

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ



Заведующий кафедрой
информационных систем
доцент Борисов Д.Н.,
подпись, расшифровка подписи
10.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ФТД.В.01 Защита персональных данных

Код и наименование дисциплины в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

09.03.02 Информационные системы и технологии

2. Профиль подготовки/специализация: Инженерия информационных систем и технологий

3. Квалификация выпускника: Бакалавр

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: информационных систем

6. Составители программы: Борисова Алла Александровна, доцент

7. Рекомендована: НМС ФКН, протокол № 5 от 05.03.2024.

(наименование рекомендующей структуры, дата, номер протокола,

отметки о продлении вносятся вручную)

8. Учебный год: 2027-2028

Семестр(ы): 7

9. Цели и задачи учебной дисциплины

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- понимание основных аспектов защиты персональных данных;
- изучение предъявляемых требований и мер, необходимых для обеспечения защиты персональных данных;

Задачи учебной дисциплины:

- приобретение практических навыков проектирования систем защиты персональных данных согласно требованиям законодательства Российской Федерации.

10. Место учебной дисциплины в структуре ООП дисциплина относится к дисциплинам, формируемой участниками образовательных отношений. Факультативы. Требуется предварительное знание информатики, введение в программирование.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий;	ОПК-6.2 Умеет применять методы алгоритмизации, языки и технологии программирования при решении профессиональных задач в области информационных систем и технологий	Знать: основные стадии разработки ПО, принцип декомпозиции задач, возможности современных программных сред и специализированных библиотек для разработки программных средств защиты конфиденциальности информации, контроля целостности данных. Уметь: выбирать программные средства и библиотеки для реализации, моделирования и исследования алгоритмов защиты персональных данных. Владеть: навыками планирования стадий исследования с подбором программной среды для компьютерного моделирования и проведения экспериментов
ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий;	ОПК-6.3 Имеет навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач	Знать: алгоритмы обработки полученных результатов исследований с использованием стандартных методов (методик) Уметь: Обработать полученные результаты исследований с использованием стандартных методов (методик) Владеть: Обработкой полученных результатов исследований с использованием стандартных методов (методик)

12. Объем дисциплины в зачетных единицах/час — 2 / 72

Форма промежуточной аттестации зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы	№ сем. 7	Всего
Аудиторные занятия	32	32
лекции	16	16
практические	16	16
лабораторные	0	0
Самостоятельная работа	40	40
Форма промежуточной аттестации (зачет – час..)	зачет	
Итого:	72	72

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Основы защиты информационных систем персональных данных	Основные характеристики информационной системы персональных данных (ИСПД). Обработка персональных данных (ПД).	
1.2	Законодательство в сфере защиты ПД	ФЗ-152, Постановление Правительства РФ №1119, основные документ ФСТЭК и ФСБ в сфере защиты ПД. Категории ПД.	
1.3	Требования по обеспечению безопасности ПД	Набор требований, определяющих выбор мер защиты ПД в ИСПД.	
1.4	Основные этапы разработки систем защиты персональных данных (СЗПД)	Основные этапы разработки систем защиты персональных данных (СЗПД): обследование, моделирование угроз, определение требований и выбор мер защиты ПД, реализация мер защиты, проверка выполнения требований.	
1.5	Документационное обеспечение СЗПД	Виды документов, разрабатываемых при создании СЗПД	
1.6	Моделирование угроз безопасности ПД	Определение актуальных нарушителей и угроз безопасности ПД на основе Методики ФСТЭК 2021. Определение уровня защищённости ИСПД.	
1.7	Проектирование СЗПД часть 1	Проектирование СЗПД для определения перечня мер, необходимых для обеспечения безопасности ПД на основе предъявляемых требований.	
1.8	Проектирование СЗПД часть 2	Выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности ПД	
1.9	Испытания и ввод в действие СЗПД	Определение состава и содержания проверок реализации мер защиты ПД, проведение проверок. Подтверждение соответствия принятых мер требованиям по обеспечению безопасности ПД, ввод в действие СЗПД.	
2. Практические занятия			
2.1	Моделирование ИСПД	Разработка практической модели ИСПД, определение бизнес-процессов, требующих обработки ПД, и видов обработки ПД.	
2.2	Определение требований к СЗПД	Определение набора требований на основе Постановления Правительства РФ №1119, основных документов ФСТЭК и ФСБ в сфере защиты ПД.	

