МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине «Защита персональных данных в информационных системах»
для студентов направления подготовки
10.03.01 Информационная безопасность
Направленность (профиль)
«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»

Ставрополь
2026

Содержание

Лабораторная работа № 1. Основные понятия и определения

Лабораторная работа № 2. Международное и национальное право в области защиты персональных данных

Лабораторная работа № 3. Содержание и основные положения Федерального закона Российской Федерации № 152-ФЗ «О персональных данных»

Лабораторная работа № 4. Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах

Лабораторная работа № 5. Особенности обработки биометрических персональных данных

Лабораторная работа № 6. Методика оценки угроз безопасности персональным данным

Лабораторная работа № 7. Оценка возможности реализации угроз безопасности персональным данным и определение их актуальности

Лабораторная работа № 8. База знаний о поведениях компьютерных злоумышленников

Лабораторная работа № 9. Построение системы защиты персональных данных

Лабораторная работа № 10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Лабораторная работа № 11. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

Лабораторная работа № 12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации

ВВЕДЕНИЕ

1. Цель и задачи освоения дисциплины

Цель освоения дисциплины «Защита персональных данных в информационных системах» является теоретическая и практическая подготовка бакалавра для проведения работ по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) в соответствии с современными требованиями, а также приобретение набора компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачи освоения дисциплины:

– формирование знаний нормативно-правовой документации в области персональных данных и умений работы с ней с использованием современных информационных технологий;

– формирование умений выявления угроз и уязвимостей безопасности персональных данных с подготовкой отчетов в цифровом или бумажном формате;

– формирование умений по разработке организационных и технических мер по обеспечению безопасности персональных данных;

– формирование навыков разработки организационно-распорядительных документов в области защиты персональных данных с использованием офисных приложений;

– формирование навыков самостоятельного изучения литературы в области обеспечения безопасности персональных данных с использованием инструментария электронных библиотечных систем, а также порталов регуляторов в области защиты информации.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИД-2 ОПК-5 Определяет рациональные меры по обеспечению организационной защиты на объекте; организует работу персонала с конфиденциальной информацией; разрабатывает проекты нормативных документов, регламентирующих работу по	– организует работу персонала с персональными данными – разрабатывает проекты нормативных документов, регламентирующих работу по защите персональных данных в информационных системах персональных данных, а

	защите информации, а также положений, инструкций и других организационно-распорядительных документов.	также положений, инструкций и других организационно-распорядительных документов
	ИД-3 ОПК-5 применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	– оценивает угрозы безопасности персональным данным в информационных системах персональных данных на основе нормативных и методических документов, регламентирующих деятельность по защите персональных данных
ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ИД-1 ОПК-2.3 Разрабатывает, внедряет и сопровождает комплексы мер по обеспечению безопасности защиты персональных данных в информационных системах	– разрабатывает, внедряет и сопровождает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных – разрабатывает внедряет и сопровождает комплекс мер по построению системы защиты персональных данных

Лабораторная работа № 1. Основные понятия и определения

Формируемые компетенции: ОПК-5 (ИД-2)

Учебные цели занятия

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать содержание и порядок разработки приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, приказа о назначении ответственного за обработку персональных данных и приказа о создании комиссии по организации и проведению работ по защите персональных данных
2. Уметь разрабатывать организационно-распорядительные документы, необходимые для эффективной защиты персональных данных в соответствии с требованиями действующего законодательства.
3. Приобрести навыки разработки необходимых документов в интересах организации работ по обеспечению безопасности ИСПДн.
4. Приобрести навыки анализа и обобщения полученных результатов.

Время 90 минут

Распределение времени занятия

Вступительная часть.	- 2 мин
Проверка готовности студентов к занятию.	- 3 мин
Учебные вопросы занятия	
1. Разработка приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	- 35 мин
2. Разработка приказа о назначении ответственного за обработку персональных данных	- 25 мин
3. Разработка приказа о создании комиссии по организации и проведению работ по защите персональных данных	- 20 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связанные с разработкой приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, приказа о назначении ответственного за обработку персональных данных и приказа о создании комиссии по организации и проведению работ по защите персональных данных.

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

Статьи 18.1 и 22.1 ФЗ №152 «О персональных данных» (Приложении №1)

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных разработать приказ о об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны, для заданных исходных данных разработать приказ о назначении ответственного за обработку персональных данных.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки третьего вопроса, обучаемые должны для заданных исходных данных разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанные для заданных исходных данных и оформленные в соответствии с требованиями делопроизводства:

1. Приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
2. Приказ о назначении ответственного за обработку персональных данных.
3. Приказ о создании комиссии по организации и проведению работ по защите персональных данных.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть после проверки преподавателем защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех заданий, выставляется оценка.

Методическая литература

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной

регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы

- http://fstec.ru/ - официальный сайт ФСТЭК РФ;
- http://www.fsb.ru/- официальный сайт ФСБ РФ;
- http://rkn.gov.ru//- официальный сайт Роскомнадзора;
- http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение

- Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.
- Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Приложение №1

Выписка из ФЗ №152 «О персональных данных»

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися

государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона.

4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

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

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

3) 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.

Лабораторная работа № 2. Международное и национальное право в области защиты персональных данных.

Формируемые компетенции: ОПК-5 (ИД-2).

Учебные цели занятия

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать содержание и порядок разработки перечня персональных данных, подлежащих защите в информационных системах персональных данных, перечня информационных систем персональных данных, в которых должна быть обеспечена безопасность информации и перечня применяемых средств защиты информации, эксплуатационной и технической документации к ним.
2. Уметь разрабатывать уведомительные и организационно-распорядительные документы, необходимые для эффективной защиты персональных данных в соответствии с требованиями действующего законодательства.
3. Приобрести навыки разработки необходимых документов в интересах организации работ по обеспечению безопасности ИСПДн.
4. Приобрести навыки анализа и обобщения полученных результатов.

Время 180 минут

Распределение времени занятия

Вступительная часть.	- 2 мин
Проверка готовности студентов к занятию.	- 6 мин
Учебные вопросы занятия	
1. Разработка перечня персональных данных, подлежащих защите в информационных системах персональных данных	- 60 мин
2. Разработка перечня информационных систем персональных данных, в которых должна быть обеспечена безопасность информации	- 40 мин
3. Разработка перечня применяемых средств защиты информации, эксплуатационной и технической документации к ним	- 60 мин
Заключение	- 6 мин.
Задание студентам для самостоятельной работы	- 4 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связанные с разработкой перечня персональных данных, подлежащих защите в информационных системах персональных данных (ИСПДн), перечня

информационных систем персональных данных, в которых должна быть обеспечена безопасность информации и перечня применяемых средств защиты информации, эксплуатационной и технической документации к ним.

