскрываем?

- ○ Не верно
- ○ Верно

Сопоставьте термины и их значения.

Шифр	преобразование исходного секретного сообщения с целью его защиты
Шифр	преобразование информации, в котором отсутствует ключ
Шифр	преобразование шифрованного сообщения в читаемую информацию
Шифр	методы преобразования информации с целью ее защиты

Современная криптография и государственные стандарты

Проверка знаний. Современная криптография и государственные стандарты

Общая группа

Выберите верные утверждения:

- ☐ DES был признан не надежным, потому что был окончательно скомпрометирован
- ☐ Правительство США признало алгоритм DES ненадежным и в настоящее время его не использует
- ☐ DES является наиболее широко признанным механизмом криптографической защиты данных, составляющих государственную тайну
- ☐ Стандарт шифрования данных, DES является государственным стандартом США

Разложите на простые множители следующие числа:

108	2·2·3·3·3
77	2·2·3·3·3
65	2·2·3·3·3
30	2·2·3·3·3
159	2·2·3·3·3

Определите, какие из пар чисел взаимно просты.

- ☐ (25,12)
- ☐ (40, 27)
- ☐ (25,15)
- ☐ (13,39)

Вычислите 3·8·5 по модулю 11

- ○ 3·8·5=2·5=10 (mod11)
- ○ 3·8·5=4·5=0 (mod11)
- ○ 3 · 8 · 5 = 2 (mod11)

Завершите утверждение корректно

Электронная подпись предназначена для [идентификации] лица, подписавшего электронный документ, и [является] полноценной заменой собственноручной подписи (в случаях, предусмотренных законом)

Пусть в некоторой сети передается зашифрованная информация. При шифровании был использован протокол RSA. Злоумышленник перехватил все сообщения и всю открытую информацию. Сможет ли он расшифровать и найти исходное сообщение?

- ○ Возможно, при условии наличия мощного вычислительного оборудования
- ○ Сможет при известных p и q
- ○ Не сможет в силу криптосойкости алгоритма
- ○ Возможно, в зависимости от значений p и q, при больших занчениях расшифровка будет не возможной, при малых значениях злоумышлинник найдет исходный текст.

Рассмотрите следующую ситуацию

> Абонент А в некоторой сети передает сообщение абоненту В, используя открытую информацию В и алгоритм шифрования RSA. Злоумышленник не может читать сообщения для В, однако, он может передать сообщение для В от лица А.

Что может сделать абонент А для того чтобы избежать этого случая?

- ○ Использовать более сложный метод шифрования или выбрать другой алгоритм
- ○ Подписать сообщение с помощью ЭЦП
- ○ Выбрать числа p и q на столько большими, на сколько это возможно

Постройте подпись RSA для сообщения m при следующих параметрах пользователя:

$$P = 5, Q = 11, c = 27, m = 7$$

- ○ 30
- ○ 26
- ○ 28

Для указанных открытых данных пользователя RSA проверьте подлинность подписанных сообщений. Выберите какие из сообщений являются подлинными.

$$N = 55, d = 3 : (7, 28), (22, 15)(16, 36)$$

- ☐ (22,15)
- ☐ (16,36)
- ☐ (7,28)

Для указанных открытых данных пользователя RSA проверьте подлинность подписанных сообщений. Выберите какие из сообщений являются подлинными.

$$N = 91, d = 5 : (15, 71), (11, 46), (16, 74)$$

- ☐ (11,46)
- ☐ (15,71)
- ☐ (16,74)

Вычислите открытые ключи Y_A, Y_B и общий ключ Z_{AB} для системы Диффи-Хеллмана с параметрами:

$$\mathrm{p} = 23, g = 5, \mathrm{X_A} = 5, \mathrm{X}_B = 7$$

- ○ $Y_A = 21, Y_B = 17, Z_{AB} = 20$
- ○ $Y_A = 20, Y_B = 17, Z_{AB} = 21$
- ○ $Y_A = 13, Y_B = 14, Z_{AB} = 10$

Найдите значение функции Эйлера $\phi(14)$.

