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/
«____»_____ 2024 г.

Рабочая программа учебной дисциплины

ВВЕДЕНИЕ В ПРОФЕССИОНАЛЬНУЮ ДЕЯТЕЛЬНОСТЬ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Специализация: (специализация№5) Безопасность открытых информационных систем
Форма обучения: очная

Курган 2024

Рабочая программа дисциплины «Введение в профессиональную деятельность» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» («Безопасность открытых информационных систем»), утвержденным для очной формы обучения «_28_» __июня__ 2024 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 августа 2024 года, протокол № 1

Рабочую программу составил:
канд. пед. наук, доцент Е.Н. Полякова

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: 2 зачетных единицы трудоемкости (72 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		1
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**32**	**32**
Лекции	16	16
Лабораторные работы	-	-
Практические занятия	16	16
Аудиторные занятия в интерактивной форме, часов	-	-
Самостоятельная работа, всего часов в том числе:	**40**	**40**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю)	22	22
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**72**	**72**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Введение в профессиональную деятельность» относится к дисциплинам модуля информационная безопасность Блока 1.

Изучение дисциплины базируется на знаниях, умениях, навыках, приобретенных обучающимися в средней школе.

Освоение данной дисциплины является необходимым при изучении дисциплин всех циклов, а также при прохождении производственной практики, при разработке курсовых и написании выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Цель дисциплины: познакомить обучающихся с основными проблемами информационной безопасности, содействовать освоению основных понятий и категорий данной предметной области.

Основными задачами дисциплины являются:

– формирование общего представления у обучающихся о выбранной ими специальности;

– изучение основной терминологии информационной безопасности;

– изучение основных задач комплексного подхода к защите информации.

Компетенции, формируемые в результате освоения дисциплины:

– способностью 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 «Введение в профессиональную деятельность», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Введение в профессиональную деятельность», 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-1$_{ОПК-1}$	Знать: роль и место информационной безопасности в системе национальной безопасности страны, принятые в обществе морально-нравственные и правовые нормы и принципы профессиональной этики, структуру основной образовательной	З (ИД-1$_{ОПК-1}$)	Знает: роль и место информационной безопасности в системе национальной безопасности страны, принятые в обществе морально-нравственные и правовые нормы и принципы профессиональной этики, структуру основной образовательной про-	Вопросы теста

		программы подготовки специалиста по защите информации и место специальности в области науки и техники		граммы подготовки специалиста по защите информации и место специальности в области науки и техники	
2.	ИД-2 $_{ОПК-1}$	Уметь: исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма, осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики, понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовность и способность к активной состязательной деятельности в условиях информационного противоборства	У (ИД-2$_{ОПК-1}$)	Умеет: исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма, осуществлять свою деятельность в различных сферах общественной жизни с обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики, понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовность и способность к активной состязательной деятельности в условиях информационного противоборства	Комплект имитационных задач
3.	ИД-3 $_{ОПК-1}$	Владеть: профессиональной терминологией в области информационной безопасности, способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности	В (ИД-3$_{ОПК-1}$)	Владеет: профессиональной терминологией в области информационной безопасности, способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности	Вопросы для сдачи зачета

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер раздела	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
			Лекции	Практические занятия
Рубеж 1		Введение	2	2
	1	Общая характеристика специальности.	4	3
	2	Основы обеспечения информационной безопасности.	6	3
Рубеж 2	3	Законодательное регулирование в сфере информационной безопасности.	4	8
		Всего:	**16**	**16**

4.2. Содержание лекционных занятий

Введение.

Организация учебного процесса. Предмет курса, его цели и задачи. Рекомендуемая литература.

1. Общая характеристика специальности.

Общая характеристика специальности «Информационная безопасность автоматизированных систем». Характеристика профессиональной деятельности выпускников, освоивших программу специалитета.

Структура основной образовательной программы подготовки специалиста по защите информации. Содержание основной образовательной программы подготовки специалиста по защите информации. Требования к результатам освоения программы специалитета.

Место специалиста в области науки и техники; объекты профессиональной деятельности специалиста; виды профессиональной деятельности выпускника. Взаимосвязь специальности с другими специальностями в области защиты информации.

2. Основы обеспечения информационной безопасности.

Информационная безопасность в системе национальной безопасности Российской Федерации. Сущность информационной безопасности, ее роль и место в системе национальной безопасности Российской Федерации. Задачи и методы обеспечения информационной безопасности Российской Федерации. Организационные основы системы обеспечения информационной безопасности Российской Федерации.

Основные понятия защиты информации. Угрозы информационной безопасности и каналы утечки информации.