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

Материал лекции по теме «Содержание и основные положения Федерального закона Российской Федерации № 152-ФЗ «О персональных данных»

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных путем решения проблемных задач разработать перечень персональных данных, подлежащих защите в информационных системах персональных данных. Перечень оформить приказом руководителя организации.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса, обучаемые должны для заданных исходных данных путем решения проблемных задач разработать перечень информационных систем персональных данных, в которых должна быть обеспечена безопасность информации. Для каждой информационной системы персональных данных указать наименование ИСПДн, тип ИСПДн (напр. сервис, файловое хранилище, веб приложение и т.д.), место нахождения ИСПДн (полный адрес), субъекты ИСПДн (напр. работники, соискатели, бывшие работники, представители государственных органов, клиенты и др.), цели обработки, сроки хранения и условия удаления, перечень обрабатываемых персональных данных, перечень действий, стороннее сопровождение. Перечень оформить приказом руководителя организации.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки третьего вопроса, обучаемые должны для заданных исходных данных путем решения проблемных задач разработать перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним. Перечень оформить приказом руководителя организации.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанные для заданных исходных данных:

1. Перечень персональных данных, подлежащих защите в информационных системах персональных данных, оформленный приказом руководителя организации.
2. Перечень информационных систем персональных данных, в которых должна быть обеспечена безопасность информации, оформленный приказом руководителя организации.

3. Перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним, оформленный приказом руководителя организации.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть загружены в систему электронного обучения и после проверки преподавателем защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий выставляется оценка.

Методическая литература

- Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы

- http://fstec.ru/ - официальный сайт ФСТЭК РФ;
- http://www.fsb.ru/- официальный сайт ФСБ РФ;
- http://rkn.gov.ru//- официальный сайт Роскомнадзора;
- http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение

- Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.
- Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Лабораторная работа № 3. Содержание и основные положения Федерального закона Российской Федерации № 152-ФЗ «О персональных данных»

Формируемые компетенции: ОПК-5 (ИД-2)

Учебные цели занятия

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать содержание и порядок разработки согласия субъекта персональных данных на обработку его персональных данных.
2. Уметь разрабатывать организационно-распорядительные документы, необходимые для эффективной защиты персональных данных в соответствии с требованиями действующего законодательства.
3. Приобрести навыки разработки необходимых документов в интересах организации работ по обеспечению безопасности ИСПДн.
4. Приобрести навыки анализа и обобщения полученных результатов.

Время 90 минут

Распределение времени занятия:

Вступительная часть.	- 5 мин
Проверка готовности студентов к занятию.	- 10 мин
Учебные вопросы занятия:	
1. Разработка согласия субъекта персональных данных на обработку его персональных данных	- 40 мин
2. Разработка журнала учета согласий субъектов персональных данных	- 30 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить практические задания, связанные с разработкой согласия субъекта персональных данных на обработку его персональных данных и журнала учета согласий субъектов персональных данных.

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения.

Статья 9 ФЗ №152 «О персональных данных» (Приложение №1)

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса, обучаемые должны для заданных исходных данных разработать согласие субъекта персональных данных на обработку его персональных данных в соответствии с требованиями руководящих документов (Приложение 2). Согласие на обработку персональных данных разрабатывается в соответствии с перечнями персональных данных, определённых на предыдущем занятии для различных категорий субъектов персональных данных отдельно.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса, обучаемые должны для заданных исходных данных разработать журнал учета согласий субъектов персональных данных.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанные для заданных исходных данных:

1. Согласия субъекта персональных данных на обработку его персональных данных для различных категорий субъектов персональных данных.
2. Журнал учета согласий субъектов персональных данных

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий выставляется оценка.

Методическая литература:

- Приказ Роскомнадзора от 24.02.2021 № 18 “Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения”
- Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

- http://fstec.ru/ - официальный сайт ФСТЭК РФ;

– http://www.fsb.ru/- официальный сайт ФСБ РФ;
– http://rkn.gov.ru//- официальный сайт Роскомнадзора;
– http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.
– Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Приложение №1

Выписка из ФЗ №152 «О персональных данных»

Статья 9. Согласие субъекта персональных данных на обработку его персональных данных

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в **пунктах 2 - 11 части 1 статьи 6**, **части 2 статьи 10** и **части 2 статьи 11** настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в **пунктах 2 - 11 части 1 статьи 6**, **части 2 статьи 10** и **части 2 статьи 11** настоящего Федерального закона, возлагается на оператора.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в **пунктах 2 - 11 части 1 статьи 6**, **части 2 статьи 10** и **части 2 статьи 11** настоящего Федерального закона.

9. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

Приложение №2

Приказ Роскомнадзора от 24.02.2021 № 18 “Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения”

Зарегистрировано в Минюсте России 21.04.2021 № 63204.

В соответствии с частью 9 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2021, № 1, ст. 58), абзацем 2 пункта 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 (Собрание законодательства Российской Федерации, 2009, № 12, ст. 1431), приказываю:

1. Утвердить требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

1.1 Настоящий приказ вступает в силу с 1 сентября 2021 г. и действует до 1 сентября 2027 г.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

Руководитель
А.Ю. Липов

Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения

Приложение
к приказу Роскомнадзора
от 24.02.2021 г. № 18

Согласие должно содержать следующую информацию:

1) фамилия, имя, отчество (при наличии) субъекта персональных данных;

2) контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных);

3) сведения об операторе-организации - наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных);

сведения об операторе - физическом лице - фамилия, имя, отчество (при наличии), место жительства или место пребывания;

сведения об операторе-гражданине, являющимся индивидуальным предпринимателем, - фамилия, имя, отчество (при наличии), идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных);

4) сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных;

5) цель (цели) обработки персональных данных;

6) категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:

персональные данные (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, семейное положение, образование, профессия, социальное положение, доходы, другая информация, относящаяся к субъекту персональных данных);

специальные категории персональных данных (расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни, сведения о судимости);

биометрические персональные данные;

7) категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов (заполняется по желанию субъекта персональных данных);

8) условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных);

9) срок действия согласия.

Лабораторная работа № 4. Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах

Формируемые компетенции: ОПК-5 (ИД-2)

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать содержание и порядок разработки Уведомления об обработке персональных данных.
2. Уметь разрабатывать уведомительные и организационно-распорядительные документы, необходимые для эффективной защиты персональных данных в соответствии с требованиями действующего законодательства.
3. Приобрести навыки разработки необходимых документов в интересах организации работ по обеспечению безопасности ИСПДн.
4. Приобрести навыки анализа и обобщения полученных результатов.

