Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

« С.3.2.1 Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

специальности подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
Специализация «Создание автоматизированных систем в защищенном исполнении»

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 4
часов в неделю – 4
всего часов – 144,
в том числе:
лекции – 36
практические занятия – 36
самостоятельная работа – 72
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: изучение основных понятий, методологии, а также развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Задачи изучения дисциплины:

1) изучением нормативных правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;

2) изучением методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;

3) практической отработкой способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Место дисциплины в структуре ООП ВПО

Дисциплина «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» относится к числу дисциплин вариативной части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – знать формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей;

«Основы информационной безопасности» – знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, владеть профессиональной терминологией в области информационной безопасности;

«Сети и системы передачи информации» – знать основные характеристики сигналов электросвязи, спектры и виды модуляции, принципы построения и функционирования систем и сетей передачи информации, способы кодирования информации, основные телекоммуникационные протоколы.

Дисциплина «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» является предшествующей для изучения следующих базовых дисциплин: «Управление информационной безопасностью», «Программно-аппаратные

средства обеспечения информационной безопасности», «Комплексное обеспечение информационной безопасности автоматизированных систем».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

способности понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-4);

способности использовать нормативные правовые акты в своей профессиональной деятельности (ПК-6);

способности осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способности разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

Студент должен знать:

- значение защиты персональных данных в условиях развития современного общества и ответственность за нарушение требований законодательства РФ по обращению с персональными данными;
- содержание основных нормативно-правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- процедуры поиска и обработки нормативные правовые акты и нормативные методические документы в области обеспечения безопасности персональных данных;
- основные виды угроз безопасности персональных данных в информационных системах персональных данных;
- содержание и порядок организации работ по выявлению угроз безопасности персональных данных.

Студент должен уметь:

- применять основные требования Федерального закона "О персональных данных" для обеспечения защиты персональных данных в соответствии с необходимым уровнем защищенности персональных данных при их обработке в ИСПДн;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности персональных данных;

- разрабатывать техническое обоснование для создания системы защиты информационных систем персональных данных;
- классифицировать действующие нормативные и методические документы ФСТЭК России, ФСБ России и Роскомнадзора в соответствии с их полномочиями;
- проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.

Студент должен владеть:

- навыками выработки требований к защите персональных данных при их обработке в информационных системах персональных данных;
- навыками работы с нормативными правовыми актами в области обеспечения безопасности персональных данных;
- методами формирования требований к защите персональных данных при их обработке в информационных системах персональных данных;
- навыками работы с технологиями поиска нормативных правовых актов и нормативных методических документов в области обеспечения безопасности персональных данных в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации;
- навыками выявления угроз безопасности персональных данных в информационных системах персональных данных.

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ Мо-ду-ля	№ Не де ли	№ Те мы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лек-ции	Коллок-виумы	Лабора-торные	Прак-тичес-кие	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**		**8**	**9**
8 семестр									
1	1	1	Правовые и организационные основы	24/1	4/1	-	-	-	20

			защиты информации ограниченного доступа						
1	3	2	Требования к защите персональных данных при их обработке в информационных системах	42/10	10/6	-	-	12/4	20
2	8	3	Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн	46/7	8/4	-	-	16/3	22
2	12	4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в ИСПДн	38/10	20/7	-	-	8/3	10
Всего				144/28	36/18	-	-	36/10	72

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5
1	2	1	Структура, задачи и основные функции органов государственной власти, отвечающих за организацию защиты персональных данных в Российской Федерации. Законодательная и нормативная база правового регулирования вопросов защиты персональных данных. Руководящие документы по защите персональных данных. Ответственность за нарушение требований законодательства РФ по обращению с персональными данными (УК+КоАП).	1, 3, 4
1	2	2	Основные понятия Федерального закона "О персональных данных". Область применения закона. Виды и цели обработки персональных данных. Специальные категории персональных данных. Биометрические персональные данные. Общедоступные, подлежащие опубликованию или обязательному раскрытию персональные данные. Реестр операторов персональных данных.	2, 6
2	2	3	Понятие информационной системы персональных данных. Требования Федерального закона "О персональных данных" к обеспечению безопасности персональных данных. Определение необходимых уровней защищенности персональных данных при их обработке в ИСПДн в зависимости от типа актуальных угроз для информационных систем,	1, 2, 5