- ○ 8
- ○ 4
- ○ 6

Для шифра Эль-Гамаля вычислите недостающие параметры d_B, r, e, m' при следующих заданных:

$$p = 19, g = 2, c_B = 5, k = 7, m = 5,$$

- ○ $d_B = 8, r = 5, e = 5, m' = 10.$
- ○ $d_B = 13, r = 14, e = 12, m' = 5$
- ○ $d_B = 16, r = 9, e = 15, m' = 10.$

Реализация криптографических алгоритмов

Проверка знаний. Реализация криптографических алгоритмов

Общая группа

Почему схему электронных платежей, которая базируется на так называемой «слепой подписи» не рекомендуется использовать на практике?

- ○ никто не знает, кому соответствует такая банкнота
- ○ не сохранена анонимность
- ○ подпись банка не секретна и известна всем
- ○ можно сфабриковать фальшивую банкноту, если известны хотя бы две настоящие

Есть независимо действующие покупатели, которые не помнят номеров ранее использованных ими банкнот, могут ли они случайно сгенерировать две или более банкноты с одинаковыми номерами, при условии что используемые в протоколе, выбпанные в качестве номеров банкнот 1024 бит?

- ○ вероятность получения когда либо двух одинаковых номеров при заданных условиях пренебрежимо мала
- ○ в представленной схеме существует большая доля вероятности получения двух одинаковых номеров
- ○ покупатели могут случайно сгенерировать две или более банкноты с одинаковыми номерами, банк примет к оплате только одну из таких банкнот

В системе электронных денег выбраны секретные параметры банка:

$P = 17, Q = 7, c = 77$, а соответствующие им открытые параметы $N = 119, d = 5$. Сформируйте электронные банкноты со следующими номерами:

$n = 11$ при $r = 5$:

- $\bar{n} = 103, \bar{s} = 52, r^{-1} = 24$, банкнота ⟨11,58⟩
- $\bar{n} = 13, \bar{s} = 13, r^{-1} = 20$, банкнота ⟨99,22⟩
- $\bar{n} = 13, \bar{s} = 52, r^{-1} = 25$, банкнота ⟨11,44⟩

$n = 99$ при $r = 6$:

- $\bar{n} = 13, \bar{s} = 13, r^{-1} = 20$, банкнота ⟨99,22⟩
- $\bar{n} = 13, \bar{s} = 52, r^{-1} = 25$, банкнота ⟨11,44⟩
- $\bar{n} = 103, \bar{s} = 52, r^{-1} = 24$, банкнота ⟨11,58⟩

Для протолкала взаимной аутентификации существует проблема передачи секретного ключа. Секретный ключ, который формируют абоненты A и B, будет всегда один и тот же, пока они не поменяют открытые ключи. Как следует поступить в подобной ситуации?

- произвести смену открытых ключей
- создавать каждый раз различные, случайно выбираемые секретные ключи
- использовать какой-либо шифр с открытым ключом для передачи секретных ключей

В процессе создания электронной банкноты при выборе односторонней функции следует использовать:

- криптографичесие хеш-функции
- любую одностороннюю функцию, проверив на выполнение свойств мультипликативности
- любую несекретную функцию f, таким образом, что f^{-1} легко вычислима

Защита информации в стандарте GSM

Проверка знаний. Защита информации в стандарте GSM

Общая группа

Что представляет собой Сота GSM-сети?

- область, накрываемая сетью GSM
- зона радио охвата одной или нескольких базовых станций, в пределах которой осуществляется прием и передача на фиксированном количестве частот
- стандарт цифровой мобильной сотовой связи, с разделением каналов по времени и частоте

Абонент покупает новый мобильный телефон. Производит первое включение. Какой тип временного международного идентификационного номера буде присвоен абоненту в первую очередь?

- IMSI
- BTS
- TMSI
- MSC

Как изменится ситуация, в случае, если аутентификация проводится не в первый раз? Абоненту будет присвоен:

- MSC
- IMSI
- TMSI
- BTS

Алгоритм аутентификации A3, осуществляется в несколько этапов. Расставьте в верном порядки этапы алгоритма.

- Отклик пересылается базовой станции
- начинается шифрование информации
- базовая станция формирует случайное число RAND
- делается вывод об успешности аутентификации
- базовая станция сравнивает свое значение отклика с полученным значением
- мобильная станция формирует входное значение для хэш-функции
- хеш-функци формирует выходное значение
- число RAND передается на мобильную станцию

Завершите утверждения корректно

Телефонный разговор в формате стандарта GSM передается в виде [последовательности кадров]. Каждый [кадр] передаваемой информации фактически шифруется [своим] ключом шифрования.

Выберите верные утверждения:

☐ Разговор шифруется только на этапе передачи информации между мобильной станцией MS и базовой приемопередающей станцией BTS

☐ Разговор шифруется на всех этапах работы с информацией

☐ Последовательный номер кадра является открытой информацией и может быть использован для расшифровывания разговора

☐ Для установки режима шифрования BTS передает мобильной станции команду на переход в режим шифрования

☐ Номер кадра является секретной и нформацией и передается в зашифрованном виде

Защита информации в телекоммуникационных системах стандартов UMTS и CDMA2000

Проверка знаний. Защита информации в телекоммуникационных системах

Общая группа

В чем отличие механизма аутентификации в стандартах UMTS и CDMA?

- ☐ возможности использования в стандарте CDMA2000 как встроенного, так и съемного модуля идентичности абонента
- ☐ алгоритмы безопасности CDMA2000 полностью стандартизированы, в то время как в стандарте UMTS лишь частично
- ☐ Процедуры аутентификации построены по разным алгоритмам, в CDMA алгоритмы аутентификации и ключевого соглашения реализуются в виде стандартизированной встроенной функции, что гарантирует возможность использования мобильной станции при смене оператора
- ☐ Прцедуры аутентификации полностью идентичны за исключением необязательных дополнений
- ☐ наличие алгоритма аутентификации UIM и функции генерирования ключа аутентификации UIM

Какой шифр для защиты информации используется в телекоммуникационной системе стандарта UMTS?

- DES
- ГОСТ
- KASUMI
- RSA
- MISTY1

Как обеспечивается целостность передаваемых данных в стандарте UMTS?

- алгоритмом шифрования, предназначенным для обеспечения конфиденциальности данных, передаваемых между домашней средой и сетью обслуживани
- алгоритмом целостности, предназначенныим для обеспечения контроля целостности данных на участке «домашняя среда — сеть обслуживания»
- стандартный алгоритм к UIA1, стандартная функция целостности f9 реализованная на базе блочного шифра KASUMI
- через идентификатор алгоритма целостности

Как обеспечивается целостность передаваемых данных в стандарте CDMA2000?

- с помощью алгоритма целостности, предназначенного для обеспечения контроля целостности данных на участке «домашняя среда — сеть обслуживания»
- с помощью усовершенствованного алгоритма обеспечения целостности HMAC
- с помощью вычисляения кода аутентификации сообщения MAC (Message Authentication Code), отвечающиего также за защиту сведений от преднамеренной модификации

Расставьте в верном порядке шаги процесса аутентификации в стандарте UMTS:

- передача вектора аутентификации от домашней среды в сеть обслуживания
- установка подлинности
- передача IMSN
- взаимное установления подлинности между модулем идентичности абонента и телекоммуникационной сетью
- модуль идентичности абонента USIM проверяет подлинность сети
- в сети обслуживания сравниваются значения содержащиеся в векторе аутентификации