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:
Ректор КГУ

_____ / Н.В. Дубив/

«31» августа 2020 г.

Рабочая программа учебной дисциплины

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

образовательной программы высшего образования –
программы специалитета
10.05.03 — Информационная безопасность автоматизированных систем
Направленность: (специализация №7) обеспечение информационной безопасности распределенных информационных систем
Формы обучения: очная

Курган 2020

Рабочая программа дисциплины «Организационной и правовое обеспечение информационной безопасности»» составлена в соответствии с учебными планами по программе специалитета «Информационная безопасность автоматизированных систем» (обеспечение информационной безопасности распределенных информационных систем), утвержденным для очной формы обучения «28» августа 2020 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 31 августа 2020 года, протокол № 1.

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

канд. юр. наук О.И. Филонова

Согласовано:

Заведующий кафедрой «БИАС»
канд. пед. наук, доцент Е.Н. Полякова

Начальник Управления
образовательной деятельности С.Н. Синицын

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

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 10 зачетных единиц трудоемкости (360 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр	
		8	9
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**128**	**80**	**48**
Лекции	80	48	32
Лабораторные работы	-	-	-
Практические занятия	48	32	16
Самостоятельная работа, всего часов в том числе:	**232**	**100**	**132**
Подготовка к экзамену	27	27	-
Подготовка к зачету	18	-	18
Контрольная работа	18	18	-
Другие виды самостоятельной работы	169	55	114
Вид промежуточной аттестации	**экзамен, зачет**	**экзамен**	**зачет с оценкой**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**360**	**180**	**180**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к базовой части Блока 1.

Дисциплина «Организационное и правовое обеспечение информационной безопасности» базируется на знаниях учебных дисциплин «Правоведение», «Правовые аспекты информационных технологий», «Гуманитарные аспекты информационной безопасности» и «Основы информационной безопасности».

Особенность курса в виде сочетания правовых и естественнонаучных знаний определяет его место в учебном процессе. Повсеместное внедрение современных информационных и телекоммуникационных технологий в процессы производства и управления требует соответствующей правовой поддержки. Принятие важных решений, связанных с информационной безопасностью, требует обязательного закрепления соответствующими локальными нормативными актами (приказами, распоряжениями). Необходимые теоретические знания и практические навыки, отработанные в процессе изучения дисциплины, являются для каждого специалиста с высшим образованием той платформой, которая позволит ежедневно повышать свой профессиональный уровень, быть полезным для окружающих и общества в целом.

Знания и умения, приобретенные в ходе изучения дисциплины «Организационное и правовое обеспечение информационной безопасности» используются обучаемыми при изучении последующих дисциплин, раскрывающих всю совокупность методов и средств защиты информации, а также при разработке курсовых работ и проектов, а также выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины является раскрытие основ правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизма их реализации, понятия и виды защищаемой информации по законодательству РФ, системы защиты государственной тайны, основ правового регулирования отношений в области интеллектуальной собственности и способов защиты этой собственности, а также понятий и видов компьютерных преступлений.

Задачи дисциплины - дать основы:

- информационного законодательства Российской Федерации;
- международного законодательства в области защиты информации;
- нормативной базы в сфере ИБ;
- организационные принципы защиты информации, включая структуру подразделений ИБ и обязанности их сотрудников.

Компетенции, формируемые в результате освоения дисциплины:

- способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной

деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

- способность к самоорганизации и самообразованию (ОК-8);
- способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);
- способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);
- способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);
- способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23).

В результате изучения дисциплины обучающийся должен:

знать:

- основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации (для ОК-4, ОК-5, ОПК-6, ПК-23);
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях (для ОПК-6, ПК-1, ПК-23);
- организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации (для ОК-5, ПК-1, ПК-21);
- виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений (для ОК-4, ОК-8, ПК-22);

уметь:

- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности (для ОПК-6, ПК-1, ПК-22);
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации (для ОК-8, ОПК-6, ПК-21);

иметь навыки:

- работы с нормативно-правовыми актами (для ОПК-6, ПК-1);
- организации и обеспечения режима секретности (для ОПК-6, ПК-21, ПК-23;