Время 90 минут

Распределение времени занятия:

Вступительная часть.	- 5 мин
Проверка готовности студентов к занятию.	- 10 мин
Учебные вопросы занятия:	
1. Разработка Уведомления о намерении осуществлять обработку персональных данных	- 30 мин
2. Составление заявления об исключении сведений из реестра операторов, осуществляющих обработку персональных данных	- 10 мин
3. Составление заявления о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных	-10 мин
4. Составление информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных	- 20 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связанные с разработкой Уведомления о намерении осуществлять обработку персональных данных, составлением Заявления об исключении сведений из реестра операторов, осуществляющих обработку персональных

данных, Заявления о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных и Информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения.

Уведомление об обработке персональных данных заполняется в соответствии со статьей 22 ФЗ №152 «О персональных данных» (Приложение №1).

Образец и Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных определены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от от 19 августа 2011 г. № 706 "Об утверждении образца формы уведомления об обработке персональных данных".

Образец формы уведомления об обработке (о намерении осуществлять обработку) персональных данных имеет следующий вид:

Руководителю Управления Федеральной службы
по надзору в сфере связи, информационных
технологий и массовых коммуникаций
по _____
(наименование территориального
органа Роскомнадзора)

Уведомление
об обработке (о намерении осуществлять обработку) персональных данных

_____
(полное и сокращенное наименования, фамилия, имя отчество)
_____
(адрес местонахождения и почтовый адрес Оператора)
руководствуясь:
_____
(правовое основание обработки персональных данных)
с целью:
_____
(цель обработки персональных данных)
осуществляет обработку:
_____
(категории персональных данных)
принадлежащих:
_____
(категории субъектов, персональные данные которых обрабатываются)
Обработка вышеуказанных персональных данных будет осуществляться путем:
_____
(перечень действий с персональными данными, общее описание используемых
Оператором способов обработки персональных данных)
Для обеспечения безопасности персональных данных принимаются следующие меры:
_____
(описание мер, предусмотренных ст. ст. 18.1 и 19 Федерального закона
_____
от 27.07.2006 N 152-ФЗ "О персональных данных", в т.ч. сведения
_____

о наличии шифровальных (криптографических) средств и наименования
_____
этих средств; фамилия, имя, отчество физического лица или наименование
_____
юридического лица, ответственных за организацию обработки персональных
_____
данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных

_____
(при наличии трансграничной передачи персональных данных в процессе их обработки указывается перечень иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)

Сведения об обеспечении безопасности персональных данных

_____
(сведения об обеспечении безопасности персональных данных в соответствии
_____
с требованиями к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных _____
(число, месяц, год)

Срок или условие прекращение обработки персональных данных

_____

_____ _____
(должность) (подпись) расшифровка подписи

"__" _____ 20__ г.

Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных

1. Настоящие Рекомендации разработаны в целях установления единых принципов и порядка заполнения уведомления об обработке (о намерении осуществлять обработку) персональных данных (далее - Уведомление).

2. Уведомление оформляется на бланке Оператора (по **форме**, прилагаемой к настоящим Рекомендациям), осуществляющего обработку персональных данных (далее - Оператор), и направляется в территориальный орган Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - территориальный орган Роскомнадзора).

3. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом.

4. В **поле** "наименование (фамилия, имя, отчество), адрес Оператора" указывается:

4.1. Для юридических лиц (Операторов):

полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица (Оператора), осуществляющего обработку персональных данных;

наименование филиала (ов) (представительства (в) юридического лица (Оператора), осуществляющего обработку персональных данных;***(1)**

адрес Оператора***(2)**;

индивидуальный номер налогоплательщика (ИНН).

4.2. Для физических лиц:

фамилия, имя, отчество физического лица (Оператора);

адрес Оператора***(3)**;

данные документа, удостоверяющего личность, дата его выдачи, наименование органа, выдавшего документ;

индивидуальный номер налогоплательщика (ИНН).

4.3. Для государственных, муниципальных органов (Операторов):

полное и сокращенное наименование государственного, муниципального органа;

наименование территориального(ых) органа(ов), осуществляющего(их) обработку персональных данных;

адрес Оператора***(4)**;

индивидуальный номер налогоплательщика (ИНН).

При указании наименования (фамилии, имени, отчества), адреса Оператора, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (**ОКВЭД**, ОКПО, **ОКОГУ**, ОКОП, **ОКФС**).

5. В **поле** "цель обработки персональных данных" указываются цели обработки персональных данных (а также их соответствие полномочиям Оператора) (**Примечание N 1**).

Примечание N 1. *Под "целью обработки персональных данных" понимаются, как цели, указанные в учредительных документах Оператора, так и цели, фактически осуществляемой Оператором деятельности по обработке персональных данных.*

6. В **поле** "категории персональных данных" указываются все категории персональных данных, подлежащих обработке:

6.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту персональных данных).

6.2. Специальные категории персональных данных (расовая принадлежность, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояния здоровья, интимной жизни).

6.3. Биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных).

7. В **поле** "категории субъектов, персональные данные которых обрабатываются" указываются категории субъектов (физических лиц) и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются (например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (Оператором), физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (Оператором) и др.).

8. В **поле** "правовое основание обработки персональных данных" указываются:

Федеральный закон, постановление Правительства Российской Федерации, иной нормативно-правовой акт, закрепляющий основание и порядок обработки персональных данных (**Примечание N 2**);

Примечание N 2. *Указываются не только соответствующие статьи* ***Федерального закона*** *"О персональных данных", но и статьи иного нормативно-правового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки персональных данных (например:* ***ст.ст. 85 - 90*** *Трудового кодекса Российской Федерации,* ***ст. 85.1*** *Воздушного кодекса Российской Федерации,* ***ст. 12*** *Федерального закона "Об актах гражданского состояния" и др.).*

Номер, дату выдачи и наименование лицензии на осуществляемый вид деятельности, с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных (**Примечание N 3**).

