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:
Проректор по образовательной и
международной деятельности
_____ / А.А. Кирсанкин /
«____»_____ 2026 г.

Рабочая программа учебной дисциплины

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Специализация №5: Безопасность открытых информационных систем

Форма обучения: очная

Курган 2026

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным для очной формы обучения 26 июня 2026 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 03 июля 2026 года, протокол № 12.

Рабочую программу составил:
канд.биол.наук А.В Человечкова

Согласовано:

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

Начальник управления
образовательной деятельности И.В. Григоренко

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

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		2
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**64**	**64**
Лекции	32	32
Лабораторные работы	-	-
Практические занятия	32	32
Аудиторные занятия в интерактивной форме, часов	-	-
Самостоятельная работа, всего часов в том числе:	**44**	**44**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю)	26	26
Контрольная работа	-	-
Вид промежуточной аттестации	**зачет с оценкой**	**зачет с оценкой**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы информационной безопасности» относится к обязательным дисциплинам модуля информационная безопасность Блока 1.

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

- Информатика.
- Технологии и методы программирования.
- 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 обучающимися при изучении других дисциплин профессионального цикла, а также при разработке курсовых и дипломных работ.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Основной целью курса является ознакомление обучающихся 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 оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства (ОПК-1).

Индикаторы и дескрипторы части соответствующей компетенции, формируемой в процессе изучения дисциплины «Основы информационной безопасности», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Основы информационной безопасности», индикаторы достижения компетенций ОПК-1, перечень оценочных средств

№ п/п	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование оценочных средств
1.	ИД-1опк-1	Знать: место и роль информационной безопасности в системе национальной безопасности РФ, основы государственной информационной политики, стратегию развития информационного общества в России	З (ИД-1опк-1)	Знает: место и роль информационной безопасности в системе национальной безопасности РФ, основы государственной информационной политики, стратегию развития информационного общества в России	Вопросы теста
2.	ИД-2 опк-1	Уметь: классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	У (ИД-2опк-1)	Умеет: классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	Комплект имитационных задач
3.	ИД-3 опк-1	Владеть: навыками безопасного использования технических средств в профессиональной деятельности, методами формирования требований по защите информации	В (ИД-3опк-1)	Владеет: навыками безопасного использования технических средств в профессиональной деятельности, методами формирования требований по защите информации	Вопросы для сдачи зачета

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	Практичес. занятия
Рубеж 1	1	*Основы безопасности автоматизированных систем*	***16***	***7***
1-ый рубежный контроль		**Тестирование**	-	1
Рубеж 2	2	*Обеспечение безопасности автоматизированных систем*	***10***	***16***
	3	*Средства защиты информации от несанкционированного доступа*	***6***	***7***
2-ой рубежный контроль		**Тестирование**	-	1
		Всего	**32**	**32**

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 основных 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 Практические занятия

Номер раздела	Наименование раздела, темы	Наименование тем практических занятий	Норматив времени, час.
1	Основы безопасности автоматизированных систем	*Практическое занятие №1.* Основные понятия в области безопасности автоматизированных систем	2
		Семинар. Угрозы безопасности автоматизированных систем.	2
		Семинар. Меры и основные принципы обеспечения безопасности. Правовые основы обеспечения автоматизированных систем.	2
		Семинар. Правовые основы обеспечения автоматизированных систем	1
1-ый рубежный контроль		***Тестирование***	**1**
2	Обеспечение безопасности автоматизированных систем	*Практическая занятие №2.* Организационная структура системы обеспечения безопасности АС.	2
		Практическое занятие №3. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях. Регламентация работ по обеспечению безопасности автоматизированных систем.	4
		Практическая работа №4. Категорирование и документирование защищенных ресурсов. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем АС.	4
		Практическая занятие №5. Обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов АС.	2
		Практическая занятие №6. Политика безопасности организации.	1
		Практическая занятие №7 Общие правила обеспечения безопасности.	1
		Практическая занятие №8. Определение требований к защите конкретной информации, её носителей и процессов обработки.	1

		Практическая занятие №9. Лицензирование и сертификация в области защиты информации.	1
3	Средства защиты информации от несанкционированного доступа	*Семинар.* Назначение и возможности средств защиты информации от несанкционированного доступа. Аппаратно-программные средства защиты информации от несанкционированного доступа.	2
		Семинар. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа.	2
		Семинар. Защита периметра компьютерных сетей и управление механизмами защиты.	2
		Семинар. Обзор существующих на рынке средств защиты информации от несанкционированного доступа.	1
2-ой рубежный контроль		***Тестирование***	**1**
		Итого	**32**

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 практической работы.

