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/
«30» сентября 2021 г.

Рабочая программа учебной дисциплины

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

образовательной программы высшего образования –
программы бакалавриата
09.03.03 Прикладная информатика
Направленность «Интеллектуальные информационные системы и технологии»
Форма обучения: очная, заочная

Курган 2021

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с учебным планом по программе бакалавриата «Прикладная информатика» (Интеллектуальные информационные системы и технологии) для очной и заочной форм обучения «30» августа 2021 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 сентября 2021 года, протокол № 2.

Рабочую программу составил:
старший преподаватель А.В Человечкова

Согласовано:

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

Заведующий кафедрой «ПОАС»
канд. тех. наук, доцент В.К. Волк

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

Начальник управления
образовательной деятельности С.Н. Синицын

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 4 зачетных единицы трудоемкости (144 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		4
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**48**	**48**
Лекции	32	32
Лабораторные работы	16	16
Практические занятия	-	-
Аудиторные занятия в интерактивной форме, часов	-	-
Самостоятельная работа, всего часов в том числе:	**96**	**96**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю)	60	60
Контрольная работа	18	18
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**144**	**144**

Заочная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		6
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**14**	**14**
Лекции	6	6
Лабораторные работы	2	2
Практические занятия	6	6
Аудиторные занятия в интерактивной форме, часов	-	-
Самостоятельная работа, всего часов в том числе:	**130**	**130**
Подготовка к зачету	27	27
Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю)	85	85
Контрольная работа	18	18
Вид промежуточной аттестации	**экзамен**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**144**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы информационной безопасности» относится обязательной части блока 1.

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

- Информатика.
- Объектно-ориентированное программирование.
- Введение в специальность.

Изучение дисциплины должно способствовать обеспечению будущего специалиста комплексом знаний, навыков и умений, которые позволят участвовать ему в развитии и поддержке стратегии развития предприятий и организаций, а практические навыки, полученные из курса «Основы информационной безопасности», будут использованы студентами при изучении других дисциплин профессионального цикла, а также при разработке курсовых и дипломных работ.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Основной целью курса является ознакомление студентов с современным состоянием проблемы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации в организациях и на предприятиях различных направлений деятельности и различных форм собственности, способов защиты от несанкционированного доступа к ней, рассмотреть на современном уровне вопросы разработки средств и систем сбора и защиты информации.

Задачами дисциплины являются: ознакомление с терминологией информационной безопасности; дать основы обеспечения информационной безопасности личности, общества, государства; методологии создания систем защиты информации; методов и средств ведения информационных войн; оценки защищенности и обеспечения информационной безопасности автоматизированных систем.

Компетенции, формируемые в результате освоения дисциплины:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3).

В результате изучения дисциплины обучающийся должен:

знать:

- сущность и понятие информации, информационной безопасности и характеристику её составляющих (для ОПК-3);
- место и роль информационной безопасности в системе национальной безопасности РФ, основы государственной информационной политики, стратегию развития информационного общества в России (для ОПК-3);

уметь:

- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации (для ОПК-3);
- анализировать и оценивать угрозы информационной безопасности объекта (для ОПК-3);

владеть:

- профессиональной терминологией в области информационной безопасности (для ОПК-3);
- навыками безопасного использования технических средств в профессиональной деятельности (для ОПК-3);
- методами оценки информационных рисков (для ОПК-3).

