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/
«31» августа 2022 г.

Рабочая программа учебной дисциплины

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

образовательной программы высшего образования –
программы специалитета
10.05.03 ─ Информационная безопасность автоматизированных систем

Специализация: (специализация №5)
безопасность открытых информационных систем

Формы обучения: очная

Курган 2022

Рабочая программа дисциплины «Обеспечение безопасности информационных систем персональных данных и государственных информационных систем» составлена в соответствии с учебными планами по программе специалитета «Информационная безопасность автоматизированных систем» (безопасность открытых информационных систем), утвержденным для очной формы обучения «30» 08 2022 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «29» 08 2022 года, протокол № 1.

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

Согласовано:

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

Начальник Управления
образовательной деятельности И.В. Григоренко

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

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 4 зачетных единицы трудоемкости (144 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	семестр 10
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**72**	**72**
Лекции	32	32
Лабораторные работы	-	-
Практические занятия	40	40
Самостоятельная работа, всего часов в том числе:	**72**	**72**
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (подготовка к практическим работам и рубежному контролю)	45	45
Вид промежуточной аттестации	**экзамен**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**144**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Обеспечение безопасности информационных систем персональных данных и государственных информационных систем» относится к вариативной части, планируемой участниками образовательных отношений, дисциплинам Блока 1. Дисциплина по выбору.

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

- Основы информационной безопасности;
- Основы теории защиты информации;
- Теоретические основы компьютерной безопасности;
- Гуманитарные аспекты информационной безопасности.

Дисциплина обеспечивает изучение дисциплин: «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» и «Информационная безопасность открытых систем», а также выполнение курсовых работ и проектов и выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины «Обеспечение безопасности информационных систем персональных данных и государственных информационных систем» является формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

Задачами дисциплины являются:

– Изучением нормативных правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;

– Изучение методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;

– Практическая обработкой способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Компетенции, формируемые в результате освоения дисциплины:

- Способен разрабатывать требования по защите информации, технические задания на создание систем защиты и руководящие документы по защите информации в открытых информационных системах (ПК-3);
- Способен определять угрозы безопасности, реализация которых может привести к нарушению безопасности информации в открытых информационных системах (ПК-4);

- Способен формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-13).

В результате изучения дисциплины обучающийся должен:

знать

- содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных (для ПК-3, ПК-4);
- основные виды угроз безопасности персональных данных в информационных системах персональных данных (для ПК-3, ПК-4);
- содержание и порядок организации работ по выявлению угроз безопасности персональных данных (для ПК-3, ПК-4, ПК-13);
- процедуры задания и реализации требований по защите информации в информационных системах персональных данных и государственных информационных системах (для ПК-13);
- меры обеспечения безопасности персональных данных (для ПК-4, ПК-13);
- порядок применения организационных и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (для ПК-13);

уметь

- формировать множество альтернативных решений, ставить цель и выбирать оценочные критерии оптимальности, формулировать ограничения на управляемые переменные, связанные со спецификой моделируемой системы (для ПК-4, ПК-13);
- планировать мероприятия по обеспечению безопасности персональных данных (для ПК-№, ПК-4 ПК-13);
- разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности персональных данных (для ПК-13);
- обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных (для ПК-13);
- проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и государственных информационных системах (для ПК-3, ПК-4);
- определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и государственных информационных системах, необходимых для блокирования угроз безопасности персональных данных (для ПК-3, ПК-4, ПК-13).

владеть

- навыками определения уровня защиты персональных данных (для ПК-3, ПК-13);
- навыками выявления угроз безопасности персональных данных в информационных персональных данных и государственных информационных системах (для ПК-3, ПК-4).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план.

