ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.Б.13 Основы информационной безопасности

Направление подготовки (специальность) *09.03.01 Информатика и вычислительная техника*

Профиль подготовки (специализация) *"Автоматизированные системы обработки информации и управления"*

Форма обучения *заочная*

СОДЕРЖАНИЕ

1. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1.1 Организационно-методические данные дисциплины

№ п.п.	Наименование темы	Общий объем часов по видам самостоятельной работы (*из табл. 5.1 РПД*)				
		подготовка курсового проекта (работы)	подготовка реферата /эссе	индивидуальные домашние задания (ИДЗ)	самостоятельное изучение вопросов (СИВ)	подготовка к занятиям (ПкЗ)
1	2	3	4	5	6	7
1.	Основные понятия, термины и определения. Основы государственной политики в области информационной безопасности.				10	
2.	Аттестация объектов информатизации по требованиям безопасности информации				10	
3.	Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне". Организационно-технические меры защиты сведений, составляющих государственную тайну				10	
4.	Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне". Организационно-технические меры защиты коммерческой тайны				26	
5.	Защита информации, не составляющей государственную				10	

	тайну, содержащейся в государственных информационных системах					
6.	Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"				66	
7.	Нормативно-правовые, морально-этические, административные, физические и технические меры				62	

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1 Стратегия национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Основу правового обеспечения информационной безопасности России помимо нормативно-правовых актов составляют концептуальные документы. Они принимаются на уровне Президента РФ, Правительства РФ и других органов государственной власти. В частности, такими документами являются Доктрина информационной безопасности РФ и Стратегия национальной безопасности РФ до 2020 года.

2.2 Требования к нормативным и методическим документам по аттестации объектов информатизации.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

ФСТЭК осуществляет следующие функции в рамках системы аттестации:

- организует обязательную аттестацию объектов информатизации;
- создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;
- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
- организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;
- аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;
- осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;
- рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации;

организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

2.3 Допуск к государственной тайне. Уголовно-правовая защита информации, составляющей государственную тайну.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.

2.4 Государственные информационные системы Использование информационно-телекоммуникационных сетей. Сведения, которые не могут составлять коммерческую тайну. Права обладателя информации, составляющей коммерческую тайну. Ответственность за нарушение требований Федерального закона «О коммерческой тайне».

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне".

Принят Государственной Думой 9 июля 2004 года. Одобрен Советом Федерации 15 июля 2004 года.

Цели и сфера действия Федерального закона:

1. Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

2.5 Аттестация информационной системы и ввод ее в действие. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации. Требования к мерам защиты информации, содержащейся в информационной системе.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;

- разработка системы защиты информации информационной системы;

- внедрение системы защиты информации информационной системы;

- аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

2.6 Состав и содержание мер по обеспечению безопасности персональных данных.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года.

Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких

средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

2.7 Нормативно-правовые, морально-этические, административные и физические меры обеспечения безопасности информации. Технические (программно-аппаратные) меры обеспечения безопасности информации.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, которые самостоятельно или в комплексе с другими средствами, реализуют следующие способы защиты:

- идентификацию (распознавание) и аутентификацию (проверку подлинности) субъектов (пользователей, процессов).

- разграничение доступа к ресурсам, регистрацию и анализ событий, криптографическое закрытие информации.

- резервирование ресурсов и компонентов систем обработки информации и др.

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 ПЗ-1 Основные понятия, термины и определения. Основы государственной политики в области информационной безопасности.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Основные термины и определения" вводит понятие информационной безопасности как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

- Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

3.2 ПЗ-2 Аттестация объектов информатизации по требованиям безопасности информации.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

3.3 ПЗ-3 Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне". Организационно-технические меры защиты сведений, составляющих государственную тайну.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

3.4 ПЗ-4,5 Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне". Организационно-технические меры защиты коммерческой тайны.

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

3.5 ПЗ-6 Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.