Примечание N 3. *Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу персональных данных (или информации, касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных условий.*

9. В **поле** "перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных", указываются действия, совершаемые Оператором с персональными данными, а также описание используемых Оператором способов обработки персональных данных:

- неавтоматизированная обработка персональных данных;
- исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;
- смешанная обработка персональных данных (**Примечание N 4**)

Примечание N 4. *При автоматизированной обработке персональных данных либо смешанной обработке, необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица) либо информация передается с использованием сети общего пользования Интернет либо без передачи полученной информации.*

10. В **поле** "описание мер, предусмотренных **статьями 18.1** и **19** Федерального закона "О персональных данных", указываются:

а) описание мер, предусмотренных **ст.ст. 18.1** и **19** Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

б) фамилия, имя, отчество физического лица или сотрудника юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

в) класс информационной системы персональных данных Оператора (**пункт 14** приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных";

г) организационные и технические меры, применяемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных.

В случае использования Оператором, осуществляющим обработку персональных данных, шифровальных (криптографических) средств указываются следующие сведения:

а) наименование, регистрационные номера и производителей используемых криптографических средств;

б) уровень криптографической защиты персональных данных;

в) уровень специальной защиты от утечки по каналам побочных излучений и наводок;

г) уровень защиты от несанкционированного доступа.

Предоставление данной информации осуществляется в соответствии с **Методическими рекомендациями** по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 г. N 149/54-144.

11. В **поле** "сведения о наличии или об отсутствии трансграничной передачи персональных данных" указываются сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки с указанием перечня иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных.

12. В **поле** "сведения об обеспечении безопасности персональных данных" указываются сведения об обеспечении безопасности персональных данных в соответствии с

требованиями к защите персональных данных, установленными Правительством Российской Федерации.

13. В **поле** "дата начала обработки персональных данных" указывается конкретная дата (число, месяц, год) начала любого действия (операции) 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 (фактическая дата начала обработки персональных данных).

14. В **поле** "срок или условие прекращения обработки персональных данных" указывается конкретная дата (число, месяц, год) или основание (условие), наступление которого повлечет прекращение обработки персональных данных.

---

*(1) Для юридических лиц с филиальной структурой указывается список субъектов Российской Федерации (с указанием кода субъекта - согласно **справочнику** "Коды регионов", утвержденному **приказом** ФНС России от 13.10.2006 года N САЭ-3-04/706@ "Об утверждении формы сведений о доходах физических лиц" (зарегистрированным Министерством юстиции Российской Федерации 17.11.2000 г., регистрационный номер 8507), на территории которых находятся филиалы (представительства) юридического лица и (или) где оператором производится обработка персональных данных. Уведомление направляется юридическим лицом в соответствующее территориальное управление Роскомнадзора по месту своего нахождения с указанием всех имеющихся филиалов (представительств).

*(2) Указывается место нахождения юридического лица в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, почтовый адрес юридического лица, контактная информация.

Для организаций, учреждений, имеющих филиалы (представительства), указываются юридический и почтовый адреса (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка персональных данных (все действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных). При этом, необходимо уточнить - обработка персональных данных осуществляется только юридическим лицом (формирование центральной информационной системы) и (или) филиалами (представительствами).

*(3) Указывается место нахождения физического лица в соответствии со свидетельством о постановке на учет физического лица в налоговом органе, почтовый адрес физического лица, контактная информация.

*(4) Указывается место нахождения государственного, муниципального органа в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, почтовый адрес государственного, муниципального органа, контактная информация.

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных разработать и заполнить форму уведомления об обработке (о намерении осуществлять обработку) персональных данных Электронные формы документов можно найти на сайте Роскомнадзора по адресу http://www.pd.rsoc.ru/operators-registry/notification/.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса, обучаемые должны для заданных исходных данных составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных.

Методические пояснения и рекомендации по выполнению третьего вопроса

В ходе отработки третьего вопроса, обучаемые должны для заданных исходных данных составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных.

Методические пояснения и рекомендации по выполнению четвертого вопроса

В ходе отработки четвертого вопроса обучаемые должны, для заданных исходных данных составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.

Отчетность за занятие

Отчет по лабораторной работе должен содержать заполненные в соответствии с рекомендациями Роскомнадзора:

1. Форму уведомления об обработке (о намерении осуществлять обработку) персональных данных.
2. Заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных.
3. Заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных.
4. Информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий выставляется оценка.

Методическая литература

- Приказ Роскомнадзора от 30.05.2017 № 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения";
- Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

- http://fstec.ru/ - официальный сайт ФСТЭК РФ;
- http://www.fsb.ru/- официальный сайт ФСБ РФ;
- http://rkn.gov.ru//- официальный сайт Роскомнадзора;
- http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

- Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.
- Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Приложение №1

Выписка из ФЗ №152 «О персональных данных»

Статья 22. Уведомление об обработке персональных данных

1. Оператор до начала обработки персональных данных обязан **уведомить** уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных **частью 2** настоящей статьи.

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с **трудовым законодательством**;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с **федеральными законами** или иными **нормативными правовыми актами** Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных **законодательством** Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

3. **Уведомление**, предусмотренное **частью 1** настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных **статьями 18.1** и **19** настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

4. **Уполномоченный орган** по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в **части 3** настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

7. В случае изменения сведений, указанных в **части 3** настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Лабораторная работа № 5. Особенности обработки биометрических персональных данных

Формируемые компетенции: ОПК-5 (ИД-3)

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать нормативные правовые документы в области защиты персональных данных.
2. Знать правовые нормативные акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.
3. Уметь применять комплексный подход к обеспечению информационной безопасности персональных данных.
4. Приобрести способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности.
5. Приобрести навыки анализа и обобщения полученных результатов.

Время 90 минут

Распределение времени занятия:

Вступительная часть.	- 5 мин
Проверка готовности студентов к занятию.	- 10 мин

Учебные вопросы занятия:

1. Классификация информационных систем персональных данных	- 15 мин
2. Определение типа угроз безопасности персональных данных	- 10 мин
3. Установление уровней защищенности персональных данных	- 40 мин
Заключение	- 5 мин
Задание студентам для самостоятельной работы	- 5 мин

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить практические задания, связанные с установлением уровней защищенности персональных данных

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

1. Классификация информационных систем персональных данных

Информационная система является информационной системой, обрабатывающей *специальные категории персональных данных*, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей *биометрические персональные данные*, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей *общедоступные персональные данные*, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей *иные категории персональных данных*, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные *данные сотрудников оператора*, если в ней обрабатываются персональные данные только указанных сотрудников. В

остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, *не являющихся сотрудниками оператора*.

2. Определение типа угроз безопасности персональных данных

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

3. Установление уровней защищенности персональных данных

При обработке персональных данных в информационных системах устанавливаются **4 уровня защищенности** персональных данных.