			вида и объема обрабатываемых в них персональных данных. Требования к защите персональных данных при их обработке в информационных системах персональных данных.	
2	2	4	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам	1, 3
2	2	5	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.	1, 3
2	2	6	Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии. Рекомендации по применению мер и средств обеспечения безопасности персональных данных от физического доступа. Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации. Классификация ТКУИ.	1, 3
2	2	7	Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях. Оценка защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.	1, 3
3	2	8	Порядок выбора организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер. Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных (Методический документ ФСТЭК «Меры защиты информации в ГИС»).	1, 2, 3

3	2	9	Оценка соответствия средств защиты информации. Технические и программные средства защиты информации, применяемые при защите информационных систем персональных данных для различных уровней защищенности.	1
3	2	10	Обеспечение безопасности персональных данных с использованием средств криптографической защиты информации.	2
3	2	11	Порядок лицензирования операторов информационных систем персональных данных	3
4	2	12	Разработка технического обоснования для создания системы защиты информационных систем персональных данных. Состав технического задания на разработку системы защиты персональных данных.	3
4	2	13	Порядок внедрения средств обеспечения информационной безопасности информационных системах персональных данных (комплект документов). Оценка эффективности ИСПДн.	3
4	2	14	Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	2, 3
4	2	15	Содержание и порядок проведения аттестации информационных систем персональных данных. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.	3
4	2	16	Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных. Периодичность и содержание работ по контролю обеспечения безопасности персональных данных. (План проверок, журнал проверок, акт проверки)	3
4	2	17	Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.	2, 3,
4	2	18	Обязанности оператора, осуществляющего обработку персональных данных. Порядок и условия обработки персональных данных без средств автоматизации. Порядок и методы обезличивания персональных данных, их обезличивание. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.	2, 4, 11-15

6. Содержание коллоквиумов

Коллоквиумы учебным планом не предусмотрены.

7. Перечень практических занятий

№ темы	Всего часов	Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	4	5
2	4	Определение необходимых уровней защищенности персональных данных при их обработке в ИСПДн в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных.	2, 16
2	8	Разработка модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных на конкретных примерах.	3, 16
3	8	Оценка соответствия средств защиты информации. Применимость технических и программных средств защиты информации при защите информационных систем персональных данных для различных уровней защищенности.	1, 2, 16
3	8	Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.	1, 2, 3, 16
4	4	Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных на конкретных примерах.	1, 2, 3, 16
4	4	Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации.	1, 2, 16

8. Перечень лабораторных работ

Лабораторные работы учебным планом не предусмотрены.

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение

1	2	3	4
1	20	Практика правоприменения законодательства в области персональных данных	4, 6, 10
	20	Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз.	1, 3, 7, 8, 9
3	4	Защита машинных носителей персональных данных (порядок уничтожения персональных данных и машиночитаемых носителей информации, используемых в обработке персональных данных)	1, 3, 11, 12, 13, 14, 15
3	5	Обеспечение целостности информационной системы и персональных данных (CRC, алгоритмы хеширования)	1, 3, 11, 12, 13, 14, 15
3	6	Анализ защищенности персональных данных	1, 3, 11, 12, 13, 14, 15
3	5	Обеспечение доступности персональных данных (backup)	1, 3, 11, 12, 13, 14, 15
4	10	Особенности обработки персональных данных в условиях государственной гражданской службы и муниципальной службы.	1, 3, 11, 12, 13, 14, 15

Виды, график контроля СРС, (по решению кафедры УМКС).

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
4 семестр			
1-3	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация), экзамен
4-7	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	Экзамен

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС [16].

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Курсовая работа учебным планом не предусмотрена.

12. Курсовой проект

Курсовой проект учебным планом не предусмотрен.

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

В процессе освоения образовательной программы формируется отдельные элементы компетенций ПК-4, ПК-6, ПК-9, ПК-13. Содержание лекционного курса и практических занятий формируют на рассматриваемом этапе элементы компетенций в части, касающейся защиты персональных данных.

Процедура оценивания знаний, умений и навыков проводится в соответствии со следующими методическими материалами и заключается в проведении устного экзаменационного опроса в виде диалога преподавателя со студентом, цель которого – систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала; отчетов по лабораторным работам, для оценки способности студента применить полученные ранее знания для организации системы защиты персональных данных, в проведении модулей и коллоквиумов, как способов межсессионной проверки знаний, умений, навыков студента в середине семестра по пройденным темам изучаемого предмета.