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	Лабораторные занятия
Рубеж 1	1	***Основы безопасности автоматизированных систем***	***16***	***6***
		Актуальность проблемы обеспечения безопасности автоматизированных систем (АС)	2	-
		Основные понятия в области безопасности автоматизированных систем	2	1
		Угрозы безопасности автоматизированных систем	4	1
		Меры и основные принципы обеспечения безопасности	2	1
		Правовые основы обеспечения автоматизированных систем	4	1
		Государственная система защита информации	2	-
		Рубежный контроль №1	-	2
Рубеж 2	2	***Обеспечение безопасности автоматизированных систем***	***10***	***6***
		Организационная структура системы обеспечения безопасности АС	4	1
		Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях	2	-
		Регламентация работ по обеспечению безопасности автоматизированных систем	2	1
		Категорирование и документирование защищенных ресурсов	1	1
		Концепция информационной безопасности. Планы защиты и	1	1

		обеспечения непрерывной работы и восстановления подсистем АС.		
		Рубежный контроль №1	-	2
Рубеж 3	3	***Средства защиты информации от несанкционированного доступа***	***6***	***4***
		Назначение и возможности средств защиты информации от несанкционированного доступа	2	1
		Аппаратно-программные средства защиты информации от несанкционированного доступа.	2	1
		Применение штатных и дополнительных средств защиты информации от несанкционированного доступа.	2	2
		Всего	**32**	**16**

Заочная форма обучения

Рубеж	**Номер раздела, темы**	**Наименование раздела, темы**	Количество часов контактной работы с преподавателем		
			Лекции	Лабораторные занятия	Практические занятия
Рубеж 1	1	***Основы безопасности автоматизированных систем***	***2***	***2***	***2***
		Актуальность проблемы обеспечения безопасности автоматизированных систем (АС)	-	-	-
		Основные понятия в области безопасности автоматизированных систем	-	-	-
		Угрозы безопасности автоматизированных систем	-	2	-
		Меры и основные принципы обеспечения безопасности	1	-	-
		Правовые основы обеспечения автоматизированных систем	-	-	2
		Государственная система защита информации	1	-	-
Рубеж 2	2	***Обеспечение безопасности автоматизированных систем***	***2***	-	***2***
		Организационная структура системы обеспечения безопасности АС	2	-	-
		Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях	-	-	2
		Регламентация работ по обеспечению безопасности автоматизированных систем	-	-	-
		Категорирование и документирование	-	-	-

		защищенных ресурсов			
		Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем АС.	-	-	-
Рубеж 3	3	***Средства защиты информации от несанкционированного доступа***	***2***	**-**	***2***
		Назначение и возможности средств защиты информации от несанкционированного доступа	2	-	-
		Аппаратно-программные средства защиты информации от несанкционированного доступа.	-	-	2
		Применение штатных и дополнительных средств защиты информации от несанкционированного доступа.	-	-	-
		Всего	**6**	**2**	**6**

4.2. Содержание лекционных занятий

1. Основы безопасности автоматизированных систем.

Актуальность проблемы обеспечения безопасности автоматизированных систем (АС). Место и роль автоматизированных систем в управлении бизнес-процессами. Обострение проблемы обеспечения безопасности автоматизированных систем (АС) на современном этапе. Защита АС как процесс управления рисками. Методы оценки целесообразности затрат на обеспечение безопасности. Особенности современных АС как объектов защиты.

Основные понятия в области автоматизированных систем. Определение безопасности АС. Информация и информационные ресурсы. Субъекты информационных систем, их безопасность. Цель защиты автоматизированной системы и циркулирующей в ней информации.

Угрозы безопасности автоматизированных систем. Уязвимость основ-ных структурно-функциональных элементов распределенных АС. Угрозы безопасности информации, АС и субъектов информационных отношений.

Классификация угроз безопасности.

Классификация каналов проникновения в АС и утечки информации. Неформальная модель нарушителя.

Меры и основные принципы обеспечения безопасности АС. Виды мер противодействия угрозам безопасности. Принципы построения системы обеспечения безопасности информации в АС.

Правовые основы обеспечения безопасности АС. Защищаемая информация. Лицензирование. Сертификация средств защиты информации и аттестация объектов информатизации. Специальные требования и рекомендации по технической защите конфиденциальной информации. Юридическая значимость электронных документов с электронной подписью. Ответственность за нарушения в сфере защиты информации.