Организационно-правовое обеспечение информационной безопасности. Инженерно-технические методы и средства защиты информации.

Программно-аппаратные методы и средства обеспечения информационной безопасности.

3. Законодательное регулирование в сфере информационной безопасности.

Структура органов государственной власти по обеспечению информационной безопасности в Российской Федерации.

Конституционные нормы о защите информационной сферы.

Федеральное законодательство в сфере информационной безопасности. Основные законы в сфере информационной безопасности.

Уголовный кодекс РФ об ответственности за совершение преступлений в сфере компьютерной информации. Трудовой кодекс РФ об ответственности за разглашение отдельных видов тайн и персональных данных.

4.3 Практические занятия

Номер раздела	Наименование раздела	Наименование тем практических занятий	Норматив времени, час.
	Введение	Структура управления КГУ. Особенности организации образовательного процесса на кафедре «БИАС». Организация труда обучающихся. Права и обязанности обучающихся.	2
1	Общая характеристика специальности.	Федеральный государственный образовательный стандарт (ФГОС ВО). Сущность профиля специальности «Информационная безопасность автоматизированных систем». Виды профессиональной деятельности и требование ФГОС ВО к уровню подготовки специалистов по специальности «Информационная безопасность автоматизированных систем»	1
		Учебный план по специальности «Информационная безопасность автоматизированных систем». Календарный учебный график. Распределение дисциплин по семестрам.	2
2	Основы обеспечения информационной безопасности.	Технология подготовки и оформление результатов самостоятельной учебной и научно-исследовательской работы обучающихся.	1
	1-ый рубежный контроль	***Контрольные вопросы***	***2***
3	Законодательное регулирование в сфере информационной безопасности.	Управление информационной безопасностью на государственном уровне: общие принципы и российская практика.	2
		Информационное воздействие на общество и информационная война.	2
		Доклад и обсуждение рефератов обучающихся	2
	2-ой рубежный контроль	***Защита реферата***	***2***
		Итого	**16**

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 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 и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела	12
Введение	2
Общая характеристика специальности	2
Основы обеспечения информационной безопасности	4
Законодательное регулирование в сфере информационной безопасности	4
Подготовка к практическим занятиям (по 1 часу на занятие)	6
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Подготовка к зачету	18
Всего:	**40**

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 заданий к рубежным контролям №1, 2.

4. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

№	Наименование	Содержание					
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения обучающихся на первом учебном занятии)*	Распределение баллов					
		Вид учебной работы:	Посещение лекций	Выполнение практической работы	Рубежный контроль №1	Рубежый контроль №2	Зачет
		Балльная оценка:	$3_б$ х 8 = $24_б$	$4_б$ х 7 = $28_б$	9	9	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 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 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.

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) 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 ответа на вопросы.

Перед проведением 1-го рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты контрольных вопросов преподаватель выдает на последней лекции по каждой теме. На рубежный контроль обучающемуся отводится 2 академических часа. Каждый из них состоит из 9 вопросов по 1 баллу каждый.

2-ой рубежный контроль проходит в форме защиты реферата. Обсуждение реферата проходит на занятии в присутствии всех обучающихся группы. За активность при обсуждении преподавателем могут быть добавлены дополнительные баллы самым активным обучающимся.

Преподаватель оценивает в баллах результаты ответов каждого обучающегося и заносит в ведомость учета текущей успеваемости.

Зачет 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

Контрольные вопросы для 1-ого рубежного контроля

1. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем».
2. Объекты профессиональной деятельности выпускников.
3. Виды профессиональной деятельности и требование ФГОС ВО к уровню подготовки специалистов по профилю «Информационная безопасность автоматизированных систем»
4. Организация учебного процесса в КГУ. Особенности организации образовательного процесса на кафедре «БИАС».
5. Организация труда обучающихся. Права и обязанности обучающихся.
6. Современный информационный поиск.
7. Основные типы информационно-поисковых задач и алгоритмы их решения.
8. Аналитико-синтетическая переработка информации: сущность, назначение, виды.
9. Интернет: поисковые системы и сервисы.
10. Технология подготовки и оформление результатов самостоятельной учебной и научно-исследовательской работы обучающихся.
11. Основные понятия защиты информации.
12. Требования к комплексным системам защиты информации.
13. Информационная безопасность в компьютерном мире.
14. Понятие компьютерных вирусов.
15. Выполнение разрушительных действий. Последствия работы вируса.
16. Антивирусные программы.