Показателем оценивания степени усвоения знаний этих элементов компетенций, является оценка, полученная на экзамене при ответе на вопросы для экзамена. Оценка выставляется по четырехбалльной шкале, соответствующей оценкам «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и осуществляется путем анализа ответа на вопросы для зачета. При этом руководствуются следующими критериями.

Оценка	Критерии оценивания результатов обучения (дескрипторы)
Отлично	заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой.
Хорошо	заслуживает обучающийся, обнаруживший полное знание учебного материала, усвоивший основную литературу, рекомендованную в программе. Оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по дисциплине и

	способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.
Удовлетворительно	заслуживает обучающийся, обнаруживший знания основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, знакомых с основной литературой, рекомендованной программой. Оценка выставляется обучающимся, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.
Неудовлетворительно	выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебного материала. Оценка ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании образовательного учреждения без дополнительных занятий по рассматриваемой дисциплине.

Умения и навыки, приобретенные студентом на этапе освоения указанных частей компетенций при преподавании рассматриваемой дисциплины, оцениваются по результатам выполнения практических работ, включающих одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описание результата, который нужно получить. Показателем оценивания степени усвоения знаний элементов компетенций, является оценка, полученная при ответе на практических занятиях. Оценка выставляется по четырехбальной шкале, соответствующей оценкам «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и осуществляется путем анализа представленного материала в ответ на практические контрольные задания. При этом руководствуются следующими критериями:

Оценка	**Критерии оценивания результатов обучения (дескрипторы)**
Отлично	выставляется студенту, если задание выполнено в полном объёме с соблюдением необходимой последовательности. Студенты работают полностью самостоятельно: подбирают необходимые для выполнения предлагаемых работ в задании источники знаний, показывают необходимые для проведения практической работы теоретические знания, практические умения и навыки.
Хорошо	выставляется студенту, если задание выполнено в полном объёме и самостоятельно. Допускаются

	отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Студенты используют указанные преподавателем источники знаний, включая страницы атласа, таблицы из приложения к учебнику, страницы из справочной литературы по предмету. Задание показывает знание учащихся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Могут быть неточности и небрежность в оформлении результатов работы.
Удовлетворительно	выставляется студенту, если задание на лабораторную работу выполняется и оформляется студентами при помощи преподавателя или хорошо подготовленных и уже выполненных на «отлично» данную работу студентов. На выполнение задания затрачивается много времени (можно дать возможность доделать работу дома). Студенты показывают знания теоретического материала, но испытывают затруднение при решении конкретной задачи.
Неудовлетворительно	выставляется, если студенты показывают плохое знание теоретического материала и отсутствие умения применить знания к решению практической задачи. Руководство и помощь со стороны преподавателя и хорошо подготовленных студентов неэффективны по причине плохой подготовки студента.

Вопросы для зачета

Зачет учебным планом не предусмотрен.

Вопросы для экзамена

1. Законодательная и нормативная база правового регулирования вопросов защиты персональных данных.
2. Федеральный закон "О персональных данных". Основные положения.
3. Понятие информационной системы персональных данных.
4. Определение необходимых уровней защищенности персональных данных при их обработке в ИСПДн.
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
6. Основные типы угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
8. Порядок выбора организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн.
9. Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных (Методический документ ФСТЭК «Меры защиты информации в ГИС»).
10. Оценка соответствия средств защиты информации.
11. Технические и программные средства защиты информации, применяемые при защите информационных систем персональных данных для различных уровней защищенности.
12. Обеспечение безопасности персональных данных с использованием средств криптографической защиты информации.
13. Порядок лицензирования операторов информационных систем персональных данных.
14. Разработка технического обоснования для создания системы защиты информационных систем персональных данных.
15. Порядок внедрения средств обеспечения информационной безопасности информационных системах персональных данных (комплект документов).
16. Оценка эффективности ИСПДн.
17. Порядок и условия обработки персональных данных без средств автоматизации.
18. Порядок и методы обезличивания персональных данных, их обезличивание.

Тестовые задания по дисциплине

Нормативно-правовое обеспечение безопасности ПДн

1.