- организации и управления деятельностью служб защиты информации на предприятии (для ОК-8, ПК-22, ПК-23).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем	
			Лекции	Практичес. занятия
8 семестр				
Рубеж 1	1	Информация как объект правового регулирования	4	-
	2	Законодательство РФ в области информационной безопасности	4	16
	3	Защита информации с ограниченным доступом	6	-
	4	Правовые режимы защиты информации	6	-
	5	Правовые вопросы защиты информации с использованием технических средств.	6	6
Рубеж 2	6	Защита интеллектуальной собственности	6	4
	7	Компьютерные преступления	6	4
	8	Расследование преступлений в сфере компьютерной информации	6	2
	9	Международное законодательство в области защиты информации	4	-
		Всего	**48**	**32**
9 семестр				
Рубеж 1	10	Основы обеспечения информационной безопасности.	2	-
	11	Анализ угроз объекту информационной безопасности.	2	-
	12	Организационные источники и каналы утечки информации.	4	-
	13	Организационные основы защиты информации на предприятии.	4	2
	14	Отнесение сведений к конфиденциальной информации.	4	1
	15	Организация допуска и доступа персонала к конфиденциальной информации.	4	3
	16	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.	2	-
Рубеж 2	17	Организация внутриобъектового и пропускного режимов на предприятии.	2	1
	18	Организация охраны предприятия и физической защиты его объектов.	2	-
	19	Планирование мероприятий по организационной защите информации на предприятии.	2	8
	20	Организация допуска предприятий к проведению работ со сведениями, составляющими государственную тайну.	4	1
		Итого:	**32**	**16**
		Всего за 8 и 9 семестр	**80**	**48**

4.2. Содержание лекционных занятий

8 семестр

Раздел 1. Информация как объект правового регулирования.

Информация как объект правового регулирования. Структура информационной сферы и характеристика ее элементов. Виды информации. Формирование информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации.

Раздел 2. Законодательство РФ в области информационной безопасности.

Понятие и структура информационной безопасности. Информационная сфера и информационная среда. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Конституционные гарантии прав граждан на информацию и механизм их реализации. Отрасли законодательства, регламентирующие деятельность по защите информации. Перспективы развития законодательства в области информационной безопасности.

Раздел 3. Защита информации с ограниченным доступом.

Государственная тайна как особый вид защищаемой информации. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система защиты государственной тайны. Режим секретности. Общие требования к системе защиты информации. Засекречивание информации. Организационные и технические способы защиты государственной тайны.

Конфиденциальная информация и её защита. Коммерческая тайна. Служебная тайна. Профессиональные тайны. Процессуальные тайны. Персональные данные.

Раздел 4. Правовые режимы защиты информации.

Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации. Правовой режим банковской тайны. Правовой режим персональных данных. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная). Правовая регламентация охранной деятельности.

Раздел 5. Правовые вопросы защиты информации с использованием технических средств.

Электронная цифровая подпись. Электронный документ как доказательство. Алгоритмы системы электронной цифровой подписи. Основные ограничения на использование электронных документов. Процедура разрешения конфликтов.

Понятия лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области защиты

информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия. Контроль за соблюдением лицензиатами условий ведения деятельности.

Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

Правовые основы защиты информации с использованием технических средств (защиты от технических разведок, применения и разработки шифровальных средств, применения электронно-цифровой подписи и т.д.).

Раздел 6. Защита интеллектуальной собственности.

Законодательство РФ об интеллектуальная собственности. Понятие интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем. Защита авторских и смежных прав. Основы патентных правоотношений. Условия патентоспособности. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Механизм патентования. Защита прав патентообладателей и авторов. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Особенности трудовых отношений.

Раздел 7. Компьютерные преступления

Понятие компьютерных преступлений и их классификация.

Уголовно-правовая характеристика компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ.

Криминалистическая характеристика компьютерных преступлений. Характеристика преступлений, совершаемых в сфере компьютерной информации. Основные виды преступлений в сфере программного обеспечения. Изготовление контрафактных экземпляров программ конечным пользователем.