Необходимость обеспечения *1-го уровня защищенности* персональных данных (УЗ1) при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения *2-го уровня защищенности* персональных данных (УЗ2) при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения *3-го уровня защищенности* персональных данных (УЗ3) при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения *4-го уровня защищенности* персональных данных (УЗ4) при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Вышеуказанные требования для оценки необходимого уровня защищенности персональных данных при их обработке в информационной системе приведены в табл. 1.

Таблица 1. Определение уровня защищенности персональных данных при их обработке в информационной системе (п.9–12 Постановления Правительства РФ №1119 от 01.11.2012 г.)

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальности угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не сотрудники	Более 100 000	УЗ1	УЗ1	УЗ2
		Менее чем 100 000	УЗ1	УЗ2	УЗ3
	Сотрудники	Более 100 000	УЗ1	УЗ2	УЗ3
		Менее чем 100 000	УЗ1	УЗ2	УЗ3
ИСПДн-Б	Не сотрудники	Более 100 000	УЗ1	УЗ2	УЗ3
		Менее чем 100 000	УЗ1	УЗ2	УЗ3
	Сотрудники	Более 100 000	УЗ1	УЗ2	УЗ3
		Менее чем 100 000	УЗ1	УЗ2	УЗ3
ИСПДн-И	Не сотрудники	Более 100 000	УЗ1	УЗ2	УЗ3
		Менее чем 100 000	УЗ1	УЗ3	УЗ4
	Сотрудники	Более 100 000	УЗ1	УЗ3	УЗ4
		Менее чем 100 000	УЗ1	УЗ3	УЗ4
ИСПДн-О	Не сотрудники	Более 100 000	УЗ2	УЗ2	УЗ4
		Менее чем 100 000	УЗ2	УЗ3	УЗ4
	Сотрудники	Более 100 000	УЗ2	УЗ3	УЗ4
		Менее чем 100 000	УЗ2	УЗ3	УЗ4

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных в перечне информационных систем персональных данных и обрабатываемых в них персональных данных (полученных в ходе выполнения занятия №2) выполнить классификацию информационных систем персональных данных.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны, для каждой информационной системы персональных данных определить тип угроз безопасности персональных данных.

Методические пояснения и рекомендации по выполнению третьего вопроса

В ходе отработки третьего вопроса обучаемые должны, для каждой информационной системы персональных данных установить уровень защищенности персональных данных. Форма акта установления уровня защищенности персональных данных в Приложении 1.

Отчетность за занятие

Отчет по лабораторной работе должен содержать заполненные в соответствии с требованиями руководящих документов:

1. Акты установления уровня защищенности персональных данных для каждой информационной системы персональных данных.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий, выставляется оценка.

Список рекомендуемой литературы

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Методическая литература

- Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

- http://fstec.ru/ - официальный сайт ФСТЭК РФ;
- http://www.fsb.ru/- официальный сайт ФСБ РФ;
- http://rkn.gov.ru//- официальный сайт Роскомнадзора;
- http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

- Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.
- Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Приложение 1

УТВЕРЖДАЮ

Генеральный директор

_____

_____

_____

«____» _____2022г.

АКТ № 1

установления уровня защищённости персональных данных в информационной системе персональных данных «Наименование системы»

Комиссия, назначенная Приказом №_____ от _____г. в составе председателя комиссии:

_____ членов комиссии:

_____

_____

Рассмотрев исходные данные на информационную систему персональных данных «Наименование системы»

1. Информационная система персональных данных «Наименование системы» является информационной системой, обрабатывающей _____*категории персональных данных*, так как в ней обрабатываются персональные данные, касающиеся _____

2. Информационная система персональных данных «Наименование системы» является информационной системой, обрабатывающей категории персональных данных *сотрудников оператора*, так как в ней обрабатываются персональные данные сотрудников оператора.

или

2. Информационная система персональных данных «Наименование системы» является информационной системой, обрабатывающей категории персональных

данных субъектов персональных данных, *не являющихся сотрудниками оператора*.

3. Количество субъектов персональных данных в информационной системе персональных данных «Наименование системы» составляет _____

4. Для информационной системы персональных данных «Наименование системы» актуальными являются угрозы безопасности _____ типа.

В соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

РЕШИЛА:

Установить

персональным данным, обрабатывающимся в информационной системе персональных данных «Наименование системы»

уровень защищённости – УЗ__.

Председатель комиссии:

Члены комиссии:

Лабораторная работа № 6. Методика оценки угроз безопасности персональным данным

Формируемые компетенции: ОПК-5 (ИД-3), ОПК-2.3. ИД-1

Учебные цели занятия

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать правовые нормативные акты и нормативные методические документы Федеральной службой по техническому и экспортному контролю
2. Уметь определять возможные негативные последствия от реализации угроз безопасности персональных данных.
3. Уметь определять возможные объекты воздействия угроз безопасности персональных данных.
4. Уметь определять источники угроз безопасности персональных данных
5. Уметь описывать способы реализации угроз безопасности персональных данных.
6. Уметь оценивать актуальность угроз безопасности персональных данных.
7. Приобрести навыки использования нормативных правовых документов в своей профессиональной деятельности.
8. Приобрести навыки анализа и обобщения полученных результатов.

Время 270 минут

Распределение времени занятия:

Вступительная часть.	- 10 мин
Проверка готовности студентов к занятию.	- 20 мин

Учебные вопросы занятия:

1. Описание систем и сетей и их характеристика как объектов защиты	- 30 мин
2. Определение негативных последствий от реализации угроз безопасности персональных данных	- 50 мин
3. Определение возможных объектов воздействия угроз безопасности персональных данных	- 40 мин
4. Определение источников угроз безопасности персональных данных	- 30 мин
5. Описание способов реализации угроз безопасности персональных данных	- 40 мин
6. Оценка актуальности угроз безопасности персональных данных	- 40 мин
Заключение	- 6 мин.
Задание студентам для самостоятельной работы	- 4 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, путем решения проблемных задач, связанные с разработкой модели угроз безопасности персональных данных при их обработке в информационных системах. По результатам выполнения лабораторной работы должна быть создана и оформлена в соответствии с руководящими документами модель угроз безопасности персональных данных при их обработке в информационных системах для заданных в начале курса исходных данных для одной из информационных систем персональных данных.

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

Основные теоретические сведения изложены в «Методике оценки угроз безопасности информации», которая утверждена ФСТЭК России 5 февраля 2021 г.