Действие ФЗ-152 распространяется на отношения, возникающие, в том числе при:

А) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации

Б) обработке персональных данных, осуществляемой федеральными органами государственной власти, с использованием средств автоматизации

В) обработке персональных данных физическими лицами без использования средств автоматизации исключительно для личных и семейных нужд

Г) обработке персональных данных, осуществляемой органами местного самоуправления с использованием средств автоматизации

2.

Под блокированием персональных данных понимают:

А) действия, направленные на предотвращение раскрытия персональных данных неопределенному кругу лиц

Б) временное прекращение обработки персональных данных

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

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

3.

К специальным категориям персональных данных отнесены:

А) персональные данные, касающиеся расовой принадлежности

Б) персональные данные, включенные в общедоступные источники персональных данных без согласия субъектов персональных данных

В) паспортные данные

Г) персональные данные, касающиеся состояния здоровья

4.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

А) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления

Б) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц

В) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного в

Г) всё выше перечисленное

5.

Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ-152 и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, установлен

А) Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"

Б) Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

В) Постановление Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми а

Г) Приказом ФСЭК от 11.02.2013 N 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

6.

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям ФЗ-152, является

А) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности

Б) федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи

В) федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации

Г) все вышеперечисленные

7.

В случае достижения цели обработки персональных данных оператор обязан:

А) прекратить обработку персональных данных (или обеспечить ее прекращение) и уничтожить персональные данные (или обеспечить их уничтожение), если иное не предусмотрено договором, иным соглашением между оператором и субъектом персональных данных

Б) осуществить блокирование обрабатываемых персональных данных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные (или обеспечить их уничтожение

В) осуществить обезличивание обрабатываемых персональных данных или обеспечить их обезличивание (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора)

Г) осуществить блокирование обрабатываемых персональных данных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечить хранение таких персональных данных в информационных системах

8.

Уничтожение персональных данных включает в себя:

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

Б) действия, в результате которых уничтожаются материальные носители персональных данных

В) действия, в результате которых становится невозможным определить принадлежность персональных данных конкретному субъекту персональных данных

Г) временное прекращение обработки персональных данных

9.

Уведомление о намерении осуществлять обработку персональных данных оператором направляется в:

А) ФСТЭК

Б) ФСБ

В) Роскомнадзор

Г) всё выше перечисленное

10.

Лицо, ответственное за организацию обработки персональных данных, обязано:

А) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

Б) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

В) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов

Г) всё выше перечисленное

Обезличивание ПДн

11.

Обезличивание ПД бывает:

a. Абсолютное
b. Относительное
c. Полное
d. Частное

12.

Свойства обезличенных данных:

a. Полнота
c. Релевантность
d. Стойкость
e. Структурированность
f. Обратимость
b. Анонимность

13.

Свойства методов обезличивания:

a. Изменяемость
c. Вариативность

d. Стойкость
e. Структурированность
f. Обратимость
b. Анонимность

14.

Метод обезличивания при котором производится замена части сведений идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным

a. метод введения идентификаторов
b. метод изменения состава или семантики
c. метод декомпозиции
d. метод перемешивания

15.

Метод обезличивания при котором производится изменение состава или семантики персональных данных путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений

a. метод введения идентификаторов
b. метод изменения состава или семантики
c. метод декомпозиции
d. метод перемешивания

16.

Метод обезличивания при котором производится разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств

a. метод введения идентификаторов
b. метод изменения состава или семантики
c. метод декомпозиции
d. метод перемешивания

17.

Метод обезличивания при котором производится перестановка отдельных значений или групп значений атрибутов персональных данных в массиве персональных данных

a. метод введения идентификаторов
b. метод изменения состава или семантики
c. метод декомпозиции
d. метод перемешивания

Основы безопасности

18.

Класс защищённости информационной системы определяется:

политикой безопасности организации
количеством потенциальных угроз и объёмом информационных массивов системы
уровнем значимости информации и масштабом системы

19.

Выделите характеристики информации, степень возможного ущерба которых определяет уровень значимости информации

целостность
доступность
конфиденциальность
аутентичность
достоверность

20.

На каком шаге выбора мер защиты информации выполняется исключение мер:

адаптация базового набора мер
определение базового набора мер
уточнение адаптированного базового набора мер
дополнение уточненного адаптированного набора мер

21.

К средствам блокирования угроз относятся:

средства экранирования
средства антивирусной защиты
системы обнаружения вторжений

22.

Аутентификация - это:

контроль процедуры идентификации
внутреннее ограничение сервиса
матрица доступа

23.

К пассивным угрозам относятся:

раскрытие содержимого сообщений
анализ потока данных
фальсификация
модификация

24.

При каком виде атаки нарушается конфиденциальность информации:

перехват
разъединение
модификация
фальсификация

25.

При каком виде атаки нарушается целостность информации:

модификация
разъединение
перехват
фальсификация

26.

Под политикой безопасности понимается:

набор документированных управленческих решений (законов, правил и норм поведения), определяющих, как организация обрабатывает, защищает и распространяет информацию
формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей
управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем

27.

На каком уровне эталонной модели OSI регламентируется межсетевое взаимодействие?

на сетевом
на сеансовом
на транспортном
на канальном

28.

Какого типа брандмауэров не существует?

Шлюз физического уровня
Экранирующий маршрутизатор
Шлюз сеансового уровня
Шлюз прикладного уровня

29.

Какая из нижеперечисленных функций обычно межсетевым экраном не выполняется?

Шифрование исходящей информации
Идентификация и аутентификация пользователей
Фильтрация информационных потоков

Разграничение доступа к ресурсам внешней сети

30.

IDS - это:

система обнаружения вторжений
протокол Интернет
алгоритм шифрования

31.

Виртуальная частная сеть VPN строится на основе:

межсетевого экрана
маршрутизатора
коммутатора

32.

Демилитаризованная зона - это:

область сети с минимальным уровнем защищенности и максимальной степенью доступа
максимально защищенная часть сети
область сети, на которую не распространяется действие межсетевого экрана

Основы технической защиты ПДн

33.

Каковы основные преимущества защищенного электронного документооборота по сравнению с ручным?

а- оперативный доступ к информации;
б- сохранность информации;
в- конфиденциальность информации;
г- гарантированная подлинность подписанного документа;
д- исключение дублирования данных;
е- все вышеперечисленные преимущества

34.

Каковы основные критерии выбора поставщиков средств защиты информации?

а- наличие фирмы производителя в реестре сертификационных органов;
б- уровень защищенности ИС;
в- назначение технического средства;
г- все вышеперечисленные;

35.

Какой федеральный орган ведет реестр сертифицированных криптографических средств защиты информации?

а- ФСТЭК России
б- ФСБ России
в- Роскомнадзор

36.

С помощью, каких средств и мероприятий обеспечивается защита информации от НСД на уровне прикладного и системного ПО?

а- разграничения доступа к информации;
б- идентификации и аутентификации;
в- аудита и мониторинга;
г- использования аппаратных ключей;
д- установки межсетевых экранов;
е- внедрения средств антивирусной защиты.

37.

С помощью каких средств и мероприятий обеспечивается защита информации от утечки по техническим каналам?

а- использования экранированного кабеля;
б- использования экранированного оборудования;
в- установки активных систем зашумления;

г- создания контролируемых зон;
д- внедрения средств анализа защищенности;
е- установки средств блокировки устройств и интерфейсов ввода-вывода информации;
ж- установки на линиях связи высокочастотных фильтров;
з- построения экранированных помещений.

38.

Какие составляющие ИС можно выделить для ее защиты от НСД?

а- прикладное и системное ПО и аппаратная часть северов и рабочих станций;
б- прикладное и системное ПО, аппаратная часть серверов и рабочих станций, коммуникационное оборудование и каналы связи, периметр информационной системы.

39.

Техническая разведка - это:

а- Скрытное получение научно-технической информации
б- Скрытное получение произвольной информации
в- Скрытное получение требуемых сведений о технических каналах утечки информации
г- Скрытное получение требуемых сведений с использованием технических каналов утечки информации

40.

Укажите правильные варианты утверждения: "Технические каналы утечки информации включают:

а- визуально-оптический канал
б- электромагнитный канал
в- радиочастотный канал
г- виброакустический канал
д- видеоканал

41.

Скремблирование - это:

а- применение кодовых фраз при передаче речевой информации
б- применение шифрования сигнала, передаваемого в линии связи
в- метод соблюдения дисциплины связи
г- применение кодирования речевого сигнала, передаваемого в линии связи

42.

Опасность ПЭМИН состоит в:

а- возможности удаленного администрирования сервера локальной сети
б- возможности несанкционированного доступа к служебной информации
в- возможности перехвата информации, обрабатываемой с помощью ОТСС
г- повышении вероятности сбоев и отказов при функционировании ОТСС

43.

Какой комплексный показатель определяется согласно ПП-1119:

а- класс информационной системы персональных данных.
б- уровень защищенности персональных данных.
в- уровень защищенности информационной системы персональных данных
г- класс государственной информационной системы

Угрозы безопасности ПДн

44.

Частота реализации угрозы является маловероятной когда:

a) отсутствуют объективные предпосылки для осуществления угрозы;
b) объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию
c) объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
d) объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты

45.

Частота реализации угрозы имеет низкую вероятность когда:

a) отсутствуют объективные предпосылки для осуществления угрозы;
b) объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию
c) объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
d) объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты

46.

Частота реализации угрозы имеет среднюю вероятность когда:

a) отсутствуют объективные предпосылки для осуществления угрозы;
b) объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию
c) объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
d) объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты

47.

Частота реализации угрозы имеет высокую вероятность когда:

a) отсутствуют объективные предпосылки для осуществления угрозы;
b) объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию
c) объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
d) объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты

48.

Показатель опасности угрозы является низким

a) если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
b) если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
c) если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.
d) если реализация угрозы не несет последствия для субъектов персональных данных;

49.

Показатель опасности угрозы является средним

a) если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
b) если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
c) если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.
d) если реализация угрозы не несет последствия для субъектов персональных данных;

50.

Показатель опасности угрозы является высоким

a) если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
b) если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
c) если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.
d) если реализация угрозы не несет последствия для субъектов персональных данных;

51.

Если 0?Y?0.3 (Y - коэффициент реализуемости угрозы), то возможность реализации угрозы признается

a) Низкой
b) Средней
c) Высокой
d) Очень высокой

52.

Если 0.3<Y?0.6 (Y - коэффициент реализуемости угрозы), то возможность реализации угрозы признается

a) Низкой
b) Средней
c) Высокой
d) Очень высокой

53.

Если 0.6<Y?0.8 (Y - коэффициент реализуемости угрозы), то возможность реализации угрозы признается

a) Низкой
b) Средней
c) Высокой
d) Очень высокой

54.

Если Y>0.8 (Y - коэффициент реализуемости угрозы), то возможность реализации угрозы признается

a) Низкой
b) Средней
c) Высокой
d) Очень высокой

Электронная подпись

55.

Обработка биометрических персональных данных может осуществляться

без согласия субъекта персональных данных
только с согласия субъекта персональных данных

56.

Перечислите функции электронной подписи:

контроль целостности
невозможность отказа от авторства
доказательное подтверждение авторства документа
конфиденциальность

57.

Виды электронной подписи:

простая
усиленная квалифицированная
усиленная неквалифицированная
усложненная
простая неквалифицированная

58.

Простая электронная подпись позволяет

установить личность лица, подписавшего документ
установить факт изменения содержимого документа
установить личность лица, подписавшего документ и факт изменения содержимого документа.

59.

Для использования усиленной электронной подписи ее владелец получает:

ключ электронной подписи и ключ проверки электронной подписи

ключ электронной подписи

ключ проверки электронной подписи

60.

Определить показатели и рассчитать уровень исходной защищенности для следующего примера: База данных, содержащих ПДн рабочих авиационного завода (государственное учреждение), где проектируют, конструируют и тестируют двигатели к гражданским самолетам. Рабочие допущены к информации, составляющей служебную тайну. База данных ПДн содержит информацию о состоянии здоровья рабочих, семейном положении, паспортных данных, профессиональных навыках (квалификация, разряд), номерах дипломов о высшем образовании.

1. Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации

2. Имеет многоточечный выход в глобальную сеть общего пользования

3. Возможные операции: запись, удаление, сортировка

4. Доступ к ИСПДн имеют ограниченный круг лиц

5. ИСПДн принадлежит одному организации-владельцу

6. Данные в ИСПДн не обезличиваются

7. ИСПДн не предоставляет ПДн сторонним пользователям

61.

Определить типы угроз в соответствии с Моделью угроз для ИСПДн представленной выше организации.