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем	
			Лекции	Практическ. занятия
Рубеж 1	*Тема 1.*	Правовые и организационные вопросы технической защиты информации ограниченного доступ	5	5
	Тема 2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	6	5
		Рубеж 1	-	2
Рубеж 2	*Тема 3*	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	8	8
	Тема 4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	8	8
	Тема 5	Практические реализации типовых моделей защищённых информационных систем обработки персональных данных	5	10
		Рубеж 2	-	2
		Всего:	**32**	**40**

4.2.Содержание лекционных занятий

Тема 1 Правовые и организационные вопросы технической защиты информации ограниченного доступ.

Основные понятия в области технической защиты информации (далее – ТЗИ). Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика её основных составляющих.

Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи, полномочия и права Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и управления ФСТЭК России по федеральным округам.

Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации.

Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

Тема 2 Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа.

Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы», целостности, конфиденциальности и доступности информации.

Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Тема 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных.

Особенности информационного элемента информационной системы персональных данных.

Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам.

Основные принципы обеспечения безопасности персональных данных при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности, самозащиты, многоуровневости, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Оценка достаточности и обоснованности запланированных мероприятий.

Рекомендации по применению мер и средств обеспечения безопасности персональных данных от физического доступа.

Тема 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Определение необходимых уровней защищённости персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объёма обрабатываемых в них персональных данных.

Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учётом актуальных угроз безопасности персональных данных и применяемых информационных технологий.

Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточнённого адаптированного базового набора мер.

Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.

Организация и перечень основных этапов обеспечения безопасности персональных данных.

Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных.

Тема 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных.

Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе её создания или модернизации.

Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных. Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.

4.3 Практические занятия

№ темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
1	Правовые и организационные вопросы технической защиты информации ограниченного доступ.	*Практическое занятие №1.* Анализ международного и Российского законодательства по вопросам обработки ПДн и обеспечения безопасности ПДн. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Права субъекта персональных данных, обязанности оператора	5
2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа.	*Практическое занятие №2.* Определение особенности обработки персональных данных, осуществляемой без использования средств автоматизации	5
	1-ый рубежный контроль	**Тестирование**	**2**
3	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	*Практическое занятие №3.* Составление перечня ПДн, перечня сотрудников, работающих с ПДн. Описание ИСПДн. Выявление угроз безопасности персональных данных при их обработке в ИСПДн. Разработка частной модели угроз безопасности ПДн. Определение актуальности угроз в соответствии с методическими документами ФСТЭК России. Разработка модели нарушителя.	8
4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	*Практическое занятие №4.* Составление частного технического задания на разработку системы защиты персональных данных. Обоснование разработки системы защиты ПДн.	8

№ темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
5	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных.	*Практическое занятие №5.* Разработка системы защиты ПДн. Выбор средств защиты информации. Программнотехнические комплексы защиты информации от несанкционированного доступа. Технические средства перекрытия технических каналов утечки информации. Организационные мероприятия.	10
	2-ой рубежный контроль	**Тестирование**	**2**
	Итого		**40**

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. Преподавателем запланировано применение на практических работах разбора конкретных ситуаций.

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

Выполнение самостоятельной работы подразумевает подготовку к практическим работам, рубежным контролям и экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	***5***
Правовые и организационные вопросы технической защиты информации ограниченного доступ	1
Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	1
Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	1
Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	1
Практические реализации типовых моделей защищённых информационных систем обработки персональных данных	1
Подготовка к практическим занятиям (по 2 часа)	36
Подготовка к рубежным контролям (по 2 часа)	4
Подготовка к экзамену	27
Всего:	**72**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по практическим занятиям.
3. Банк тестовых заданий к рубежным контролям № 1, № 2.
4. Вопросы к экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание					
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	***Распределение баллов, 10 семестр***					
		Вид учебной работы:	Посещение лекций	Выполнение практической работы	Рубежный контроль №1	Рубежный контроль №2	Экзамен
		Балльная оценка:	$1{,}5_б$ x 16=$24_б$	$6_б$ x 5 =30	8	8	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и на экзамене	60 и менее баллов – неудовлетворительно; незачет; 61…73 – удовлетворительно; зачет; 74… 90 – хорошо; 91…100 – отлично					