Способы совершения преступлений в сфере компьютерной информации. Перехват информации. Несанкционированный доступ к СКТ. Манипуляция данными и управляющими командами.

Компьютерные вирусы. Общие сведения. Классификация вирусов. Классификация антивирусных средств. Методы защиты от компьютерных вирусов.

Тенденции развития компьютерной преступности в России.

Раздел 8. Расследование преступлений в сфере компьютерной информации.

Криминалистические аспекты проведения расследования компьютерных преступлений. Привлечение специалистов к участию в расследовании. Специфика обращения с машинными носителями компьютерной информации.

Тактика обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий. Осмотр места происшествия. Обыск. Следственные версии.

Экспертиза преступлений в сфере компьютерной информации. Объекты компьютерно-технической экспертизы. Исследование программного обеспечения. Исследование баз данных. Исследование аппаратного обеспечения ЭВМ.

Раздел 9. Международное законодательство в области защиты информации.

Законодательство РФ об участии в международном информационном обмене. Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена. Национальные законодательства о компьютерных правонарушениях и защите информации.

Международное право в сфере охраны программных продуктов. Международное сотрудничество в области борьбы с компьютерной преступностью.

9 семестр.

Раздел 10. Основы обеспечения информационной безопасности.

Роль и место информации и информационных технологий в современной жизни. Основные формы проявления информации и их свойства.

Информационная безопасность и ее обеспечение. Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации. Основные направления организационной защиты на объекте. Структура сил и средств организационной защиты информации. Компетенции органов власти в сфере ИБ: ФСБ России, СВР России, ФСО, ФСТЭК. Концептуальные документы о сфере ИБ.

Раздел 11. Анализ угроз объекту информационной безопасности.

Понятие угрозы и ее основные свойства. Классификация угроз. Анализ и оценка угроз информационной безопасности объекта. Модели нарушителей информационной безопасности на объекте. Формы преступного посягательства. Ущерб информационной безопасности предприятия. Оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации.

Раздел 12. Организационные источники и каналы утечки информации.

Основы теории информации. Коммуникационный процесс. Источники конфиденциальной информации и каналы ее утечки.

Раздел 13. Организационные основы защиты информации на предприятии.

Основные направления, принципы и условия организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Основные методы, силы и средства, используемые для организации защиты информации.

Раздел 14. Отнесение сведений к конфиденциальной информации.

Отнесение сведений к различным видам конфиденциальной информации. Отнесение сведений к коммерческой тайне. Реквизиты носителей сведений.

Засекречивание и рассекречивание сведений. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей.

Организация контроля за состоянием защиты конфиденциальной информации на предприятии. Понятие и основные объекты контроля.

Раздел 15. Организация допуска и доступа персонала к конфиденциальной информации.

Общие положения. Разрешительная система доступа персонала к конфиденциальной информации.

Основные положения допуска должностных лиц и граждан к государственной тайне. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа лицу в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну, и их носителям.

Порядок доступа к конфиденциальной информации командированных лиц.

Раздел 16. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.

Основы работы с персоналом предприятия. Подбор, расстановка и работа с кадрами. Основные этапы работы с персоналом. Методы работы с персоналом и их характеристика. Мотивация деятельности персонала.

Раздел 17. Организация внутриобъектового и пропускного режимов на предприятии.

Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия. Организация пропускного и внутриобъектового режима. Работа по организации внутриобъектового режима. Основные подходы и принципы.

Силы и средства, используемые при организации внутриобъектового режима. Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации.

Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

Раздел 18. Организация охраны предприятия и физической защиты его объектов.

Организация охраны предприятия. Средства и методы физической защиты объектов. Системы сигнализации, видеонаблюдения, контроля доступа. Служба безопасности объекта. Технологические меры поддержания информационной безопасности объектов. Физическая защита объектов предприятия.

Раздел 19. Планирование мероприятий по организационной защите информации на предприятии.

Основные цели планирования. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.

Организация защиты информации при проведении совещаний. Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов.

Организация режима и охраны объектов в процессе транспортировки. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения.

Организация защиты информации при осуществлении рекламной деятельности. Общие положения.