Задание для 2-ого рубежного контроля

По дисциплине «Введение в профессиональную деятельность» обучающиеся готовят реферат по теме, предложенной преподавателем или выбранной самостоятельно, но согласованной с преподавателем. Практические занятия проходят в форме обсуждения рефератов обучающихся. Подготовка реферата позволяет закрепить теоретические знания по дисциплине, приобрести навыки самостоятельного углубленного изучения одного из разделов курса.

При подготовке реферата обучающиеся получают навыки и умение работать с источниками и литературой, анализировать факты и данные специальной литературы, излагать прочитанное современным профессиональным языком.

Реферат должен быть оформлен в соответствии с требованиями, предъявляемыми к подготовке и оформлению научных работ.

Реферат, как и любой документ, пишется и оформляется в соответствии с определенными стандартами, в России — ГОСТов. Объем реферата 20-25 страниц в компьютерном исполнении.

Структура реферата состоит из введения, основной части, заключения, список литературы и приложений.

Введение. Раздел должен содержать постановку проблемы в рамках выбранной научной темы и обоснование выбора проблемы, ее актуальность, новизна.

Во введении дается краткая характеристика изучаемой темы, обосновывается ее актуальность, личная заинтересованность автора в ее исследовании, отмечается практическая значимость изучения данного вопроса, где это может быть использовано. Здесь же называются и конкретные задачи, которые предстоит решить в соответствии с поставленной целью.

Основная часть. В данном разделе должна быть раскрыта тема. В основной части, как правило, разделенной на главы, необходимо раскрыть все пункты составленного плана, связно изложить накопленный и проанализированный материал. Излагается суть проблемы, различные точки зрения на нее, собственная позиция автора реферата. Важно добиться того, чтобы основная идея, выдвинутая во введении, пронизывала всю работу, а весь материал был нацелен на раскрытие главных задач. Каждый раздел основной части должен открываться определенной задачей и заканчиваться краткими выводами.

Заключение. В заключении подводятся итоги по всей работе, суммируются выводы, содержащие ясные ответы на поставленные в цели исследования (иногда с учетом различных точек зрения на изложенную проблему), отмечается то новое, что получено в результате работы над данной темой. Заключение по объему не должно превышать введение.

Примерные темы рефератов:

1. Выдающиеся ученые и их вклад в развитие вычислительной техники и систем информационной безопасности.
2. Защита информационных ресурсов.
3. Инженерно-технические методы и средства защиты информации.
4. Информационная безопасность в банковской сфере. Электронные деньги. Банковские терминалы.
5. История и основные тенденции развития компьютерной техники и систем информационной безопасности.
6. История развития криптографии. Тенденции и перспективы развития криптографии и стеганографии.
7. Методы и средства противодействия угрозам информационной безопасности.
8. Обследование организации на предмет обеспечения информационной безопасности.
9. Организационно-правовое обеспечение информационной безопасности.
10. Основные этапы работы по защите информации.
11. Особенности защиты информации, распространяемой по сетям.
12. Поиск просчетов в организации доступа к информации.

13. Понятие компьютерных вирусов. Выполнение разрушительных действий. Антивирусные программы.

14. Понятие угрозы информационной безопасности и классификация угроз.

15. Правила доступа при работе с информацией.

16. Причины и последствия атак на информацию.

17. Проблема защиты информации и пути ее решения.

18. Программно-аппаратные методы и средства обеспечения информационной безопасности.

19. Роль глобальной сети Internet в современном обществе и особенности ее защиты. Социальные сети.

20. Сетевые технологии: история развития, современные исследования.

21. Современные системы защиты.

22. Спам. Спамеры и хакеры. Ограждение от спама.

23. Средства защиты физических носителей и материальных информационных объектов от кражи, подделки несанкционированного копирования и уничтожения.

24. Требования к комплексным системам защиты информации.

25. Угрозы информационной безопасности и каналы утечки информации.

26. Целостность и эффективность системы защиты информации, её обязательные компоненты.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Антивирусные программы.

2. Выполнение разрушительных действий. Последствия работы вируса.

3. Доктрина информационной безопасности.

4. Задачи и методы обеспечения информационной безопасности Российской Федерации.

5. Инженерно-технические методы и средства защиты информации.

6. Информационная безопасность в системе национальной безопасности Российской Федерации.

7. Конституционные нормы о защите информационной сферы.

8. Конституция РФ.

9. опасности и каналы утечки информации.

10. Организационно-правовое обеспечение информационной безопасности.

11. Организационно-правовое обеспечение информационной безопасности. Инженерно-технические методы и средства защиты информации.

12. Организационные основы системы обеспечения информационной безопасности Российской Федерации.

13. Основные законы в сфере информационной безопасности.

14. Основные понятия защиты информации. Угрозы информационной без

15. Понятие компьютерных вирусов.