2.3	Моделирование угроз безопасности ПД, определение уровня защищённости ИСПД	Определение актуальных нарушителей и угроз безопасности ПД на основе Методики ФСТЭК 2021. Определение уровня защищённости ИСПД.	
2.4	Формирование документа на разработку СЗПД	Формирование документа на разработку СЗПД, определяющего перечень мер, необходимых для обеспечения безопасности ПД на основе предъявляемых требований.	
2.5	Формирование документов, определяющих функции средств защиты информации	Формирование документов, определяющих выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности ПД.	
2.6	Формирование эксплуатационной документации	Формирование документов, содержащих описание настроек средств защиты информации, порядок действий для проверки функционирования средств защиты и их настроек.	
2.7	Формирование документации по испытаниям и вводу в действие СЗПД	Формирование программы и методики испытаний, документа оценки эффективности принятых мер, ввод в действие СЗПД	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				Всего
		Лекции	Практические	Лабораторные	Самостоятельная работа	
1	Основы защиты информационных систем персональных данных	1	1		4	6
2	Законодательство в сфере защиты ПД	1	1		4	6
3	Требования по обеспечению безопасности ПД	2	1		4	7
4	Основные этапы разработки систем защиты персональных данных (СЗПД)	2	2		4	8
5	Документационное обеспечение СЗПД	2	1		4	7
6	Моделирование угроз безопасности ПД	2	1		4	7
7	Проектирование СЗПД часть 1	2	3		6	11
8	Проектирование СЗПД часть 2	2	3		6	11
9	Испытания и ввод в действие СЗПД	2	3		4	9
	Итого	16	16		40	72

14. Методические указания для обучающихся по освоению дисциплины

Студентам читать рекомендованную литературу, во время проверки выполнения лабораторных работ, преподавателю рекомендуется проводить теоретический опрос с целью определения степени усвоения материала.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова. — Уфа : БашГУ, 2020. — 120 с. — ISBN 978-5-7477-5228-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179914
2	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-8370-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/175506

б) дополнительная литература:

№ п/п	Источник
1	Гусев, А. Ю. Судебная практика о применении законодательства, регулирующего вопросы защиты персональных данных : учебное пособие / А. Ю. Гусев. — Москва : Проспект, 2019. — 63 с. — ISBN 978-5-392-29690-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/151026
2	Дупан (Гутникова), А. С. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет : монография / А. С. Дупан (Гутникова), А. Б. Жулин, А. К. Жарова ; под редакцией Дупан (Гутниковой) А.С.. — Москва : Высшая школа экономики, 2016. — 344 с. — ISBN 978-5-7598-1386-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100135
3	Ильин, О. Ю. Актуальные вопросы российского права: защита персональных данных, антикоррупционное законодательство, правовой статус личности, противодействие терроризму и экстремистской деятельности : учебное пособие / О. Ю. Ильин. — Тверь : ТвГТУ, 2020. — 104 с. — ISBN 978-5-7995-1114-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171323

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1.6	www.lib.vsu.ru – ЗНБ ВГУ

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для спо / В. И. Петренко, И. В. Мандрица. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744
2	Организация защиты персональных данных : учебное пособие / составители А. М. Макаров [и др.]. — Ставрополь : СКФУ, 2015. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155243

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

- 1) лекционная аудитория, оснащенная мультимедиа проектором;
- 2) класс для проведения практических занятий;

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Раздел дисциплины (модуля)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Моделирование ИСПД и определение требований к СЗПД	ОПК-6	ОПК-6.2 ОПК-6.3	Контрольная работа 1
2	Моделирование угроз безопасности ПД, определение уровня защищённости ИСПД	ОПК-6	ОПК-6.2 ОПК-6.3	Контрольная работа 2
3	Проектирование, испытания и ввод в действие СЗПД	ОПК-6	ОПК-6.2 ОПК-6.3	Контрольная работа 3

Промежуточная аттестация

Форма контроля – зачет

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- Устный опрос на практических занятиях;
- Контрольная работа по теоретической части курса;
- Практические работы.

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос на практических занятиях	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной ниже
3	Практическая работа	Содержит 9 практических заданий,	При успешном выполнении работы ставится оценка

		предусматривающих разработку, тестирование и эксплуатацию различных криптографических и стеганографических алгоритмов.	зачтено, в противном случае ставится оценка не зачтено
--	--	--	--

Пример задания для выполнения практической работы

Контрольная работа 1

Вариант 1

- 1) Основные характеристики информационной системы персональных данных.
- 2) Набор требований, определяющих выбор мер защиты персональных данных и в информационной системы персональных данных.
- 3) Определение набора требований на основе Постановления Правительства РФ №1119, основных документов ФСТЭК и ФСБ в сфере защиты персональных данных.