Защита информации при осуществлении публикаторской деятельности. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации при взаимодействии со СМИ.

Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества. Защита информации при выезде персонала предприятия за границу. Общие положения. Организация подготовки к передаче другим государствам сведений, составляющих государственную тайну.

Организация защиты информации при приеме на предприятии иностранных представителей. Порядок выезда персонала, осведомленного в сведениях, составляющих государственную тайну, за границу.

Раздел 20. Организация допуска предприятий к проведению работ со сведениями, составляющими государственную тайну.

Организация и обеспечение режима секретности. Основные положения лицензирования деятельности предприятий в области защиты государственной тайны. Алгоритм работы лицензирующего органа. Организация проведения государственной аттестации руководителей предприятий.

4.3. Практические занятия

Номер темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
		8 семестр	
2	Законодательство РФ в области информационной безопасности	*Практическое занятие №1.* Основы теории правового обеспечения информационной безопасности.	2
		Практическое занятие №2. Государственная система защиты информации.	2
		Практическое занятие №3. Нормативная база обеспечения защиты информации.	2
		Практическое занятие №4. Защита персональных данных.	2

		Практическое занятие №5. Авторское и патентное право.	2
		Практическое занятие №6. Защита государственной и коммерческой тайны.	2
		Практическое занятие №7. Электронная цифровая подпись. Защита прав и законных интересов субъектов информационной сферы.	2
	1-ый рубежный контроль	***Тестирование***	***2***
5	Правовые вопросы защиты информации с использованием технических средств.	*Практическое занятие №8.* Лицензирование деятельности в сфере ИБ. Сертификация продукции в сфере ИБ. Порядок проведения сертификационных испытаний. Сертификация продукции, ввозимой из-за границы.	2
		Практическое занятие №9. Сравнение полномочий ФСБ и ФАПСИ в области обеспечения информационной безопасности.	2
		Практическое занятие №10. Осуществление оперативно-розыскных мероприятий, нарушающих конституционные права и свободы.	2
6	Защита интеллектуальной собственности	*Практическое занятие №11.* Изучение вопросов защиты интеллектуальной собственности в Российской Федерации.	4
	2-ой рубежный контроль	***Тестирование***	***2***
7	Компьютерные преступления	*Практическое занятие №12.* Состав компьютерных преступлений.	2
8	Расследование преступлений в сфере компьютерной информации.	*Практическое занятие №13.* Сравнение ФЗ «Об Оперативно-розыскной деятельности» и нормативно-правовых актов об ОРМ и Закона «О частной детективной и охранной деятельности».	2
	Итого		**32**
		9 семестр	
13	Организационные основы защиты информации на предприятии.	*Практическое занятие №1.* Организационные основы защиты информации сотрудников. Варианты организационных структур. Основные документы службы информационной безопасности.	2
14	Отнесение сведений к конфиденциальной информации.	*Практическое занятие №2.* Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений.	1
15	Организация допуска и доступа персонала к конфиденциальной информации.	*Практическое занятие №3.* Организация допуска и доступа персонала к конфиденциальной информации.	1

	1-ый рубежный контроль	***Тестирование***	***2***
17	Организация внутриобъектового и пропускного режимов на предприятии.	*Практическое занятие №4.* Организация внутриобъектового и пропускного режимов на предприятии. Организация охраны предприятия и физической защиты его объектов.	1
19	Планирование мероприятий по организационной защите информации на предприятии.	*Практическое занятие №5.* Планирование мероприятий по организационной защите информации на предприятии.	2
		Практическое занятие №6. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.	2
		Практическое занятие №7. Реализация режимных мер в ходе подготовки и проведения закрытых совещаний и переговоров.	2
	2-ой рубежный контроль	***Тестирование***	*2*
20	Организация допуска предприятий к проведению работ со сведениями, составляющими государственную тайну.	*Практическое занятие №8.* Организация допуска предприятий к проведению работ со сведениями, составляющими государственную тайну.	1
	Итого		**16**

4.5 КОНТРОЛЬНАЯ РАБОТА

Целью контрольной работы «Правовое обеспечение и организация защиты информации на предприятии (в организации)» является реализация полученных знаний по дисциплине «Организационное и правовое обеспечение информационной безопасности» и соответствие приобретенным компетенциям.