Государственная система защиты информации. Главные направления работ по защите информации. Структура государственной системы защиты информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации. Финансирование мероприятий по защите информации.

2. Обеспечение безопасности автоматизированных систем.

Организационная структура системы обеспечения безопасности АС. Технология управления безопасностью информации и ресурсов в АС. Институт ответственных за обеспечение информационной безопасности. Регламентация действий пользователей и обслуживающего персонала АС. Политика безопасности организации. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты. Распределение функций по обеспечению безопасности АС. Организационно-распорядительные документы по обеспечению безопасности АС.

Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях. Проблема человеческого фактора. Общие правила обеспечения безопасности. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения требований обеспечения безопасности. Порядок работы с носителями ключевой информации.

Регламентация работ по обеспечению безопасности автоматизированных систем. Регламентация правил парольной и антивирусной защиты. Регламентация порядка допуска к работе и изменения полномочий пользователей АС. Регламентация порядка изменения конфигурации аппаратно-программных средств АС. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.

Категорирование и документирование защищенных ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов.

Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем АС. Концепция информационной безопасности организации. План защиты информации. План обеспечения непрерывной работы и восстановления подсистем АС.

3. Средства защиты информации от несанкционированного доступа.

Назначение и возможности средств защиты информации от несанкционированного доступа. Основные механизмы защиты АС. Защита периметра компьютерных сетей и управление механизмами защиты. Страхование информационных рисков.

Аппаратно-программные средства защиты информации от несанкционированного доступа. Рекомендации по выбору средств защиты информации от несанкционированного доступа. Обзор существующих на рынке средств защиты информации от несанкционированного доступа. Средства аппаратной поддержки. Способы аутентификации.

Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. Стратегия безопасности Microsoft. Защита от вмешательства в процессе нормального функционирования АС. Разграничение доступа зарегистрированных пользователей к ресурсам АС. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.

4.3. Лабораторные занятия

Номер раздела	Наименование раздела, темы	Наименование тем лабораторных занятий	Норматив времени, час.	
			очная	заочная
1	Основы безопасности автоматизированных систем	*Лабораторное занятие №1.* Основные понятия в области безопасности автоматизированных систем. Угрозы безопасности автоматизированных систем.	2	-
		Лабораторное занятие. Угрозы безопасности автоматизированных систем.	-	2
		Лабораторное занятие №2. Меры и основные принципы обеспечения безопасности. Правовые основы обеспечения автоматизированных систем.	2	-
		Рубежный контроль №1. Тестирование.	2	-
2	Обеспечение безопасности автоматизированных систем	*Лабораторное занятие №3.* Организационная структура системы обеспечения безопасности АС. Регламентация работ по обеспечению безопасности автоматизированных систем.	2	-
		Лабораторное занятие №4. Категорирование и документирование защищенных ресурсов. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем АС.	2	-
		Рубежный контроль №2. Тестирование.	2	-
3	Средства защиты информации от несанкционированного доступа	*Лабораторное занятие №5.* Назначение и возможности средств защиты информации от несанкционированного доступа. Аппаратно-программные средства защиты информации от несанкционированного доступа.	2	-
		Лабораторное занятие №6. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа.	2	-
	Итого		**16**	**2**

4.4. Практические занятия (для заочной формы обучения)

Номер раздела	Наименование раздела, темы	Наименование тем практических занятий	Норматив времени, час.
			заочная
1	Основы безопасности автоматизированных систем	*Практическое занятие №1.* Правовые основы обеспечения автоматизированных систем.	2
2	Обеспечение безопасности автоматизированных систем	*Практическое занятие №2.* Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях .	2
3	Средства защиты информации от несанкционирован-ного доступа	*Практическое занятие №3.* Аппаратно-программные средства защиты информации от несанкционированного доступа.	2
	Итого		**6**

4.5. Контрольная работа для очной и заочной форм 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 работу 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.

Титульный лист работы представлен в Приложении 1. 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.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работы (и практической работы для заочной формы обучения).