<table>
<tr><td>№</td><td>Наименование</td><td colspan="6">Содержание</td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="6">Распределение баллов, 10 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>Экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>$1,5_б$ х 16=$24_б$</td><td>$6_б$ х 5 =30</td><td>8</td><td>8</td><td>30</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматически экзаменационной оценки «удовлетворительно» по дисциплине, возможность получения бонусных баллов</td><td colspan="6">Для допуска к промежуточной аттестации (экзамену) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все практические работы.
Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов: 68 для получения «автоматически» оценки удовлетворительно».
По согласованию с преподавателем студенту, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на практических работах, 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 «автоматически» оценка «хорошо» или «отлично».</td></tr>
<tr><td>4</td><td>Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра</td><td colspan="6">В случае если к промежуточной аттестации (экзамену) 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 пропущенной практической работы – до 6 баллов. Прохождение рубежных контролей – до 8 баллов за каждый.
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.</td></tr>
</table>

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме тестирования.

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

Примерные варианты тестовых заданий для рубежного контроля №1 и №2 приведены ниже и состоят из 8 вопросов по 1 баллу каждый. На каждый рубежный контроль студенту отводится 2 академических часа.

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

Экзамен проходит в традиционной форме по билетам. Билет состоит из 2 вопросов. Перечень вопросов преподаватель выдает заранее, на последней лекции в семестре. Время, отводимое студенту на подготовку вопросов, составляет 1 академический час. Каждый вопрос оценивается в 15 баллов.

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

6.4. Примеры оценочных средств для рубежных контролей и экзамена

Примерные перечень вопросов для рубежного контроля №1

1. Какой документ определяет требования к защите персональных данных при их обработке в информационных системах персональных данных:

а. Постановление от 1 ноября 2012 г. N 1119;

б. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21;

в. ФЗ -152 «О персональных данных».

2. Информационная система, обрабатывающая персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных является:

а. информационной системой, обрабатывающей специальные категории персональных данных;

б. информационной системой, обрабатывающей биометрические персональные данные;

в. информационной системой, обрабатывающей общедоступные персональные данные;

г. информационной системой, обрабатывающей иные категории персональных данных.

3. В каком случае фотографию можно отнести к биометрическим персональным данным?

а. В случае если эта фотография находится в личном деле;

б. В случае если фотография зарегистрирована в СКУД (система контроля управления доступом);

в. В случае если эта фотография сделана в публичном месте.

4. Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки — это...

а. канал атаки;

б. атака;

в. контролируемая зона

5. Информационная система, обрабатывающая персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных является:

а. информационной системой, обрабатывающей специальные категории персональных данных;

б. информационной системой, обрабатывающей биометрические персональные данные;

в. информационной системой, обрабатывающей общедоступные персональные данные;

г. информационной системой, обрабатывающей иные категории персональных данных.

6. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных определяет документ:

а. Постановление от 1 ноября 2012 г. 1119;

б. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21;

в. ФЗ -152 «О персональных данных».

7. Технический канал утечки информации — это…

а. совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

б. совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

в. совокупность программных и техническую элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

8. Угрозы безопасности персональных данных — это...

а. совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

б. совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

в. совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

9. Сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию — это...

а. Биометрические персональные данные;

б. Специальные персональные данные;

в. Общедоступные персональные данные.

10. Какие действия можно производить с персональными данными?

а. чтение и рассылка;

б. хранение, уничтожение;

в. обезличивание, блокирование;

г. фасовка и упаковка.

11. Идентификация это:

а) процесс предъявления пользователем идентификатора;

б) процесс подтверждения подлинности;

в) сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов.

Примерные перечень вопросов для рубежного контроля №2

1. Какие из перечисленных угроз относятся к случайным угрозам компьютерной информации:

а) несанкционированный доступ к информации, вредительские программы;

б) электромагнитные излучения и наводки, несанкционированная модификация структур;

в) стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала.