Контрольная работа выполняется в соответствии с индивидуальным заданием. Содержание контрольной работы в соответствие с задание определено в методических указаниях к выполнению контрольной работы. Объем контрольной работы 15-20 страниц.

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.

Залогом качественного выполнения практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано на практических занятиях коллективное взаимодействие и разбор конкретных ситуаций, а также обсуждение неясных моментов и ситуаций по лекционному курсу.

Для текущего контроля успеваемости 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, выполнение контрольной работы, подготовку к практическим занятиям, к рубежным контролям, подготовку к экзаменам, зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела	113
Информация как объект правового регулирования	4
Законодательство РФ в области информационной безопасности	4
Защита информации с ограниченным доступом	4
Правовые режимы защиты информации	6
Правовые вопросы защиты информации с использованием технических средств	6
Защита интеллектуальной собственности	6
Компьютерные преступления	6
Расследование преступлений в сфере компьютерной информации	6
Международное законодательство в области защиты информации	6
Основы обеспечения информационной безопасности	6
Анализ угроз объекту информационной безопасности	4
Организационные источники и каналы утечки информации	6
Организационные основы защиты информации на предприятии	6
Отнесение сведений к конфиденциальной информации	6
Организация допуска и доступа персонала к конфиденциальной информации	6
Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	6
Организация внутриобъектового и пропускного режимов на предприятии	6
Организация охраны предприятия и физической защиты его объектов	6
Планирование мероприятий по организационной защите информации на предприятии	6
Организация допуска предприятий к проведению работ со сведениями, составляющими государственную тайну	6
Подготовка к практическим занятиям (по 2 часа на каждое занятие)	48
Подготовка к рубежным контролям (по 2 часа на каждый рубеж)	8
Подготовка к контрольной работе	18
Подготовка к экзаменам	27
Подготовка к зачету	18
Всего:	**232**

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 практическим занятиям.
3. Банк тестовых заданий к рубежным контролям №1, №2, №3 и №4.
4. Контрольная работа.
5. Перечень вопросов к зачету.
6. Перечень вопросов к экзаменам.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="8">Содержание</td></tr>
<tr><td rowspan="6">1</td><td rowspan="6">Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="8">Распределение баллов</td></tr>
<tr><td colspan="8">8 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение практической работы</td><td>Контрольная работа</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>0,5б х 24= 12б</td><td>3б х 13 = 39б</td><td>5</td><td>7</td><td>7</td><td>30</td></tr>
<tr><td colspan="8">9 семестр</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><td></td></tr>
<tr><td>Балльная оценка:</td><td>1б х 16=16б</td><td>5б х 8 = 40б</td><td>7</td><td>7</td><td>30</td><td></td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и на экзамене</td><td colspan="8">60 и менее баллов – неудовлетворительно; незачет;
61…73 – удовлетворительно; зачет;
74… 90 – хорошо;
91…100 – отлично</td></tr>
</table>

3	Критерии допуска к промежуточной аттестации, возможности получения автоматически экзаменационной оценки по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (экзамену, зачету с оценкой) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все практические работы и контрольную работу в 8 семестре. Для получения экзаменационной оценки «удовлетворительно» «автоматически» студенту необходимо набрать 68 баллов. По согласованию с преподавателем студенту, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен, зачет с оценкой «автоматически» оценка «хорошо» или «отлично».
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 (экзамену, зачету с оценкой) 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 и защита пропущенных практической работы – до 5 баллов. 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 со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

На каждое тестирование при рубежном контроле студенту отводится 2 часа. Варианты тестовых заданий для рубежных контролей №1, №2, №3 и №4 состоят из 10 вопросов.

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

Экзамен проводится в традиционной форме. Экзаменационный билет состоит из 2-х вопросов, каждый их которых оценивается в 15 баллов. Время, отводимое студенту на подготовку к ответу на вопросы составляет 1 астрономический час.

Зачет – в форме устного ответа на 2 вопроса. Перечень вопросов преподаватель выдает заранее. Время, отводимое студенту на подготовку

вопросов, составляет 1 академический час. Каждый вопрос оценивается в 15 баллов.