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для выбранной на первом занятии организации, учитывая результаты предыдущих занятий описать для одной из информационных систем персональных данных в части применимости:

- наименование систем и сетей, для которых разработана модель угроз безопасности персональных данных;
- класс защищенности, категорию значимости систем и сетей, уровень защищенности персональных данных;
- нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети;
- назначение, задачи (функции) систем и сетей, состав обрабатываемой персональных данных и их правовой режим;
- основные процессы (бизнес-процессы) оператора персональных данных, для обеспечения которых создаются (функционируют) системы и сети;
- состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей;
- описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации);
- описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации,

средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет»;

– информацию о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, о модели предоставления вычислительных услуг, о распределении ответственности за защиту информации между оператором персональных данных и поставщиком вычислительных услуг, об условиях использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (при наличии).

К модели угроз безопасности персональных данных могут прилагаться схемы и рисунки, иллюстрирующие состав и архитектуру систем и сетей, интерфейсы взаимодействия компонентов системы и сети, группы пользователей, а также другие поясняющие материалы.

По результатам отработки первого вопроса заполнить разделы 1 и 2 Модели угроз безопасности персональных данных (Приложение 1).

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса, обучаемые должны:

– описать виды рисков (ущербов), актуальных для оператора персональных данных, которые могут наступить от нарушения или прекращения основных процессов;

– описать негативные последствия, наступление которых в результате реализации (возникновения) угроз безопасности персональных данных может привести к возникновению рисков (ущерба).

По результатам отработки второго вопроса заполнить раздел 3 Модели угроз безопасности персональных данных (Приложение 1).

Методические пояснения и рекомендации по выполнению третьего вопроса

В ходе отработки третьего вопроса, обучаемые должны:

– описать наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемых персональных данных, или обеспечивают реализацию основных процессов оператора персональных данных;

– описать виды воздействия на компоненты систем и сетей, реализация которых нарушителем может привести к негативным последствиям.

К модели угроз безопасности персональных данных может прилагаться схема с отображением объектов воздействия и их назначения в составе архитектуры систем и сетей.

По результатам отработки третьего вопроса заполнить раздел 4 Модели угроз безопасности персональных данных (Приложение 1).

Методические пояснения и рекомендации по выполнению четвертого вопроса

В ходе отработки четвертого вопроса обучаемые должны:

- составить характеристику нарушителей, которые могут являться источниками угроз безопасности персональных данных, и возможные цели реализации ими угроз безопасности персональных данных;
- определить категории актуальных нарушителей, которые могут являться источниками угроз безопасности персональных данных;
- описать возможности нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.

К модели угроз безопасности персональных данных могут прилагаться рисунки, иллюстрирующие возможности нарушителей, и другие поясняющие материалы.

По результатам отработки четвертого вопроса заполнить раздел 5 Модели угроз безопасности персональных данных (Приложение 1).

Методические пояснения и рекомендации по выполнению пятого вопроса

В ходе отработки пятого вопроса, обучаемые должны:

- описать способы реализации (возникновения) угроз безопасности персональных данных, которые могут быть использованы нарушителями разных видов и категорий;
- описать интерфейсы объектов воздействия, доступные для использования нарушителями способов реализации угроз безопасности персональных данных.

К модели угроз безопасности персональных данных может прилагаться схема с отображением типов логических, физических интерфейсов объектов воздействия, в том числе требующих физического доступа к ним, а также соответствующие им способы реализации угроз безопасности персональных данных.

По результатам отработки пятого вопроса заполнить раздел 6 Модели угроз безопасности персональных данных (Приложение 1).

Методические пояснения и рекомендации по выполнению шестого вопроса

В ходе отработки шестого вопроса, обучаемые должны:

- определить перечень возможных (вероятных) угроз безопасности персональных данных для соответствующих способов их реализации и уровней возможностей нарушителей;
- описать возможные сценарии реализации угроз безопасности персональных данных;
- сделать выводы об актуальности угроз безопасности персональных данных.

К модели угроз безопасности персональных данных может прилагаться схема с отображением сценариев реализации угроз безопасности персональных данных.

По результатам отработки шестого вопроса заполнить раздел 6 Модели угроз безопасности персональных данных (Приложение 1).

Отчетность за занятие

Отчет по лабораторной работе должен содержать «Модель угроз безопасности персональных данных» для одной из информационных систем персональных данных для выбранной организации, оформленную в соответствии с Приложением 1.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий, выставляется оценка.

Список рекомендуемой литературы

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
2. Методика оценки угроз безопасности информации. Утверждена ФСТЭК России 5 февраля 2021 г.

Методическая литература

– База знаний о тактике и методах противника, https://attack.mitre.org/
– Банк данных угроз безопасности информации, https://bdu.fstec.ru/threat
– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

– http://fstec.ru/ - официальный сайт ФСТЭК РФ;
– http://www.fsb.ru/- официальный сайт ФСБ РФ;
– http://rkn.gov.ru//- официальный сайт Роскомнадзора;
– http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о

государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

– Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Приложение 1.

Рекомендуемая структура модели угроз безопасности персональных данных

УТВЕРЖДАЮ

Руководитель организации
или иное уполномоченное
лицо

_____

«___» _____20__г.

Модель угроз безопасности персональных данных
для информационной системы персональных данных «Наименование системы»
наименование системы и (или) сети

1. Общие положения

Раздел «Общие положения» содержит:

назначение и область действия документа;

нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности персональных данных и разработки модели угроз;

наименование оператора персональных данных;

подразделения, должностные лица, ответственные за обеспечение защиты персональных данных;

наименование организации, привлекаемой для разработки модели угроз безопасности персональных данных (при наличии).

2. Описание систем и сетей и их характеристика как объектов защиты

Раздел «Описание систем и сетей и их характеристика как объектов защиты» содержит:

наименование систем и сетей, для которых разработана модель угроз безопасности персональных данных;

класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных;

нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети;

назначение, задачи (функции) систем и сетей, состав обрабатываемых персональных данных и их правовой режим;

основные процессы (бизнес-процессы) оператора персональных данных, для обеспечения которых создаются (функционируют) системы и сети;

состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей;

описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации);

описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет»;

информацию о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, о модели предоставления вычислительных услуг, о распределении ответственности за защиту персональных данных между оператором персональных данных и поставщиком вычислительных услуг, об условиях использования информационно-телекоммуникационной

инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (при наличии).

К модели угроз безопасности персональных данных могут прилагаться схемы и рисунки, иллюстрирующие состав и архитектуру систем и сетей, интерфейсы взаимодействия компонентов системы и сети, группы пользователей, а также другие поясняющие материалы.

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности персональных данных

Раздел «Возможные негативные последствия от реализации (возникновения) угроз безопасности персональных данных» содержит:

описание видов рисков (ущербов), актуальных для оператора персональных данных, которые могут наступить от нарушения или прекращения основных процессов;

описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности персональных данных может привести к возникновению рисков (ущерба).