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале работы.

Преподавателем запланировано применение на лабораторных занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

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 лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам и к рубежным контролям (для очной формы обучения), лабораторно-практическим занятиям (для заочной формы обучения), выполнение контрольной работы, подготовку к зачету (для очной формы обучения) и к экзамену (для заочной формы обучения).

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.	
	очная	заочная
Подготовка к лабораторным работам (по 2 часа на каждое занятие)	16	2
Подготовка к практическим занятиям (по 2 часа на каждое занятие)	-	6
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4	-
Подготовка к зачету, экзамену	18	27
Выполнение контрольной работы	18	18
Другие виды самостоятельной работы	**40**	**77**

(подготовка к занятиям)		
1. Основы безопасности автоматизированных систем	10	25
2. Обеспечение безопасности автоматизированных систем	15	25
3. Средства защиты информации от несанкционированного доступа	15	27
Всего:	**96**	**130**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ 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 лабораторным работам.

3. Банк тестовых заданий к рубежным контролям № 1, № 2 (для очной формы обучения).

4. Контрольная работа для очной и заочной форм обучения.

5. Вопросы к зачету (для очной формы обучения).

6. Вопросы к экзамену (для заочной формы обучения).

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание						
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов						
		Вид учебной работы:	Посещение лекций	Выполнение лабораторной работы	Контрольная работа	Рубежный контроль №1	Рубежный контроль №2	Зачет
		Балльная оценка:	$1_б$ x 16 = $16_б$	$4_б$ x 8 = $32_б$	10	6	6	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично						

3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (зачету) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные работы и контрольную работу. Для получения на зачете «зачтено» «автоматически» студенту необходимо набрать 61 балл. По согласованию с преподавателем студенту, набравшему минимум баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на лекционных и лабораторных занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях и выставлено «зачтено» автоматически.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение пропущенной лабораторной работы (при невозможности дополнительного проведения лабораторной работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 3 баллов; прохождение рубежного контроля – до 5 баллов; выполнение письменной работы по теме, предложенной преподавателем – до 10 баллов. Ликвидация академических задолженностей, контрольной работы, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 24 вопросов. На каждое тестирование при рубежном контроле студенту отводится 2 академических часа.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответа на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

Экзамен проводится в устной форме. Студенты должны ответить на два вопроса билета, каждый из которых оценивается в 15 баллов. Перечень экзаменационных вопросов выдается для подготовки заранее. Время, отводимое на подготовку вопросов составляет 1 астрономический час.

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

6.4. Примеры оценочных средств для рубежных контролей, зачета и экзамена

1-ый рубежный контроль

1. Активный перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

2. Как называется способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то?

1. «За дураком»; 2. «Брешь»; 3. «Компьютерный абордаж»;
4. «За хвост»; 5. «Неспешный выбор».

3. Защита информации – это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

2-ой рубежный контроль

1. Защита информации от разглашения – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

2. Носитель информации – это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;

5. участник правоотношений в информационных процессах.

3. Троянские программы, скрытно осуществляющие анонимный доступ к различным Интернет-ресурсам, обычно используются для рассылки спама:

1. Trojan-PSW; 2. Trojan-Spy; 3. Trojan-Proxy;

4. Trojan-Downloader; 5. Trojan-Dropper.

Примерные темы контрольных работ

1. Основы и цели политики безопасности в компьютерных сетях. Многоуровневая защиты корпоративных сетей.
2. Методы организации антивирусной защиты компьютерных систем

3. Анализ методов и средств защиты от несанкционированного копирования и использования программ.
4. Анализ методов гарантированного удаления конфиденциальной информации на электронных носителях.
5. Компьютерная стеганография.
6. Анализ современного законодательства в области защиты персональных данных.
7. Информационное противоборство.
8. Современные методы и средства аутентификации.
9. Кибербезопасность и киберпреступники.
10. Информационные войны и средства информационного противоборства.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ (ДЛЯ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ)