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

На каждое тестирование при рубежном контроле студенту отводится 45 минут (1 академический час).

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

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

8 СЕМЕСТР 9 СЕМЕСТР

1-ый рубежный контроль

1. Документированная информация – это:

а) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

б) содержание сообщений, сведений и сигналов;

в) зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

2. Условия прекращения допуска должностного лица или гражданина к государственной тайне:

а) расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий; длительным отсутствием на рабочем месте (например по болезни); возникновения обстоятельств, являющихся согласно статье 22 Закона «О государственной тайне» основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

б) расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий; однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны; возникновения обстоятельств, являющихся согласно статье 22 Закона «О государственной тайне» основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

в) в связи с переходом на новую должность; однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны; в связи с увольнением из предприятия.

3. Допуск специалиста к коммерческим секретам обязывает:

а) строго соблюдать требования инструкций по работе с коммерческими секретами; ответственность за нарушение режима информационной безопасности.

б) строго соблюдать требования руководства предприятия по вопросам трудового договора; обязательства по предоставлению гарантий и компенсаций за работу с конфиденциальной информацией.

в) быстрый карьерный рост по работе; применять свои права в области соблюдения режима информационной безопасности.

2-ой рубежный контроль

1. Система безопасности предприятия действует на основе следующих организационно-правовых документов:

а) Конституции РФ. Устава области. Федерального закона «О безопасности».

б) Устава. Положения о системе собственной безопасности. Руководства по защите конфиденциальной информации. Инструкции о порядке работы с иностранными специалистами. Руководства по инженерно-технической защите помещений и технических средств.

в) Конвенции по правам человека. Положения о системе коллективной безопасности. Приказов и инструкций по безопасности.

2. Имущественные права на программы для ЭВМ или базы данных, созданные в порядке выполнения служебных обязанностей или по заданию работодателя (если в договоре не оговорено иное), принадлежат:

а) только автору программы или базы данных;

б) только автору программы или базы данных и его наследникам;

в) работодателю.

3. Обладатель информации, составляющей государственную тайну, имеет право:

а) использовать информацию, составляющую государственную тайну, для собственных нужд;

б) по своему усмотрению передавать секретную информацию сторонним организациям;

в) вносить предложения по вопросам совершенствования режима охраны государственной тайны.

8 СЕМЕСТР

Примерный перечень вопросов к экзамену в 8-ом семестре

1. Структура информационной сферы и характеристика ее элементов. Виды информации.
2. Формирование информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации.
3. Понятие и структура информационной безопасности. Информационная
4. сфера и информационная среда.

5. Субъекты и объекты правоотношений в области информационной безопасности.

6. Понятие и виды защищаемой информации по законодательству РФ.

7. Конституционные гарантии прав граждан на информацию и механизм их реализации.

8. Отрасли законодательства, регламентирующие деятельность по защите информации.

9. Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

10. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне.

11. Меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны).

12. Система контроля за состоянием защиты государственной тайны.

13. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.).

14. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

15. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.

16. Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.

17. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).

18. Правовая регламентация охранной деятельности.

19. Понятия лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию.

20. Правовая регламентация лицензионной деятельности в области защиты информации.

21. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации.

22. Специальные экспертизы и государственная аттестация руководителей.

23. Органы лицензирования и их полномочия. Контроль за соблюдением лицензиатами условий ведения деятельности.

24. Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации.

25. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

26. Правовые основы защиты информации с использованием технических средств (защиты от технических разведок, применения и разработки шифровальных средств, применения электронно-цифровой подписи и т.д.).

27. Понятие интеллектуальной собственности. Объекты и субъекты авторского права.

28. Исключительные авторские права. Смежные права. Защита авторских и смежных прав.

29. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.

30. Основы патентных правоотношений. Условия патентоспособности.

31. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями.

32. Авторы изобретений и патентообладатели. Механизм патентования. Защита прав патентообладателей и авторов.

33. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Особенности трудовых отношений.