2. Для защиты от случайных угроз компьютерной информации используют:

а) обучение пользователей правилам работы с КС, разрешительную систему доступа в помещение;

б) межсетевые экраны, идентификацию и аутентификацию пользователей;

в) дублирование информации, создание отказоустойчивых КС, блокировка ошибочных операций.

3. Системы анализа уязвимостей позволяют:

а) выявить злоумышленника работающего в компьютерной сети;

б) выявить уязвимости проектируемой системы защиты информации;

в) выявить уязвимости действующей системы защиты информации.

4. За несоблюдение положений закона 152-ФЗ «О персональных данных» предусматривается:

а) гражданская, уголовная, административная ответственность;

б) дисциплинарная и другие виды ответственности;

в) все перечисленные виды ответственности.

5. Блокирование персональных данных:

а) временное прекращение обработки персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

в) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

6. Обезличивание персональных данных:

а) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных;

в) все перечисленные действия.

7. Какую роль играют центры сертификации ключей:

а) они играют роль доверенной третьей стороны для доказывания факта передачи информации;

б) они служат для регистрации абонентов, изготовления сертификатов открытых ключей, хранения изготовленных сертификатов, поддержания в актуальном состоянии справочника действующих сертификатов и выпуска списка досрочно отозванных сертификатов;

в) они выдают сертификат соответствия длины сгенерированных ключей требованиям нормативных документов.

8. При проведении контроля за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах персональных данных регуляторы:

а) вправе знакомиться с персональными данными, обрабатываемыми в информационных системах персональных данных;

б) не вправе знакомиться с персональными данными, обрабатываемыми в информационных системах персональных данных;

в) вправе знакомиться с персональными данными, обрабатываемыми в информационных системах персональных данных, только в установленных законом случаях.

9. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах осуществляются:

а) ФСТЭК России и ФСБ России;

б) ФСТЭК России и органами Роскомнадзора;

в) ФСБ России и органами Роскомнадзора.

10. Перечислите виды электронной подписи:

а) простая, сложная, комбинированная;

б) простая, квалифицированная, сложная;

в) простая, квалифицированная, неквалифицированная.

11. СТР-К при защите государственных систем, обрабатывающих ПДн:

а) применяется в полном объеме;

б) не применяется;

в) применяется при реализации мер по защите технических средств государственных информационных систем.

12. Распространение аттестата соответствия на другие сегменты информационной системы:

а) допускается при условии их соответствия сегментам информационной системы, прошедшим аттестационные испытания;

б) допускается по решению оператора с оформлением акта;

в) не допускается.

13. Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита:

а) речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов;

б) физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн;

в) всех видов информации.

14. Что является организационной формой защиты информации:

а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения.

15. Что является правовой формой защиты информации:

а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения.

16. Что является инженерно-технической формой защиты информации:

а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения.

17. К числу определяющих признаков, по которым производится классификация информационных систем, относятся:

а) наличие в информационной системе информации различного уровня конфиденциальности;

б) уровень значимости информации и масштаб информационной системы;

в) режим обработки данных в информационной системе - коллективный или индивидуальный.

18. Для ИСПДн устанавливается:

а) два уровня защищенности персональных данных;

б) три уровня защищенности персональных данных;

в) четыре уровня защищенности персональных данных;

19. Оценка эффективности реализованных мер по защите ПДн в государственных ПС:

а) проводится в рамках обязательной аттестации государственной информационной системы по требованиям защиты информации;

б) проводиться оператором самостоятельно в рамках мероприятий по контролю;

в) форма оценки эффективности, а также форма и содержание документов, разрабатываемых по результатам (в процессе) оценки, ФСТЭК России не установлены.