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

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к практическим работам, к рубежным контролям и подготовку к зачету с оценкой.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем	**8**
Основы безопасности автоматизированных систем Обеспечение безопасности автоматизированных систем Средства защиты информации от несанкционированного доступа	2 3 3
Подготовка к практическим занятиям (по 2 часа на каждое занятие)	16
Подготовка к рубежным контролям (по 1часу на каждый рубежный контроль)	2
Подготовка к зачету с оценкой	18
Всего:	**44**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ.

2.Отчеты по практическим занятиям.

3. Банк тестовых заданий к рубежным контролям № 1, № 2.

4. Вопросы к зачету с оценкой

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

<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 обучающихся на первом учебном занятии)</td><td colspan="6">Распределение баллов</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение практической работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Зачет с оценкой</td></tr>
<tr><td>Балльная оценка:</td><td>$1,5_б$ x 16 = $24_б$</td><td>$2_б$ x 16 = $32_б$</td><td>7</td><td>7</td><td>30</td></tr>
<tr><td>2</td><td colspan="2">Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета</td><td colspan="5">60 и менее баллов – неудовлетворительно; не зачтено;
61…73 – удовлетворительно; зачтено;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td colspan="2">Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов</td><td colspan="5">Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается.
Для получения зачета с оценкой без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность.
Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается.
За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30.
Основанием для получения дополнительных баллов являются:
- выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем;
- участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.</td></tr>
</table>

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету с оценкой) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. 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.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися 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 обучающемуся отводится 2 академических часа.

Баллы обучающемуся 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 обучающегося по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

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

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

6.4. Примеры оценочных средств для рубежных контролей и зачета с оценкой

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.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ С ОЦЕНКОЙ

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.

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. Новоструев А.В. Тезаурус в сфере информационной безопасности [Электронный ресурс]: учебное пособие: [для студентов вузов, обучающихся по направлениям и специальностям в области информационной безопасности] / А.В. Новоструев, В.М. Солодовников, А.А. Терентьева; Министерство образования и науки Российской Федерации, Курганский государственный университет; [науч. ред. Д.И. Дик]. - Электрон. текстовые дан. (тип файла: pdf; размер: 3,86 Mb). - Курган: Издательство Курганского государственного университета, 2014. - 468. – Доступ из ЭСБ КГУ.

8. Стандарты информационной безопасности [Электронный ресурс]: методические указания к практическому занятию для студентов направлений 10.05.03 и 10.03.01 / Министерство науки и высшего образования Российской Федерации, Курганский государственный университет, Кафедра "Безопасность информационных и автоматизированных систем"; [сост.: В.В. Москвин]. - Электрон. текстовые дан. (тип файла: pdf; размер: 840 Kb). - Курган: Издательство Курганского государственного университета, 2018. - 29, [1] с.: рис., табл. - Библиогр.: с. 28-29. – Доступ из ЭСБ КГУ.

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. Требования.

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

1. [Электронный ресурс] Internet Security Glossary, Version 2 (http:/ /www.ietf.org/rfc/rfc4949.txt)
2. [Электронный ресурс] Behavior of and Requirements for Internet Firewalls (http:/ /www.ietf.org/rfc/rfc2979.txt)
3. ЭБС http://www.znanium.com/
4. ЭБС http://www.studentlibrary.ru
5. http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел
6. http://window.edu.ru/. Единое окно доступа к образовательным ресурсам
7. http://elibrary.ru/. Научная электронная библиотека
8. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально- техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

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.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Основы информационной безопасности»

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Специализация №5:

Безопасность открытых информационных систем

Трудоемкость дисциплины: 3 з.е. (108 академических часа)

Семестр: 2 (очная форма обучения)

Форма промежуточной аттестации: зачет с оценкой

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.

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.