34. Понятие оперативно-розыскной деятельности и оперативно-розыскных мероприятий по законодательству РФ. Органы, уполномоченные на осуществление оперативно-розыскной деятельности.

35. Преступления в сфере компьютерной информации. Признаки и элементы состава преступления.

36. Криминалистическая характеристика компьютерных преступлений. Расследование компьютерного преступления.

37. Криминалистические аспекты проведения расследования. Сбор доказательств. Экспертиза преступлений в области компьютерной информации.

38. Законодательство РФ об участии в международном информационном обмене. Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена.

Примерный перечень вопросов к зачету в 9-ом семестре

1. Информационная безопасность и ее обеспечение. Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации.
2. Основные направления организационной защиты на объекте. Структура сил и средств организационной защиты информации.
3. Компетенции органов власти в сфере ИБ: ФСБ России, СВР России, ФСО, ФСТЭК. Концептуальные документы о сфере ИБ.
4. Понятие угрозы и ее основные свойства. Классификация угроз.
5. Анализ и оценка угроз информационной безопасности объекта.
6. Модели нарушителей информационной безопасности на объекте. Формы преступного посягательства.

7. Ущерб информационной безопасности предприятия. Оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации.

8. Источники конфиденциальной информации и каналы ее утечки.

9. Основные направления, принципы и условия организационной защиты информации.

10. Основные подходы и требования к организации системы защиты информации. Основные методы, силы и средства, используемые для организации защиты информации.

11. Отнесение сведений к различным видам конфиденциальной информации. Отнесение сведений к коммерческой тайне. Реквизиты носителей сведений.

12. Засекречивание и рассекречивание сведений. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.

13. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей.

14. Организация контроля за состоянием защиты конфиденциальной информации на предприятии. Понятие и основные объекты контроля.

15. Основные положения допуска должностных лиц и граждан к государственной тайне. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска.

16. Основания для отказа лицу в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну, и их носителям.

17. Порядок доступа к конфиденциальной информации командированных лиц.

18. Основы работы с персоналом предприятия. Подбор, расстановка и работа с кадрами.

19. Основные этапы работы с персоналом. Методы работы с персоналом и их характеристика. Мотивация деятельности персонала.

20. Организация пропускного и внутриобъектового режима. Работа по организации внутриобъектового режима. Основные подходы и принципы.

21. Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации.

22. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

23. Организация охраны предприятия. Средства и методы физической защиты объектов. Системы сигнализации, видеонаблюдения, контроля доступа.

24. Служба безопасности объекта. Технологические меры поддержания информационной безопасности объектов. Физическая защита объектов предприятия.

25. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.

26. Организация защиты информации при проведении совещаний. Планирование мероприятий по защите информации при подготовке к проведению совещания.

27. Организация допуска участников совещания к обсуждаемым вопросам.

Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов.

28. Организация режима и охраны объектов в процессе транспортировки. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения.

29. Защита информации при осуществлении публикационной деятельности. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации при взаимодействии со СМИ.

30. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.

31. Защита информации при выезде персонала предприятия за границу. Общие положения. Организация подготовки к передаче другим государствам сведений, составляющих государственную тайну.

32. Порядок выезда персонала, осведомленного в сведениях, составляющих государственную тайну, за границу.

33. Организация и обеспечение режима секретности.

34. Основные положения лицензирования деятельности предприятий в области защиты государственной тайны.

35. Организация проведения государственной аттестации руководителей предприятий.

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. Куняев Н.Н. Правовое обеспечение национальных интересов Российской федерации в информационной сфере. Логос 2010 – 348с, Доступ из ЭБС http//znanium.com/bookread2?book=469026

2. Правовое обеспечение информационной безопасности: Учебное пособие для студентов высших учебных заведений / С.Я. Казанцев, О.Э. Згадзай, Р.М. Оболенский и др.; Под редакцией С.Я. Казанцева. – М.: Издательский центр «Академия», 2005. – 240 с.

3. Романов О.А. Организационное обеспечение информационной безопасности: учебник для высших учебных заведений/ О.А.Романов, С.А.Бабин, С.Г.Жданов. - М: Академия,2008. – 192 с.

4. 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.