62.

Для примера п.60 рассчитать актуальные угрозы, связанные с НСД к ПД.

63.

Для примера п.60 рассчитать актуальные угрозы, связанные с ПЭМИН.

64.

Для примера п.60 определить утечки по оптическим каналам.

65.

Для актуальных угроз из примера п.60 определить набор технических и программных средства защиты информации, применяемых при защите информационных систем персональных данных для их нейтрализации.

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВПО в рамках учебного курса предусмотрены активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В связи с этим предусмотрено применение мультимедийных средств и презентаций, обсуждение докладов студентов, лекции с элементами деловых игр, тестирование, консультации, решение ситуационных задач, дискуссии.

Общее количество занятий, проводимых в интерактивных формах, не менее 28.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обязательные издания

1. Аверченков В.И. Защита персональных данных в организации [Электронный ресурс]: монография/ Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 124 c.— Режим доступа: http://www.iprbookshop.ru/6993.— ЭБС «IPRbooks», по паролю
2. Губенков А. А. Обеспечение безопасности персональных данных : учеб. пособие для студ. направления 090303.65 "Информационная безопасность автоматизированных систем" и бакалавров направления 090900.62 "Информационная безопасность" / А. А. Губенков. - Саратов : СГТУ, 2015. - 1эл. опт. диск (CD-ROM): ил., табл. - Электронный аналог печатного издания. Режим доступа: http://lib.sstu.ru/books/zak 51_15.pdf
3. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 121 c.— Режим доступа: http://www.iprbookshop.ru/16708.— ЭБС «IPRbooks», по паролю

Дополнительные издания

4. Петрыкина Н.И. Правовое регулирование оборота персональных данных [Электронный ресурс]: теория и практика/ Петрыкина Н.И.— Электрон. текстовые данные.— М.: Статут, 2011.— 135 c.— Режим доступа: http://www.iprbookshop.ru/28992.— ЭБС «IPRbooks», по паролю
5. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем [Электронный ресурс]/ А.В. Благодаров [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 116 c.— Режим доступа: http://www.iprbookshop.ru/37183.— ЭБС «IPRbooks», по паролю
6. Кухаренко Т.А. Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (2-е издание переработанное и дополненное) [Электронный ресурс]/ Кухаренко Т.А.— Электрон. текстовые данные.— Саратов: Ай Пи Эр Медиа, 2012.— 197 c.— Режим доступа: http://www.iprbookshop.ru/21134.— ЭБС «IPRbooks», по паролю

Периодические издания

7. Вестник СГТУ (http://lib.sstu.ru/index.php/menuskrellib/91-mperiodizdan)
8. Инновационная деятельность (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsionnaya-deyatelnost/)
9. Журнал «Инновации + Паблисити» (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsii-pablisiti/)
10. Информационная безопасность регионов (http://www.seun.ru/content/nauka/5/1/index.php).

Интернет-ресурсы

11. Искусство управления информационной безопасностью. URL:http://iso27000.ru/ (дата обращения: 1.06.2015).
12. SecurityLab.ru - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. URL:http://www.securitylab.ru/ (дата обращения: 1.06.2015).
13. Архив изданий по информационной безопасности. URL:http://www.itsec.ru/ (дата обращения: 1.06.2015).
14. Информационный ресурс по безопасности. URL:http://www.securrity.ru (дата обращения: 1.06.2015).
15. Информационная безопасность вашего бизнеса. URL:http://www.leta.ru (дата обращения: 1.06.2015).

Источники ИОС

16. Весь лекционный материал размещен в электронной форме в ИОС направления ИБС интернет-ресурсов СГТУ имени Гагарина Ю.А. https://portal.sstu.ru/Fakult/FETIP/IBS/b324_/default.aspx.

16. Материально-техническое обеспечение дисциплины.

Для осуществления образовательного процесса по дисциплине необходима типовая лекционная аудитория, оснащенная маркерной доской; персональным компьютером; проектором или большим монитором; программным обеспечением Microsoft Office Профессиональный плюс 2007 или Microsoft Office Профессиональный плюс 2010.

Для проведения практических занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор Pentium IV 3 ГГц, ОЗУ 2 Гбайта, НЖМД 200 Гбайт с пакетом программ Microsoft Office Профессиональный плюс 2007 или Microsoft Office Профессиональный плюс 2010.