20. Уровень защищенности ПДн устанавливается в зависимости от:

а) типа угроз, актуальных для ИСПДн и категории обрабатываемых ПДн;

б) объема ПДн, обрабатываемых в ИСПДн;

в) типа угроз, актуальных для ИСПДн, категории обрабатываемых ПДн, объема ПДн, обрабатываемых в ИСПДн.

21. Аттестацию информационных систем по требованиям безопасности информации:

а) оператор проводит самостоятельно, с привлечением штатных специалистов по защите информации;

б) проводит орган по аттестации, аккредитованный ФСТЭК России;

в) государственные информационные системы не подлежат аттестации.

22. Какие основные способы разграничения доступа применяются в компьютерных системах:

а) дискреционный и мандатный;

б) по специальным спискам и многоуровневый;

в) по группам пользователей и специальным разовым разрешениям.

23. Какие основные компоненты входят в состав удостоверяющего центра:

а) центр сертификации, центр авторизации, АРМ администратора;

б) центр регистрации, центр авторизации, АРМ администратора;

в) центр сертификации, центр регистрации, АРМ администратора.

24. Что собой представляет сертификат электронного ключа подписи:

а) это электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

б) это документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

в) это логическая посимвольная свертка подписываемого сообщения, зашифрованная на открытом ключе получателя.

Примерный перечень вопросов к экзамену

1. Основные понятия, используемые в ФЗ "О ПДн". Принципы обработки ПДн;
2. Условия обработки ПДн;
3. Приказ ФСБ России от 10.08.14 г. N378: Состав и содержание организационных и технических мер для 4 уровня защищенности ПДн;
4. Специальные категории ПДн;
5. Управление запуском (обращениями) компонентов ПО, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения;
6. Общая характеристика уязвимостей ИСПДн;
7. Меры по обеспечению безопасности ПДн при их обработке;
8. Общая характеристика источников угроз НСД в ИСПДн;
9. Угрозы НСД к информации ИСПДн;
10. Лица, ответственные за организацию обработки ПДн в организациях. Ответственность за нарушение требований ФЗ "О ПДн";
11. Уполномоченный орган по защите прав субъектов ПДн;
12. Общие требования при обработке ПДн работника и гарантии их защиты. Передача ПДн работника;
13. Права работников в целях обеспечения защиты ПДн, хранящихся у работодателя;
14. Административная ответственность за нарушения в сфере обработки и защиты ПДн;
15. Уголовная ответственность за преступления в сфере обработки и защиты ПДн. Дисциплинарная и материальная ответственность за нарушения в сфере обработки и защиты персональных данных работников;
16. Классификация угроз безопасности ПДн: признаки классификации и классы угроз Общие положения и меры по обеспечению безопасности ПДн при их обработке, осуществляемой без использования средств автоматизации;
17. Классификация угроз безопасности ПДн: характеристики ИСПДн, свойства среды распространения информативных сигналов, содержащих ПДн, возможности источников УБПДн;
18. Канал реализации УБПДн;
19. Требования к защите ПДн при их обработке в ИСПДн: Система защиты ПДн, виды ИСПДн, типы актуальных угроз безопасности ПДн;
20. Требования к защите ПДн при их обработке в ИСПДн: необходимые условия и требования обеспечения 4-1 уровней защищенности ПДн;

21. Приказ ФСТЭК от 18.02.13 г. N 21: Состав и содержание мер по обеспечению безопасности ПДн;

22. Приказ ФСБ России от 10.08.14 г. N378: Состав и содержание организационных и технических мер для 3-1 уровней защищенности ПДн;

23. Свойства обезличенных данных. Характеристики методов обезличивания ПДн. Требования к свойствам получаемых обезличенных данных. Требования к свойствам метода обезличивания;

24. Приказ ФСБ России от 10.08.14 г. N 378: СКЗИ класса КС2, КС3, КВ, КА;

25. Приказ ФСБ России от 10.08.14 г. N 378: СКЗИ класса КС1;