5. Рассолов М.М. Информационное право: Учебное пособие. - М.:Юристъ,

1999.-400 с.

1. Конфиденциальное делопроизводство и защищенный электронный докуменооборот; учебник/А.Г. Фабричев, А.С. Демушкин, Т.В. Кондрашова, Н.Н. Куняев – М; Логос,2017 – 452с (Новая университетская библиотека) – Доступ из ЭБС ISBN 978598704 5411 http//www studentlibray.ru/book/9785987047118.html

7.2. Дополнительная учебная литература

2. Гринсберг А.С., Горбачев Н.Н., Теплякова А.А. Защита информационных ресурсов государственного управления: Учебное пособие для вузов. – М.: Юнити-Дана, 2003. – 327 с.

3. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студентов высших учебных заведений / А.А. Стрельцов [и др.]; под ред. А.А. Стрельцова. — М.: Академия, 2008. – 256с.

4. Информационное право. Конспект лекций: учебное пособие – Москва, Проспект, 2016 – 144с – Доступ из ЭБС: ISBN 978-5-392-19524-4 http//www studentlibray.ru/book/9785392195244html

7.3 Нормативные правовые акты

1.Конституция Российской Федерации. Принята 12 декабря 1993 года всенародным голосованием. М., 1993.

2.Гражданский кодекс Российской Федерации, 1994г. Любое издание.

3.Доктрина информационной безопасности Российской Федерации: Утв. Президентом РФ 9 сентября 2000г., № Пр-1895 // Рос. газ. – 2000. – 28 сент.

4.Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г.

5.О внешней разведке: Федеральный закон, 10 янв. 1996г.

6.О государственной тайне: Закон РФ, 21 июля 1993г.

7.Перечень сведений конфиденциального характера: Утв. Указом Президента РФ, 6 марта 1997г.

8.О персональных данных: Федеральный закон от 27.07.2006 № 152.

9.Уголовный кодекс Российской Федерации от 13 июня 1996г.

7.4 Международные правовые акты

1. Европейская Конвенция о защите прав человека и основных свобод // Международные акты о правах человека. Сборник документов. М, 2005. С. 539 – 570.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

1. Филонова О.И. Методические указания к практическим занятиям по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. Курган: кафедра «БИАС», 2017. – 15 с.

2. Полякова Е.Н. Методические указания к выполнению практических занятий и самостоятельной работе студентов по дисциплине «Организационное

и правовое обеспечение информационной безопасности». для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. Курган: кафедра «БИАС», 2017. – 13 с.

3. Филонова О.И. Правовое обеспечение и организация защиты информации на предприятии (в организации). Методические указания к выполнению контрольной работы по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. Курган: кафедра «БИАС», 2017. – 8 с.

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

1. Информационно-справочная система «КонсультантПлюс».
2. http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел
3. http://window.edu.ru/. Единое окно доступа к образовательным ресурсам
4. http://elibrary.ru/. Научная электронная библиотека
5. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

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

11. 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.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Организационное и правовое обеспечение информационной безопасности»

образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Направленность: (специализация №7)
Обеспечение информационной безопасности распределенных информационных систем

Трудоемкость дисциплины: 10 з.е. (360 академических часа)
Семестр: 8 и 9 (очная форма обучения)
Форма промежуточной аттестации: экзамен, зачет с оценкой

Содержание дисциплины

Информация как объект правового регулирования. Законодательство РФ в области информационной безопасности. Защита информации с ограниченным доступом. Правовые режимы защиты информации. Правовые вопросы защиты информации с использованием технических средств. Защита интеллектуальной собственности. Компьютерные преступления. Расследование преступлений в сфере компьютерной информации. Международное законодательство в области защиты информации.

Основы обеспечения информационной безопасности. Анализ угроз объекту информационной безопасности. Организационные источники и каналы утечки информации. Организационные основы защиты информации на предприятии. Организация допуска и доступа персонала к конфиденциальной информации. Организация внутриобъектового и пропускного режимов на предприятии. Организация охраны предприятия и физической защиты его объектов. Организация допуска предприятий к проведению работ со сведениями, составляющими государственную тайну.