16. Программно-аппаратные методы и средства обеспечения информационной безопасности.

17. Программно-аппаратные методы и средства обеспечения информационной безопасности.

18. Структура органов государственной власти по обеспечению информационной безопасности в Российской Федерации.

19. Сущность информационной безопасности, ее роль и место в системе национальной безопасности Российской Федерации.

20. Трудовой кодекс РФ об ответственности за разглашение отдельных видов тайн и персональных данных.

21. Уголовный кодекс РФ об ответственности за совершение преступлений в сфере компьютерной информации.

22. Угрозы информационной безопасности и каналы утечки информации.

23. Федеральное законодательство в сфере 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

Основная учебная литература:

1. Гришина, Н.В. Организация комплексной системы защиты информации [Текст] / Н.В.Гришина - М.: Гелиос АРВ, 2007. – 256с.

2. Запечников, С.В. Информационная безопасность открытых систем. Угрозы безопасности, уязвимости, атаки, подходы к защите [Текст] / С.В. Запечников, Н.Г. Милославская, А.И. Толстой - Т.1 - М.: Горячая линия - Телеком, 2006. – 216с

3. Максимов, Н.В. Современные информационные технологии [Текст] : учебное пособие / Н.В. Максимов, Т.Л Партыка, И.И. Попов - М.: Форум, 2011.-512с.

4. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] : учебное пособие / А.А. Малюк - М.: Горячая линия – Телеком, 2004. – 280с.

5. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.03. «Информационная безопасность автоматизированных систем (уровень специалитета)»: утвержден приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1509. URL: http://www.consultant.ru/document/cons_doc_LAW_209464/43cc57d7e548db1ec458e8b6915c7671ef988682/

6. Хохлов, Г.И. Основы теории информации [Текст]: учебное пособие / Г.И. Хохлов – М. : Издательский центр «Академия», 2008. -171с.

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

7.2 Дополнительная учебная литература:

1. Галатенко, В.А. Стандарты информационной безопасности. Курс лекций. Текст / В.А. Галатенко - М, Интуит, 2006. – 264с.

2. Дик, Д.И. Дипломное проектирование. Текст: методические указания по выполнению выпускной квалификационной работы для студентов направления (специальности) 090000 (090105) / Д.И. Дик – Курган: РИЦ Курганского государственного университета, 2011. – 118 с.

7.3 Методическая литература:

1. Полякова Е.Н. Методические указания для самостоятельной работы по дисциплине «Введение в специальность» для студентов очной формы обучения специальности 10.05.03 «Информационная безопасность автоматизированных систем». РИЦ Курганского государственного университета. 2017. – 20 с.

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

1) http://www.intuit.ru - Интернет-Университет Информационных Технологий;

2) http://www.edu.ru - Федеральный портал «Российское образование» - содержит различные федеральные образовательные ресурсы;

3) http://window.edu.ru – единое окно доступа к федеральным образовательным ресурсам;

4) http://www.fstec.ru – сайт Федеральной службы по техническому и экспортному контролю России. (ФСТЭК России).

5) http://www.counsultant.ru - справочная правовая система «Консультант Плюс»;

6) http://www.garant.ru – справочная правовая система «Гарант».

7) http://минобрнауки.рф/ Министерство образования и науки Российской Федерации.

8) http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел

9) http://window.edu.ru/. Единое окно доступа к образовательным ресурсам

10) http://elibrary.ru/. Научная электронная библиотека

11) 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

«Введение в профессиональную деятельность»

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Специальность: (специализация №5)

Безопасность открытых информационных систем

Трудоемкость дисциплины: 2 з.е. (72 академических часа)

Семестр: 1(очная форма обучения)

Форма промежуточной аттестации: зачет

Содержание дисциплины. Основные разделы

Организация учебного процесса. Предмет курса, его цели и задачи. Сущность и содержание основной образовательной программы подготовки специалистов по защите информации по направлению «Информационная безопасность автоматизированных систем». Основы обеспечения информационной безопасности. Основные понятия защиты информации. Угрозы информационной безопасности и каналы утечки информации. Организационно-правовое обеспечение информационной безопасности. Инженерно-технические методы и средства защиты информации. Программно-аппаратные методы и средства обеспечения информационной безопасности.

ЛИСТ
регистрации изменений (дополнений) в рабочую программу учебной дисциплины
«Введение в профессиональную деятельность»

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

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Полякова Е.Н. /

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

Заведующий кафедрой _____ «___»_____20___ г.

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

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Полякова Е.Н. /

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

Заведующий кафедрой _____ «___»_____20___ г.