1. Актуальность проблемы обеспечения безопасности автоматизированных систем (АС). Место и роль автоматизированных систем в управлении бизнес-процессами.
2. Защита АС как процесс управления рисками. Особенности современных АС как объектов защиты.
3. Угрозы безопасности автоматизированных систем.
4. Уязвимость основных структурно-функциональных элементов распределенных АС.
5. Угрозы безопасности информации, АС и субъектов информационных отношений.
6. Классификация угроз безопасности.
7. Классификация каналов проникновения в АС и утечки информации.
8. Неформальная модель нарушителя.
9. Меры и основные принципы обеспечения безопасности АС.
10. Виды мер противодействия угрозам безопасности.
11. Принципы построения системы обеспечения безопасности информации в АС.
12. Правовые основы обеспечения безопасности АС.
13. Защищаемая информация. Лицензирование. Сертификация средств защиты информации и аттестация объектов информатизации.
14. Специальные требования и рекомендации по технической защите конфиденциальной информации.
15. Юридическая значимость электронных документов с электронной подписью. Ответственность за нарушения в сфере защиты информации.
16. Государственная система защиты информации.
17. Организация защиты информации в системах и средствах информатизации и связи.
18. Организационная структура системы обеспечения безопасности АС.
19. Технология управления безопасностью информации и ресурсов в АС.
20. Регламентация действий пользователей и обслуживающего персонала АС.

21. Политика безопасности организации.
22. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
23. Распределение функций по обеспечению безопасности АС.
24. Организационно-распорядительные документы по обеспечению безопасности АС.
25. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях.
26. Обязанности ответственного за обеспечение безопасности информации в подразделении.
27. Ответственность за нарушения требований обеспечения безопасности.
28. Порядок работы с носителями ключевой информации.
29. Регламентация работ по обеспечению безопасности автоматизированных систем.
30. Регламентация правил парольной и антивирусной защиты.
31. Регламентация порядка допуска к работе и изменения полномочий пользователей АС.
32. Регламентация порядка изменения конфигурации аппаратно-программных средств АС.
33. План защиты информации.
34. Назначение и возможности средств защиты информации от несанкционированного доступа.
35. Основные механизмы защиты АС.
36. Защита периметра компьютерных сетей и управление механизмами защиты. Страхование информационных рисков.
37. Аппаратно-программные средства защиты информации от несанкционированного доступа.
38. Средства аппаратной поддержки.
39. Способы аутентификации.
40. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. Разграничение доступа зарегистрированных пользователей к ресурсам АС.
41. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа.
42. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (ДЛЯ ЗАОЧНОЙ ФОРМЫ ОБУЧЕНИЯ)

1. Информация как объект защиты. Конфиденциальность, целостность и доступность информации.
2. Модели ценности информации. Информационный поток.
3. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).
4. Угрозы. Классификация угроз безопасности.

5. Модели угроз и модель нарушителя.
6. Утечки информации. Каналы утечек информации.
7. Классификация каналов утечек информации.
8. Основные направления обеспечения компьютерной безопасности.
9. Основные уровни защиты информации.
10. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.
11. Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации.
12. Стеганографические методы защиты.
13. Контроль целостности информации на МНИ.
14. Цифровая подпись.
15. Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак.
16. Средства реализации атак.
17. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
18. Технологии обнаружения компьютерных атак и их возможности.
19. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).
20. Вредоносное программное обеспечение.
21. Компьютерные вирусы. Классификация вирусов.
22. Антивирусное программное обеспечение. Классификация антивирусов.
23. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.
24. Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования.
25. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.
26. Типы межсетевых экранов. Схемы межсетевого экранирования.

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. Мельников В.П. Информационная безопасность и защита информации. Издательский центр «Академия», 2008. – 336 с.

2. Ярочкин В.И. Информационная безопасность.- М.: Академический проект, 2008. – 544 с.