26. Опишите рекомендуемый порядок выбора методов обезличивания в соответствии с классом задач обработки, а также рекомендуемый порядок выбора типа технологии обработки обезличенных данных;

27. Опишите процедуру организации обработки обезличенных данных, а также правила работы Операторов с обезличенными данными;

28. Опишите следующие методы обезличивания ПДн: введения идентификаторов, изменения состава или семантики, декомпозиции, перемешивания;

29. Опишите процедуру выбора мер по обеспечению безопасности ПДн, подлежащих реализации в ИС в рамках системы защиты ПДн, а также требования к СЗИ в соответствии с Приказом ФСТЭК от 18.02.13 г. N 21;

30. Опишите особенности организации обработки ПДн, осуществляемой без использования средств автоматизации;

31. Опишите с помощью блок-схемы административную процедуру принятия решения о проведении проверок, проведения проверок, оформления результатов и принятия мер по результатам проверок, а также виды проверок, осуществляемых Роскомнадзором;

32. Опишите программу проведения работ по контролю (надзору) ФСБ за использованием шифровальных (криптографических) средств, применяемых для обеспечения безопасности ПДн в ИСПДн;

33. Опишите порядок идентификации ИСПДн, а также общую процедуру определения актуальных угроз и уровней защищенности ИСПДн организации;

34. Опишите порядок реализации мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ "О ПДн" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися гос. или муниц. Органами;

35. Опишите порядок уведомления об обработке ПДн;

36. Опишите порядок исполнения оператором обязанностей при обращении к нему субъекта ПДн либо при получении запроса субъекта ПДн или его представителя, а также уполномоченного органа по защите прав субъектов ПДн, а также обязанностей по устранению нарушений законодательства, допущенных при обработке ПДн, по уточнению, блокированию и уничтожению ПДн;

37. Опишите порядок реализации обязанностей оператора при сборе ПДн, а также меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ "О ПДн";

38. Опишите порядок реализации прав субъектов ПДн при принятии решений на основании исключительно автоматизированной обработки их ПДн и права на обжалование действий или бездействия оператора;

39. Опишите порядок определения актуальных угроз безопасности ПДн в ИСПДн;

40. Опишите порядок идентификации и аутентификации пользователей, являющихся работниками оператора;

41. Опишите процедуру управления (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

42. Опишите порядок реализации прав субъекта ПДн на доступ к его ПДн;

43. Опишите порядок учета машинных носителей информации;

44. Опишите процедуру определения событий безопасности, подлежащих регистрации, и сроков их хранения;

45. Опишите порядок реализация антивирусной защиты;

46. Опишите порядок трансграничной передачи ПДн, а также особенности обработки ПДн в государственных или муниципальных ИСПДн;

47. Опишите порядок выявления, анализа и устранения уязвимостей информационной системы;

48. Опишите процедуру контроля целостности ПО, включая ПО СЗИ;

49. Опишите порядок получения и содержание согласия субъекта ПДн на обработку его ПДн Опишите порядок идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;

50. Опишите процедуры контроля и управления физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены;

51. Опишите порядок защиты периметра (физических и (или) логических границ) ИС при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

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. О персональных данных: Комментарий к Федеральному закону от 27 июля 2006 года№ 152-ФЗ (постатейный) / Р. В. Амелин [и др.] // Консультант Плюс, 2013.

2. Вихорев С. В. Диалоги о безопасности информации, или введение в основы построения систем обеспечения информации: пособие // С. В. Вихорев, А. М. Сычев. - Москва: Медиа Группа «Авангард», 2015. - 640 с.

3. Мещеряков В. А. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления: научно-методическое пособие //В. А. Мещеряков [и др.] - Воронеж: ВИ МВД России, 2014. - 189 с.

4. Лихо дедов Д. Ю. Организация безопасности персональных данных в подразделениях органов внутренних дел: учебное пособие // Д. Ю. Лиходедов. - Воронеж: ВИ МВД России, 2014. - 43 с.