4. Возможные объекты воздействия угроз безопасности персональных данных

Раздел «Возможные объекты воздействия угроз безопасности персональных данных» содержит:

наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемых персональных данных, или обеспечивают реализацию основных процессов оператора персональных данных;

описание видов воздействия на компоненты систем и сетей, реализация которых нарушителем может привести к негативным последствиям.

К модели угроз безопасности персональных данных может прилагаться схема с отображением объектов воздействия и их назначения в составе архитектуры систем и сетей.

5. Источники угроз безопасности персональных данных

Раздел «Источники угроз безопасности персональных данных» содержит:

характеристику нарушителей, которые могут являться источниками угроз безопасности персональных данных, и возможные цели реализации ими угроз безопасности персональных данных;

категории актуальных нарушителей, которые могут являться источниками угроз безопасности персональных данных;

описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.

К модели угроз безопасности персональных данных могут прилагаться рисунки, иллюстрирующие возможности нарушителей, и другие поясняющие материалы.

6. Способы реализации (возникновения) угроз безопасности персональных данных

Раздел «Способы реализации (возникновения) угроз безопасности персональных данных» включает:

описание способов реализации (возникновения) угроз безопасности персональных данных, которые могут быть использованы нарушителями разных видов и категорий;

описание интерфейсов объектов воздействия, доступных для использования нарушителями способов реализации угроз безопасности персональных данных.

К модели угроз безопасности персональных данных может прилагаться схема с отображением типов логических, физических интерфейсов объектов воздействия, в том числе требующих физического доступа к ним, а также соответствующие им способы реализации угроз безопасности информации.

7. Актуальные угрозы безопасности персональных данных

Раздел «Актуальные угрозы безопасности персональных данных» включает:

перечень возможных (вероятных) угроз безопасности персональных данных для соответствующих способов их реализации и уровней возможностей нарушителей;

описание возможных сценариев реализации угроз безопасности персональных данных;

выводы об актуальности угроз безопасности персональных данных.

К модели угроз безопасности персональных данных может прилагаться схема с отображением сценариев реализации угроз безопасности информации.

Лабораторная работа № 7. Оценка возможности реализации угроз безопасности персональным данным и определение их актуальности

Формируемые компетенции: ОПК-2.3 (ИД-1).

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать нормативные правовые документы в области защиты персональных данных.
2. Знать правовые нормативные акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.
3. Уметь применять комплексный подход к обеспечению информационной безопасности персональных данных.
4. Приобрести способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности.
5. Приобрести навыки анализа и обобщения полученных результатов.

Время 90 минут

Распределение времени занятия:

Вступительная часть.	- 5 мин
Проверка готовности студентов к занятию.	- 10 мин
Учебные вопросы занятия:	
1. Определение основных целей, задач и общей стратегии построения системы защиты персональных данных (СЗПДн) организации.	- 30 мин
2. Определение основных требований и базовых подходов их реализации для достижения требуемого уровня безопасности информации	- 40 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связанные с разработкой Концепции информационной безопасности.

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

«Концепция обеспечения безопасности информации в автоматизированной системе организации» (далее - Концепция) определяет систему взглядов на проблему обеспечения безопасности информации в АС организации, и представляет собой систематизированное изложение целей и задач защиты, основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в АС.

Основные положения и требования Концепции распространяются на все структурные подразделения организации, в которых осуществляется автоматизированная обработка подлежащей защите информации, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования АС.

Концепция является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности информации в АС;

– принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

– координации деятельности структурных подразделений при проведении работ по созданию, развитию и эксплуатации АС с соблюдением требований обеспечения безопасности информации;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности АС.

Правовой основой Концепции должны являться Конституция Российской Федерации. Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы Федеральной службой по техническому и экспортному контролю (ФСТЭК), Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) и других нормативных документов, регламентирующих вопросы защиты информации в АС.

При разработке Концепции должны учитываться основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно - программных средств защиты и противодействия угрозам безопасности информации, а также текущее состояние и перспективы развития информационных технологий.

Основные положения Концепция должны базироваться на качественном осмыслении вопросов безопасности информации и не концентрировать

внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

Положения Концепции предусматривают существование в рамках проблемы обеспечения безопасности информации в АС двух относительно самостоятельных направлений, объединенных единым замыслом: защита информации от утечки по техническим каналам и защита информации в автоматизированных системах от несанкционированного доступа.

В Концепции информационной безопасности должны быть отражены следующие вопросы:

- характеристика АС организации, как объекта информационной безопасности (объекта защиты):
  - назначение, цели создания и эксплуатации АС организации;
  - структура, состав и размещение основных элементов ас организации, информационные связи с другими объектами;
  - категории информационных ресурсов, подлежащих защите;
  - категории пользователей АС организации, режимы использования и уровни доступа к информации;
- интересы затрагиваемых при эксплуатации ас организации субъектов информационных отношений;
- уязвимость основных компонентов АС организации
- цели и задачи обеспечения информационной безопасности организации и основные пути их достижения (решения задач системы защиты)
- перечень основных опасных воздействующих факторов и значимых угроз информационной безопасности:
  - внешние и внутренние нарушители;
- подход к оценке риска в АС организации;
- основные положения технической политики в области обеспечения безопасности информации АС организации;
- принципы обеспечения информационной безопасности организации;
- основные меры и методы (способы) защиты от угроз, средства обеспечения требуемого уровня защищенности ресурсов АС:
- организационные (административные) меры защиты
- структура, функции и полномочия подразделения обеспечения информационной безопасности;
- физические средства защиты;
- технические (программно-аппаратные) средства защиты;
- управление системой обеспечения безопасности информации;
- контроль эффективности системы защиты;
- первоочередные мероприятия по обеспечению безопасности информации АС организации;

– перечень нормативных документов, регламентирующих деятельность в области защиты информации;
– основные термины и определения.

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных определить основные цели, задачи и общую стратегию построения системы защиты персональных данных (СЗПДн) организации.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны, для заданных исходных данных определить основные требования и базовые подходы их реализации для достижения требуемого уровня безопасности информации. На основании этих данных составить Концепцию информационной безопасности.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанную в соответствии с требованиями руководящих документов Концепцию информационной безопасности.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий выставляется оценка.