Вариант 2

- 1) Обработка персональных данных.
- 2) Набор требований, определяющих выбор мер защиты персональных данных и в информационной системы персональных данных.
- 3) Разработка практической модели информационной системы персональных данных, определение бизнес-процессов, требующих обработки персональных данных, и видов обработки персональных данных.

Вариант 3

- 1) Основные характеристики информационной системы персональных данных.
- 2) ФЗ-152, Постановление Правительства РФ №1119, основные документ ФСТЭК и ФСБ в сфере защиты персональных данных. Категории персональных данных.
- 3) Определение набора требований на основе Постановления Правительства РФ №1119, основных документов ФСТЭК и ФСБ в сфере защиты персональных данных.

Контрольная работа 2

Вариант 1

- 1) Основные этапы разработки систем защиты персональных данных (СЗПД): обследование, моделирование угроз, определение требований и выбор мер защиты персональных данных, реализация мер защиты, проверка выполнения требований.
- 2) Определение актуальных нарушителей и угроз безопасности персональных данных на основе Методики ФСТЭК 2021.

Вариант 2

- 1) Виды документов, разрабатываемых при создании систем защиты персональных данных
- 2) Определение уровня защищённости информационной системы персональных данных.

Вариант 3

- 1) Определение актуальных нарушителей и угроз безопасности персональных данных на основе Методики ФСТЭК 2021.

2) Формирование документа на разработку систем защиты персональных данных, определяющего перечень мер, необходимых для обеспечения безопасности персональных данных на основе предъявляемых требований.

Контрольная работа 3

Вариант 1

1) Проектирование систем защиты персональных данных для определения перечня мер, необходимых для обеспечения безопасности персональных данных на основе предъявляемых требований.

2) Определение состава и содержания проверок реализации мер защиты персональных данных, проведение проверок.

3) Формирование программы и методики испытаний, документа оценки эффективности принятых мер, ввод в действие систем защиты персональных данных

Вариант 2

1) Выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности персональных данных

2) Подтверждение соответствия принятых мер требованиям по обеспечению безопасности ПД, ввод в действие систем защиты персональных данных.

3) Формирование документов, содержащих описание настроек средств защиты информации, порядок действий для проверки функционирования средств защиты и их настроек

Вариант 3

1) Проектирование систем защиты персональных данных для определения перечня мер.

2) Проектирование систем защиты персональных данных выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности персональных данных.

3) Формирование программы и методики испытаний, документа оценки эффективности принятых мер, ввод в действие систем защиты персональных данных

Приведенные ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний:

ОПК-6

Задания закрытого типа

1. Общедоступные персональные данные – это

а) Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных;

б) Персональные данные, доступ неограниченного круга лиц к которым предоставлен в соответствии с федеральными законами;

в) Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2. Специальные категории персональных данных – это

а) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

б) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни;

в) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни;

г) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости.

3. Трансграничная передача персональных данных – это

а) Передача персональных данных на территорию иностранного государства;

б) Передача персональных данных на территорию другого субъекта РФ органу власти данного субъекта, физическому лицу или юридическому лицу данного субъекта РФ;

в) Передача персональных данных на территорию иностранного государства или органу власти иностранного государства;

г) Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

4. Целостность информации – это

а) Состояние информации, при котором отсутствует любое ее изменение;

б) Состояние информации, при котором изменение осуществляется только преднамеренно субъектами, имеющими на него право;

в) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

5. Что такое персональные данные?

а) Любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

б) Информация о частной жизни физического лица, доступ к которой он решил ограничить;

в) Сведения о религиозных убеждениях, политических взглядов, расовой и национальной принадлежности субъекта персональных данных;

г) Любые сведения независимо от формы их представления.

6. Оператор персональных данных - это:

а) Государственный орган, осуществляющий автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке;

б) Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

в) Юридическое лицо, осуществляющее автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке;

г) Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, но не определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

7. Обработка персональных данных - это

а) Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных);

б) Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, осуществляемые с помощью средств вычислительной техники;

в) Чтение, запись, сортировка, модификация, передача персональных данных в информационной системе.

8. Распространение персональных данных это

а) Действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

б) Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

в) Передача персональных данных оператору персональных данных.

9. Предоставление персональных данных это

а) Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

б) Действия, направленные на раскрытие персональных данных по мотивированному запросу.

10. Уничтожение персональных данных это

а) Действия, в результате которых становится невозможно определить субъекта персональных данных в информационной системе 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) Удаление персональных данных из информационной системы персональных данных;

г) Действия, направленные на уничтожение носителей персональных данных.

Задания открытого типа

1. Какой срок в соответствии с ФЗ-152 предусмотрен для сообщения субъекту (его представителю) Оператором информации о наличии ПДн и предоставить возможность ознакомления с ними? _____ -

2. Если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные в срок не превышающий: _____ рабочих дней

3. На сколько групп подразделяются классы защищенности автоматизированной системы обработки информации?

4. Кто должен своевременно обнаруживать факты несанкционированного доступа к персональным данным? _____

5. К какой категории относятся персональные данные, позволяющие идентифицировать субъекта? _____

6. Какое свойство информации требуется обеспечить в типовых информационных системах обработки персональных данных? _____

7. Сколько органов по сертификации действует в России? _____

8. Какой срок действия у сертификата средства защиты информации? _____

9. Какой орган является регулятором в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПД (не криптографическими методами) при их обработке в ИСПД? _____

10. _____ – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его ФИО, дата рождения, имущественное, социальное положение, другая информация

Задания с развернутым ответом

1. Васечкин, ответчик по гражданскому делу № 2-6131/15, увидел на сайте Воронежского городского суда текст судебного акта по данному делу и свои фамилию, имя и отчество в тексте судебного акта. Васечкин не подписывал соглашения на обработку персональных данных. Васечкину не понравилось, что его персональные данные фигурируют в судебном акте, так как это компрометирует его как недобросовестного подрядчика по договору строительного подряда. Оцените ситуацию. Правомерны ли действия суда?

Решение задачи должно быть обосновано правовыми нормами.

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня практических работ, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Соотношение показателей, критериев и шкалы оценивания результатов обучения представлено в следующей таблице.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, выполнение заданий, предусмотренных программой, знакомство с основной литературой, рекомендованной программой. Присутствуют погрешности в ответе на зачете и при выполнении контрольных заданий.		<i>Зачет</i>
Имеются пробелы в знаниях основного учебно-программного материала, принципиальные ошибки в выполнении предусмотренных программой заданий, наличие которых препятствует дальнейшему обучению студента.		<i>Не зачет</i>

КИМ формируется из трех теоретических вопросов и одной практической задачи.

Перечень вопросов к зачету:

1. Основные характеристики информационной системы персональных данных (ИСПД). Обработка персональных данных (ПД).
2. ФЗ-152, Постановление Правительства РФ №1119, основные документ ФСТЭК и ФСБ в сфере защиты ПД. Категории ПД.
3. Набор требований, определяющих выбор мер защиты ПД в ИСПД.

4. Основные этапы разработки систем защиты персональных данных (СЗПД): обследование, моделирование угроз, определение требований и выбор мер защиты ПД, реализация мер защиты, проверка выполнения требований.
5. Виды документов, разрабатываемых при создании СЗПД
6. Определение актуальных нарушителей и угроз безопасности ПД на основе Методики ФСТЭК 2021.
7. Определение уровня защищённости ИСПД.
8. Проектирование СЗПД для определения перечня мер, необходимых для обеспечения безопасности ПД на основе предъявляемых требований.
9. Выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности ПД
10. Определение состава и содержания проверок реализации мер защиты ПД, проведение проверок.
11. Подтверждение соответствия принятых мер требованиям по обеспечению безопасности ПД, ввод в действие СЗПД.
12. Разработка практической модели ИСПД, определение бизнес-процессов, требующих обработки ПД, и видов обработки ПД.
13. Определение набора требований на основе Постановления Правительства РФ №1119, основных документов ФСТЭК и ФСБ в сфере защиты ПД.
14. Определение актуальных нарушителей и угроз безопасности ПД на основе Методики ФСТЭК 2021.
15. Определение уровня защищённости ИСПД.
16. Формирование документа на разработку СЗПД, определяющего перечень мер, необходимых для обеспечения безопасности ПД на основе предъявляемых требований.
17. Формирование документов, определяющих выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности ПД.
18. Формирование документов, содержащих описание настроек средств защиты информации, порядок действий для проверки функционирования средств защиты и их настроек.
19. Формирование программы и методики испытаний, документа оценки эффективности принятых мер, ввод в действие СЗПД.