3. Галатенко В.А. Основы информационной безопасности: Курс лекций.- М.: Интернет- Университет Информационных технологий, 2006. – 208 с.

4. Расторгуев С.П. Основы информационной безопасности. Издательский центр «Академия» 2009.

5. Куприянов А.И. Основы защиты информации. Издательский центр «Академия», 2009. – 256 с.

6. Новоструев, А.В., Солодовников, В.М., Терентьева, А.А. Тезаурус в сфере информационной безопасности [Текст]/ А.В. Новоструев, В.М. Солодвников, А.А. Терентьева : Учебное пособие. – Курган: Изд-во Курганского гос. Ун-та, 2014. – 471 с.

7.2 Дополнительная учебная литература:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. М.: Горячая линия-Телеком, 2006.

7.3 Методическая литература

1. Москвин В.В., Полякова Е.Н. Методические указания к выполнению лабораторных работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». Часть 1. РИЦ Курганского государственного университета. 2017.- 52 с.

2. Москвин В.В., Полякова Е.Н. Методические указания к выполнению лабораторных работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». Часть 2. РИЦ Курганского государственного университета. 2017.- 41 с.

7.4 Нормативно-правовое обеспечение дисциплины:

1. Доктрина информационной безопасности Российской Федерации. (утв. Указом Президента РФ 5 декабря 2016 г. №646).

2. Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1.

3. Закон РФ «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

5. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

6. Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ.

7. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 27.10.1994).

8. Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 25.11.1995, приказ №199).

9. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утв. Государственной технической комиссией при Президенте РФ 30.08.2002, приказом №282).

10. ISO/IEC 27001 - 2005 (2013). Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требовавния.

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

1. [Электронный ресурс] Internet Security Glossary, Version 2 (htt:/ /www.ietf.org/rfc/rfc4949.txt)
2. [Электронный ресурс] Behavior of and Requirements for Internet Firewalls (htt:/ /www.ietf.org/rfc/rfc2979.txt)

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Информационно-справочная система «КонсультантПлюс».

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A.

11. 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.

Приложение1

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)
Кафедра «Безопасность информационных и автоматизированных систем»

Контрольная работа по дисциплине
«Основы информационной безопасности»

ТЕМА:

09.03.03 – Прикладная информатика
Направленность «Интеллектуальные информационные системы и технологии»

Выполнил студент группы _____ _____
(подпись) (фамилия, имя, отчество)

Проверил преподаватель _____
(должность, подпись) (фамилия, имя, отчество)

Оценка _____

Курган 20__

ЛИСТ
регистрации изменений (дополнений) в рабочую программу учебной дисциплины «Основы информационной безопасности»

Изменения / дополнения в рабочую программу на 20___ / 20___ учебный год:

_____

_____

_____

_____

_____

_____

Ответственный преподаватель _____ / Человечкова А.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.

Изменения / дополнения в рабочую программу на 20___ / 20___ учебный год:

_____

_____

_____

_____

_____

_____

Ответственный преподаватель _____ / Человечкова А.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.

Аннотация к рабочей программе дисциплины

«Основы информационной безопасности»

образовательной программы высшего образования –
программы бакалавриата

09.03.03 – Прикладная информатика

Направленность:

Интеллектуальные информационные системы и технологии

Трудоемкость дисциплины: 4 з.е. (144 академических часа)

Семестр: 4 (очная форма обучения); 6 заочная форма обучения)

Форма промежуточной аттестации: зачет – очная форма обучения; экзамен – заочная форма обучения.

Содержание дисциплины. Основные разделы

Понятие национальной безопасности. Виды безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации. Основные понятия. Общеметодологические принципы теории информационной безопасности. Анализ угроз информационной безопасности. Проблемы информационной войны. Государственная информационная политика. Проблемы региональной информационной безопасности. Виды информации. Методы и средства обеспечения информационной безопасности. Нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации.