Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор
_____ Т.Р. Змызгова
«31» августа 2022 г.

Рабочая программа учебной дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

образовательной программы высшего образования –
программы бакалавриата

46.03.02 - Документоведение и архивоведение

Направленность:
Документоведение и документационное обеспечение управления

Формы обучения: очная, заочная

Курган 2022

Рабочая программа дисциплины «Информационная безопасность и защита информации» составлена в соответствии с учебным планом по программе бакалавриата Документоведение и архивоведение (Документоведение и документационное обеспечение управления), утвержденным:
для очной формы обучения «30» 08 2022 года.
для заочной формы обучения «30» 08 2022 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «29» 08 2022, протокол № 1.

Рабочую программу составил
ст. преподаватель А.В. Человечкова

Согласовано:

Заведующий кафедрой «БИАС»
канд. тех. наук, доцент Д.И. Дик

Заведующий кафедрой
«История и документоведение» Т.В. Козельчук

Начальник управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической работе
Учебно-методического отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Очная форма обучения

Всего: 5 зачетных единицы трудоемкости (180 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		7
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**78**	**78**
Лекции	26	26
Практические занятия	52	52
Самостоятельная работа, всего часов в том числе:	**102**	**102**
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (самостоятельное изучение тем (разделов) дисциплины)	75	75
Вид промежуточной аттестации	**Экзамен**	**Экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**180**	**180**

Заочная форма обучения

Всего: 5 зачетных единицы трудоемкости (180 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		10
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**38**	**38**
Лекции	20	20
Практические занятия	18	18
Самостоятельная работа, всего часов в том числе:	**142**	**142**
Контрольная работа	18	18
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (самостоятельное изучение тем (разделов) дисциплины)	97	97
Вид промежуточной аттестации	**Экзамен**	**Экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**180**	**180**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность и защита информации» относится к обязательной части Блока1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- Информационные технологии.

Знания, умения и навыки, полученные при освоении дисциплины «Информационная безопасность и защита информации», являются необходимыми для освоения последующих дисциплин: «Конфиденциальное делопроизводство», а также при выполнении выпускной квалификационной работы.

Требования к входным знаниям, умениям, навыкам и компетенциям:

Студент должен знать: основные принципы устройства и функционирования ЭВМ; способен применять к решению прикладных задач базовые алгоритмы обработки информации; основные методы, способы и средства получения, хранения, переработки информации, готов работать с компьютером как средством управления информацией.

Студент должен уметь: использовать фундаментальные понятия информатики; выбирать программные средства для кодирования и сжатия информации.

Студент должен владеть: теоретическими знаниями и навыками применения современных средств обработки данных, методами представления, сбора и обработки информации.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью освоения дисциплины «Информационная безопасность и защита информации» является: усвоение теоретических знаний, практических умений и навыков в области защиты информации, овладение компетенциями по квалифицированному применению на практике профессиональной терминологии, по классификации защищаемой информации средств и систем её защиты, проведению целенаправленного поиска в различных источниках информации по защите информации, в том числе в глобальных компьютерных системах.

Задачами освоения дисциплины «Информационная безопасность и защита информации» являются ознакомление с источниками информации в области защиты информации, в том числе с ресурсами в сети Интернет, современными проблемами защиты информации; изучение средств защиты информации на объектах информатизации, общих принципов построения и функционирования систем обеспечения информационной безопасности.

Компетенции, формируемые в результате освоения дисциплины:

– Способен находить организационно-управленческие решения при решении задач в сфере своей профессиональной деятельности (ОПК-2);

– Способен использовать базовые знания в области информационно-

коммуникационных технологий в сфере своей профессиональной деятельности; (ОПК-4);

– Способен работать с документами, содержащими информацию ограниченного доступа, применяя современные методы её защиты (ПК-22).

В результате изучения дисциплины обучающийся должен:

– знать концепцию защиты информации, конституционные и законодательные основы ее реализации; информационно-правовые аспекты безопасности информационных ресурсов (для ОПК-2);

– знать способы ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты (для ОПК-4).

– уметь применять навыки работы с документами, содержащими информацию ограниченного доступа (для ПК-22);

– владеть нормативно-правовыми документами, международными и отечественными стандартами в области информационных систем и технологий (для ОПК-2);

– владеть методами защиты информации (для ОПК-4);

– владеть навыками работы с документами, содержащими информацию ограниченного доступа (для ПК-22).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план

Очная форма обучения

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
			Лекции	Практич. занятия
Рубеж 1	1	Криптографические методы защиты информации. Основные понятия шифрования.	2	-
	2	Симметричные методы шифрования. Методы замены (подстановок). Моноалфавитные методы шифрования.	2	12
	3	Полиалфавитные методы шифрования.	2	8
		Рубежный контроль № 1	-	2
Рубеж 2	4	Полиграммные методы шифрования.	2	12
	5	Методы перестановок.	2	8
	6	Криптоанализ.	2	4
	7	Асимметричные системы с открытым ключом. Электронная цифровая подпись	4	4
	8	Основные понятия и положения защиты информации в компьютерных системах	2	-
	9	Классификация угроз безопасности. Распространенные угрозы безопасности.	4	-

	10	Правовое регулирование защиты информации в России. Стандарты информационной безопасности.	4	-
		Рубежный контроль № 2	-	2
		Всего:	**26**	**52**

Заочная форма

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
			Лекции	**Практич. занятия**
Рубеж 1	1	Криптографические методы защиты информации. Основные понятия шифрования.	2	-
	2	Симметричные методы шифрования. Методы замены (подстановок). Моноалфавитные методы шифрования.	2	4
	3	Полиалфавитные методы шифрования.	2	4
Рубеж 2	4	Полиграммные методы шифрования.	2	4
	5	Методы перестановок.	2	2
	6	Криптоанализ.	2	2
	7	Асимметричные системы с открытым ключом. Электронная цифровая подпись	2	2
	8	Основные понятия и положения защиты информации в компьютерных системах	2	-
	9	Классификация угроз безопасности. Распространенные угрозы безопасности.	2	-
	10	Правовое регулирование защиты информации в России. Стандарты информационной безопасности.	2	-
		Всего:	**20**	**18**

4.2. Содержание лекционных занятий

Тема 1. Криптографические методы защиты информации. Основные понятия шифрования.

Основные понятия криптографии. Классификация методов криптографического преобразования информации. Основные понятия шифрования. Понятия криптосистем.

Тема 2. Симметричные методы шифрования. Методы замены (подстановок). Моноалфавитные методы шифрования.

Сущность методов замены (подстановки). Шифрование методами Цезаря, Цезаря с ключевым словом, Атбаш, квадрата Полибия, аффинная система шифрования Цезаря, Трисемуса.

Тема 3. Полиалфавитные методы шифрования.

Сущность полиалфавитных методов шифрования. Шифр Вижинера, Гронсфельда.

Тема 4. Полиграммные методы шифрования.

Сущность полиграммных шифров замены. Шифр Плейфера. Сущность аналитических методов шифрования. Шифр на использовании матричной алгебры. Алгоритм шифрования и расшифрования методом «Двойной квадрат Уитстона».

Тема 5. Методы перестановок.

Сущность методов перестановки. Примеры простейших перестановок. Метод шифрования, основанный на применении маршрутов Гамильтона.

Тема 6. Проблемная лекция. Криптоанализ.

Основные понятия криптоанализа. Начальные условия криптоанализа. Метод частотного анализа на примере шифра Цезаря.

Тема 7. Асимметричные системы с открытым ключом. Электронная цифровая подпись.

Математические основы шифрования с открытым ключом. Понятие асимметричной криптосистемы, односторонних функции. Криптосистема RSA, Эль Гамаля, PGP (Pretty Good Privacy).Понятие электронной цифровой подписи (ЭЦП). Разновидности ЭЦП. Принцип работы ЭЦП. Функции хэширования. Алгоритмы шифрования.

Тема 8. Основные понятия и положения защиты информации в компьютерных системах.

Понятие, особенности, свойства информации. Предмет и объект защиты информации.

Тема 9. Классификация угроз безопасности. Распространенные угрозы безопасности.

Понятие угроз безопасности. Классификация возможных угроз информационной безопасности автоматизированных систем (АС) по базовым признакам. Случайные и преднамеренные угрозы. Характеристика распространенных угроз безопасности АС. Основные виды угроз АС. Основные методы реализации угроз информационной безопасности.

Тема 10. Правовое регулирование защиты информации в России. Стандарты информационной безопасности. Российские стандарты безопасности информационных технологий.

Конституция РФ. Федеральный закон «Об информации, информатизации и защите информации». Законодательство в области защиты государственной тайны в РФ. Роль органов государственной власти РФ в создании правовых механизмов защиты информации. Роль стандартов информационной безопасности. Международный стандарт ISO/IEC 17799:2000 (BS 77991:2000) «Информационные технологии – Управление информационной безопасностью». Германский стандарт BSI. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий». Российские стандарты, регулирующие информационную безопасность. Стандарт «Критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408.

4.3. Практические занятия

Номер раздела, темы	Наименование раздела, темы	Наименование практических занятий	Норматив времени, час.	
			Очная форма	Заочная
2	Симметричные методы шифрования. Методы замены (подстановок). Моноалфавитные методы шифрования.	Методы шифрования Цезаря, Атбаш, квадрата Полибия.	4	1
		Методы шифрования Цезаря с ключевым словом.	2	1
		Аффинная система шифрования Цезаря	2	1
		Метод шифрования Трисемуса	4	1
3	Полиалфавитные методы шифрования.	Шифр Вижинера	4	4
		Шифр Гронсфельда	4	-
Рубежный контроль № 1			2	-
4	Полиграммные методы шифрования.	Шифр Плейфера.	4	2
		Шифр с использованием методов матричной алгебры.	4	2
		«Двойной квадрат Уитстона».	4	-
5	Методы перестановок.	Метод перестановок, основанный на применении маршрутов Гамильтона.	8	2
6	Криптоанализ.	Криптоанализ методом частотного анализа	4	2
7	Асимметричные системы с открытым ключом. Электронная цифровая подпись	Криптосистема RSA	4	2
Рубежный контроль № 2			2	-
Всего:			**52**	**18**

4.4 Контрольная работа для заочной формы обучения

В процессе выполнения контрольной работы у студентов формируются навыки ведения самостоятельной работы. Контрольные задания способствуют более углубленному изучению основ дисциплины и повышению теоретической и профессиональной подготовки студентов. Написание контрольной работы способствует лучшему усвоению материала.

Студент выбирает одну из предложенных преподавателем тем, самостоятельно готовит презентацию работы и выносит ее на обсуждение на занятии.

Результат выполнения контрольной работы оформляется в виде пояснительной записки, объемом 15-20 страниц, которая содержит:

- титульный лист;
- содержание;
- введение;

- основную часть отчета;
- заключение;
- список использованных источников;
- приложения.

При оформлении контрольной работы студент должен руководствоваться методическими указаниями к оформлению текстовой документации для студентов. По результатам проверки представленной студентом контрольной работы преподаватель принимает решение о допуске ее к защите или возвращает студенту на доработку в соответствии с отмеченными замечаниями.

Тематика контрольных работ

1. Виды криптографической защиты: стеганография, кодирование, сжатие.
2. Методы криптографической защиты (Российские и зарубежные). Распространение и применение.
3. Сертифицированные криптографические средства защиты информации в России.
4. Виды симметричного шифрования. Принципы их действия. Плюсы и минусы.
5. Моноалфавитные методы шифрования.
6. Полиалфавитные методы шифрования.
7. Полиграммные методы шифрования.
8. Криптоанализ. Методы и способы реализации для поточных алгоритмов шифрования.
9. Методы и способы реализации криптоанализа для блочных алгоритмов шифрования.
10. Сравнение и анализ Российских и зарубежных ассиеметричных (потоковых) алгоритмов шифрования.
11. Сравнение и анализ Российских и зарубежных ассиеметричных (блочных) алгоритмов шифрования.
12. Криптографическая система. Виды криптографических систем.
13. Криптостойкость алгоритмов. Способы и методы повышения.
14. ЭЦП. Типы ЭЦП. Удостоверяющие центры и цифровые сертификаты.
15. Классификация угроз безопасности. Объекты и субъекты ЗИ.
16. Базовая модель угроз. Построение модели угроз. Модель нарушителя.
17. Угрозы безопасности информации в ПК. Случайные угрозы (примеры и последствия).
18. Угрозы безопасности информации в ПК. Преднамеренные угрозы (примеры и последствия).
19. Правовое регулирование ЗИ в России. Права и обязанности субъектов ЗИ.

20. Стандарты информационной безопасности. Сравнительный анализ Российских и зарубежных стандартов

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность и защита информации» преподается в течение одного семестра в виде лекционных и практических занятий, на которых происходит объяснение, усвоение, проверка материала.

На лекционных занятиях рекомендуется использование иллюстративного материала (текстовой, графической и цифровой информации), мультимедийных форм презентаций.

При прослушивании лекций рекомендуется в конспекте отмечать важные моменты, которые направлены на качественное выполнение практических занятий.

Залогом качественного выполнения практических занятий является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале практического занятия.

В преподавании дисциплины применяются образовательные технологии: метод проблемного изложения материала; самостоятельное ознакомление студентов с источниками информации, использование иллюстративных материалов (фотографии, компьютерные презентации), демонстрируемых на современном оборудовании, общение в интерактивном режиме.

Самостоятельная работа студента, наряду с практическими аудиторными занятиями в группе выполняется (при непосредственном или опосредованном контроле преподавателя) по учебникам и учебным пособиям, оригинальной современной литературе по профилю.

Рубежные контроли проходят в форме беседы по вопросам и выполнения заданий по вариантам (примерный список вопрос и заданий приведен в п. 6.4).

Практические работы выполняются с использованием программного продукта Microsoft Office Excel. Рекомендуется повторить навыки использования указанной программы.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к практическим занятиям, к рубежным контролям (для очной форм обучения), выполнение контрольной

работы (для заочной формы обучения) и подготовку к экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	**Рекомендуемая трудоемкость, акад. час.**	
	Очная форма обучения	**Заочная форма обучения**
Самостоятельное изучение тем дисциплины:	**47**	**88**
Основные понятия шифрования. Понятия криптосистем.	6	11
Понятие, особенности, свойства информации. Предмет и объект защиты информации.	5	11
Основные виды угроз АС. Основные методы реализации угроз информационной безопасности.	6	11
Законы в сфере информационной безопасности.	6	11
Стандарты информационной безопасности.	6	11
Понятие национальной безопасности	6	11
Государственная информационная политика. Информационная война. Информационное оружие	6	11
Каналы утечки информации Классификация каналов утечки информации.	6	11
Подготовка к практическим занятиям (по 1 часу на каждое занятие)	**24**	**9**
Подготовка к рубежным контролям (по 2 часа на каждый рубеж)	**4**	**-**
Контрольная работа	**-**	**18**
Подготовка к экзамену	**27**	**27**
Всего:	**102**	**142**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ (для очной формы обучения).
2. Отчеты студентов по практическим занятиям.
3. Банк заданий к рубежным контролям № 1, № 2 (для очной формы обучения).
4. Банк вопросов к экзамену.
5. Контрольная работа (для заочной формы обучения).

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

Очная форма обучения

<table>
<tr><td>№</td><td>Наименование</td><td colspan="6">Содержание</td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="6">Распределение баллов для зачета</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение и защита отчетов по практическим занятиям</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>$2_б$ x 13 = $26_б$</td><td>$2,5_б$ x 12 = $30_б$</td><td>7</td><td>7</td><td>30</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и экзамена</td><td colspan="6">60 и менее баллов – неудовлетворительно; не зачтено;
61…73 – удовлетворительно; зачтено;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов</td><td colspan="6">Для допуска к промежуточной аттестации (экзамену) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и выполнить рубежный контроль № 1, 2, выполнить и защитить практические задания.
Для получения «автоматически» экзаменационной оценки «удовлетворительно» студенту необходимо набрать за семестр минимум 68 баллов.
По согласованию с преподавателем студенту, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активное участие на консультациях, оригинальность принятых решений в ходе выполнения практических занятий, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена автоматически оценка «хорошо» или «отлично».</td></tr>
<tr><td>4</td><td>Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра</td><td colspan="6">В случае если к промежуточной аттестации (экзамену) набрана сумма менее 50 баллов, не выполнены все задания, необходимо выполнить дополнительные задания до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических и лабораторных работ.
Формы дополнительных заданий (назначаются преподавателем):
- выполнение и защита пропущенной практической работы (при невозможности дополнительного проведения работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 2,5 баллов. Прохождение рубежных контролей – до 7 баллов за каждый.
Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.</td></tr>
</table>

6.3. Процедура оценивания результатов освоения дисциплины

Рубежный контроль №1 в форме выполнения практической работы. Рубежный контроль №2 в форме самостоятельной работы по теоретическим вопросам.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

На подготовку к ответу студенту отводится время не менее 30 минут.

Преподаватель оценивает выполнение задания на рубежном контроле № 1 № 2 - до 7 баллов для очной формы обучения соответственно. Каждое задание оценивается в 1 балл. Полученные результаты заносит в ведомость учета текущей успеваемости.

Билеты для экзамена состоят из 2 вопросов и практического задания. Ответы на каждый вопрос оценивается до 10 баллов, выполнение практического задания оценивается до 10 баллов. Время, отводимое студенту на подготовку к ответу на экзаменационный билет, составляет 1 астрономический час.

Результаты текущего контроля успеваемости и экзамена заносятся преподавателем в экзаменационную ведомость, которые сдается в организационный отдел института в день экзамена, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей и экзамена

Примерный список вопросов к экзамену:

1. Основные понятия защиты информации.
2. Основные понятия информационной безопасности.
3. Классификация угроз информационной безопасности.
4. Случайные и преднамеренные угрозы.
5. Распространенные угрозы безопасности.
6. Основные виды угроз АС.
7. Основные методы реализации угроз информационной безопасности.
8. Стандарты безопасности. Роль стандартов информационной безопасности.
9. Классификация методов криптографического преобразования информации.
10. Основные понятия шифрования.
11. Криптосистемы. Основные понятия крпиптосистем.
12. Основные понятия и методы криптоанализа.
13. Методы шифрования Цезаря, Атбаша, квадрата Полибии.
14. Шифрование методом Цезаря с ключевым словом.
15. Аффинная система шифрования.
16. Шифрование по методу Трисемуса.
17. Полиграммные шифры. Шифр Плейфера.
18. Полиграммные шифры. Метод шифрования, основанный на использовании матричной алгебры.

19. Шифр Виженера.
20. Двойной квадрат Уитстона (шифр Уитстона).
21. Метод шифрования Гронсфельда.
22. Метод шифрования «Маршруты Гамильтона».
23. Асимметричные криптосистемы. Пример.
24. Классы удаленных угроз и их характеристика.
25. Принципы построения защищенных вычислительных сетей.

Примерные вопросы для рубежных контролей

Рубежный контроль №1:

1. Используя метод шифрования ПЛЕЙФЕРА с ключом k="ЧИСЛО" расшифровать текст АВЫГЕЫЧА (матрица составляется размером 4x8).

2. Методом двойного квадрата Уитстона зашифровать слово РЕСУРСЫ с ключами k1= ТАИНА, к2=ЧИСЛО.

3. Зашифровать исходный текст: <МЕТОДЫ_ШИФРОВАНИЯ_С_СИММЕТРИЧНЫМ_КЛЮЧОМ>, используя метод перестановки (маршруты Гамильтона).

Ключ: К=<1,2,1>. Для шифрования используются следующие таблица и два маршрута:

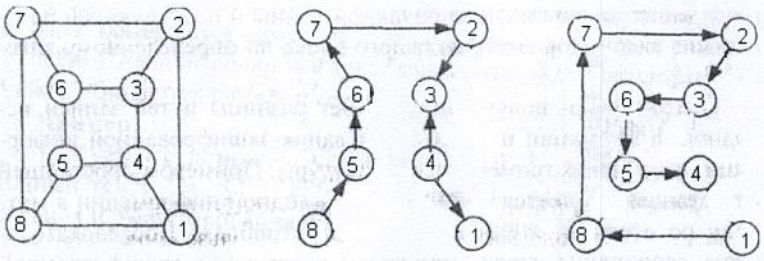

Таблица Маршрут № 1 Маршрут № 2

Рубежный контроль №2:

1. Что понимается под защитой информации?
2. Что относится к конфиденциальным данным?
3. Что такое политика безопасности?
4. В чем состоит главная задача стандартов информационной безопасности?
5. Перечислите основные международные стандарты информационной безопасности.
6. На какие классы разделены угроз безопасности информации в компьютерной системе?
7. Что понимается под случайными угрозами?
8. Что понимается под преднамеренными угрозами?
9. Что такое удаленная угроза?
10. Какие существуют меры обеспечения информационной безопасности?

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и

промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности. [Электронный ресурс]: Учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84с. – URL: http://window.edu.ru/catalog/pdf2txt/669/63669/33948.

2. Камышев Э.Н. Информационная безопасность и защита информации. [Электронный ресурс]: Учебное пособие. - Томск: ТПУ, 2009. - 95 с. – URL: http://window.edu.ru/catalog/pdf2txt/033/75033/55482.

3. Макаренко С. И. Информационная безопасность. [Электронный ресурс]: Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил. – URL: http://window.edu.ru/catalog/pdf2txt/775/77775/58783.

7.2. Дополнительная учебная литература

1. Математические основы криптографии. Теория сравнений и ее приложения [Электронный ресурс]: методические указания и контрольные задания по дисциплине «Криптографические методы защиты информации» для студентов специальности 090303.65 и направления 231000.62 / Министерство образования и науки Российской Федерации, Курганский государственный университет, Кафедра "Безопасность информационных и автоматизированных систем"; [сост.: Т.Р. Змызгова]. - Электрон. текстовые дан. (тип файла: pdf ; размер: 368 Kb). - Курган: Издательство Курганского государственного университета, 2014. - 29 с.: табл. - Библиогр.: с. 29. – Доступ из ЭСБ КГУ

2. Нестеров С. А. Информационная безопасность и защита информации. [Электронный ресурс]: Учебное пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с. – URL: http://window.edu.ru/catalog/pdf2txt/462/67462/48880.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

1. Методы шифрования [Электронный ресурс]: методические рекомендации для студентов направлений 230700.62, 09.03.03, 050100.62, 44.03.01 / Министерство образования и науки Российской Федерации, Курганский государственный университет, Кафедра информационных технологий и методики преподавания информатики; [сост.: О.А. Сидорова]. - Электрон. текстовые дан. (тип файла: pdf ; размер: 526 Kb). - Курган: Издательство Курганского государственного университета, 2016. - 39, [1] с.: рис., табл. - Библиогр.: с. 39. – Доступ из ЭСБ КГУ

9. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. it.kgsu.ru - Сайт кафедры ИТ и МПИ «Шаг за шагом»
2. protect.htmlweb.ru/ - Защита информации в компьютерных системах
3. http://crypto.hut2.ru/crypto.php - Раздел сайта "Информационная безопасность и криптография"

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows 7/10, Microsoft PowePoint 2010.

Для организации практических занятий используется Microsoft Excel,.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Компьютерный класс, мультимедийное оборудование (переносной персональный компьютер, мультимедийный проектор, мультимедийный экран).

12. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Информационная безопасность и защита информации»

образовательной программы высшего образования – программы бакалавриата

46.03.02 - Документоведение и архивоведение

Направленность:
Документоведение и документационное обеспечение управления

Трудоемкость дисциплины: 5 ЗЕ (180 академических часа)
Семестр: 7 (очная форма обучения), 10 (заочная форма обучения)
Форма промежуточной аттестации: Экзамен
Форма обучения: очная, заочная.

Содержание дисциплины

Криптографические методы защиты информации; основные понятия шифрования; классификация методов криптографической защиты информации; шифрование; стандарты информационной безопасности; классификация угроз безопасности; распространенные угрозы безопасности; основные понятия и положения защиты информации в компьютерных системах; правовое регулирование защиты информации в России.