5. Обеспечение безопасности персональных данных. Электронное учебно-методическое пособие. Под общей редакцией Я. Н. Топилина. ООО «Издательский Дом «Афина», Санкт-Петербург. - 2017 г. - 136 с.

6. Гусев, А. Ю. Судебная практика о применении законодательства, регулирующего вопросы защиты персональных данных: учебно-практическое пособие / Гусев А. Ю. - Москва: Проспект, 2019. - 64 с. - ISBN 978-5-392-29690-3. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785392296903.html - Режим доступа: по подписке.

7. Петренко, В. И. Защита персональных данных в информационных системах: учебное пособие / В. И. Петренко. — Ставрополь: СКФУ, 2016. — 201 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/155246. — Режим доступа: для авториз. пользователей.

8. Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных" (вместе с "Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ") (Зарегистрировано в Минюсте России 10.09.2013 N 29935) http://base.garant.ru/70451476/.

7.2 Дополнительная учебная литература

1. Змеев С. А. Методы и средства повышения защищенности автоматизированных систем на основе задания требований к механизмам защиты: учеб. пособие / С. А. Змеев [и др.]. - Воронеж: Воронежский институт МВД РФ, 2013. -105 с.

2. Брауде-Золотарев М.Ю., Сербина Е. С., Негородов В. С., Волошин И. Г. Персональные данные в государственных информационных ресурсах

[Электронный ресурс]: Дело РАНХиГС, 2016. – 56 с. - Доступ из ЭБС «znanium.com».

7.3 МЕТОДИЧЕСКАЯ ЛИТЕРАТУРА

1. «Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации», утв. Банком России, АРБ, Ассоциацией региональных банков России (Ассоциация «Россия»);
2. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утв. Заместителем директора ФСТЭК России от 15 февраля 2008 г.;
3. Приказ Роскомнадзора от 30 мая 2017 года N 94 Об утверждении Методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения (с изменениями на 30 октября 2018 года);
4. Официальный портал персональных данных (Роскомнадзор) - http://pd.rkn.gov.ru/;
5. Банк данных угроз безопасности информации, размещенный на официальном сайте ФСТЭК России – www.bdu.fstec.ru.

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

1. Информационно-правовой портал Гарант - URL: http://www.garant.ru;
2. Официальный сайт компании - КонсультантПлюс». URL: http://www. consultant.ru;
3. Электронный фонд «Техэксперт» - URL: https://cntd.ru/;
4. Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/;
5. Официальный сайт Федеральной службы по техническому и экспортному контролю -URL: http://fstec.ru;
6. Официальный сайт Федеральной службы безопасности - URL: http: //www. fsb.ru;
7. Официальный сайт Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций - URL: http://rkn.gov.ru.

9. 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:

1. Операционная система Microsoft Windows;
2. Пакет офисных программ Microsoft Office/LibraryOffice;
3. Программное обеспечения для чтения файлов в формате PDF.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet.

Лекции и практические занятия проводятся в аудитории, оснащенной следующими средствами:

Учебная аудитория для проведения лекционных, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Оснащение аудитории:

1. Комплект учебной мебели: парты, стол преподавательский, стулья, доска;
2. Мультимедийная система: проектор LCD, экран настенный;
3. Лицензионное программное обеспечение: ОС Microsoft Windows;
4. Свободно распространяемое программное обеспечение: офисный пакет LibreOffice, программа просмотра pdf-документов FineReader.

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
«Обеспечение безопасности информационных систем персональных данных и государственных информационных систем»

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

Трудоемкость дисциплины: 4 з.е. (144 академических часа)
Семестр: 10 (очная форма обучения)
Форма промежуточной аттестации: экзамен

Содержание дисциплины

Правовые и организационные вопросы технической защиты информации ограниченного доступ. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Практические реализации типовых моделей защищённых информационных систем обработки персональных данных.