Список рекомендуемой литературы

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Методическая литература:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

– http://fstec.ru/ - официальный сайт ФСТЭК РФ;
– http://www.fsb.ru/- официальный сайт ФСБ РФ;
– http://rkn.gov.ru//- официальный сайт Роскомнадзора;
– http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

– Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Лабораторная работа № 8. База знаний о поведениях компьютерных злоумышленников

Формируемые компетенции: ОПК-2.3 (ИД-1)

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать нормативные правовые документы в области защиты персональных данных.
2. Знать правовые нормативные акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.
3. Уметь применять комплексный подход к обеспечению информационной безопасности персональных данных.
4. Приобрести способность участвовать в работах по реализации политики информационной безопасности.
5. Приобрести навыки анализа и обобщения полученных результатов.

Время 90 минут

Распределение времени занятия:

Вступительная часть.	- 5 мин
Проверка готовности студентов к занятию.	- 10 мин
Учебные вопросы занятия:	
1. Определение состава системы защиты персональных данных.	- 30 мин
2. Определение требований к персоналу информационных систем персональных данных	- 40 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связанные с разработкой Политики информационной безопасности.

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

Политика информационной безопасности (ПИБ) — набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области защиты информации. На основе ПИБ строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение ИС в различных ситуациях.

Для конкретной ИС политика безопасности должна быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д.

Следует рассматривать такие направления защиты ИС:

- защита объектов информационной системы;
- защита процессов, процедур и программ обработки информации;
- защита каналов связи;
- подавление побочных электромагнитных излучений;
- управление системой защиты.

Очевидно, что каждое из указанных НАПРАВЛЕНИЙ должно быть детализировано в зависимости от особенностей структуры ИС.

Кроме этого ПИБ должна описывать следующие ЭТАПЫ создания СЗИ:

- определение информационных и технических ресурсов, подлежащих защите;
- выявление полного множества потенциально возможных угроз и каналов утечки информации;
- проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
- определение требований к системе защиты;
- осуществление выбора средств защиты информации и их характеристик;
- внедрение и организация использования выбранных мер, способов и средств защиты;
- осуществление контроля целостности и управление системой защиты.

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

1. Невозможность миновать защитные средства;
2. Усиление самого слабого звена;
3. Недопустимость перехода в открытое состояние;
4. Минимизация привилегий;
5. Разделение обязанностей;
6. Многоуровневая защита;
7. Разнообразие защитных средств;
8. Простота и управляемость информационной системы;
9. Обеспечение всеобщей поддержки мер безопасности.

1. Принцип невозможности миновать защитные средства означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через СЗИ. Не должно быть “тайных” модемных входов или тестовых линий, идущих в обход экрана.

2. Надежность любой СЗИ определяется самым слабым звеном. Часто таким звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

3. Принцип недопустимости перехода в открытое состояние означает, что при любых обстоятельствах (в том числе нештатных), СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ.

4. Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

5. Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно для предотвращения злонамеренных или неквалифицированных действий системного администратора.

6. Принцип многоуровневой защиты предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией — управление доступом и, как последний рубеж, — протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

7. Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками преодоления СЗИ.

8. Принцип простоты и управляемости информационной системы в целом и СЗИ в особенности определяет возможность формального или неформального доказательства корректности реализации механизмов защиты. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

9. Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Рекомендуется с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

В настоящее время лучше всего изучены два вида политики безопасности: избирательная и полномочная, основанные, соответственно на избирательном и полномочном способах управления доступом.

Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:

- все субъекты и объекты системы должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД), иногда ее называют матрицей контроля доступа. Такая модель получила название матричной.

Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как “доступ на чтение”, “доступ на запись”, “доступ на исполнение” и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей МД.

Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно избирательное управление доступом реализует принцип “что не разрешено, то запрещено”, предполагающий явное разрешение доступа субъекта к объекту. Матрица доступа — наиболее простой подход к моделированию систем доступа.

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость и небольшие накладные расходы.

Основу полномочной политики безопасности составляет полномочное управление доступом, которое подразумевает, что:

– все субъекты и объекты системы должны быть однозначно идентифицированы;

– каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

– каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру и, таким образом, в системе можно реализовать иерархически восходящий поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект, кроме уровня прозрачности, имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Основное назначение полномочной политики безопасности — регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии в нижние, а также блокирование возможного проникновения с нижних уровней в верхние. При этом она функционирует на

фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных определить состав системы защиты персональных данных.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны, для заданных исходных данных определить требования к персоналу информационных систем персональных данных. На основании этих данных составить Политику информационной безопасности.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанную в соответствии с требованиями руководящих документов Политику информационной безопасности.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий выставляется оценка.

Список рекомендуемой литературы

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Методическая литература:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

– http://fstec.ru/ - официальный сайт ФСТЭК РФ;
– http://www.fsb.ru/- официальный сайт ФСБ РФ;
– http://rkn.gov.ru//- официальный сайт Роскомнадзора;
– http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

– Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Лабораторная работа № 9. Построение системы защиты персональных данных

Формируемые компетенции: ОПК-2.3 (ИД-1)

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать нормативные правовые документы в области защиты персональных данных.
2. Знать правовые нормативные акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.
3. Уметь формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности.
4. Приобрести способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности.
5. Приобрести способность формировать процедуры для управления информационной безопасностью.

Время 180 минут

Распределение времени занятия:

Вступительная часть.	- 10 мин
Проверка готовности студентов к занятию.	- 20 мин
Учебные вопросы занятия:	
1. Определение перечня мероприятий для плана	- 20 мин
2. Определение формы реализации мероприятий, срока выполнения и ответственных лиц	- 40 мин
3. Разработка плана мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных	- 40 мин
4. Разработка плана внутренних проверок режима защиты персональных данных в информационных системах персональных данных	- 40 мин
Заключение	- 6 мин.
Задание студентам для самостоятельной работы	- 4 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связанные с разработкой плана мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

План мероприятий по обеспечению защиты персональных данных (далее – План), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных.

План составляется на основании списка мер, методов и средств защиты, определенных в Концепции информационной безопасности и Политике информационной безопасности.

Выбор конкретных мероприятий осуществляется на основании анализа Отчета по результатам внутренней проверки и Модели угроз безопасности.

В План включаются следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План включаются следующая информация:

- название мероприятия;
- периодичность мероприятия (разовое/периодическое);
- исполнитель мероприятия/ответственный за исполнение.

План внутренних проверок составляется на все информационные системы персональных данных организации.

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных на основании ранее разработанных Концепции и Политики информационной безопасности определить перечень мероприятий для плана.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны, для заданных исходных данных определить формы реализации мероприятий, срок выполнения и ответственных лиц.

Методические пояснения и рекомендации по выполнению третьего вопроса

В ходе отработки третьего вопроса обучаемые должны, для заданных исходных данных разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных.

Методические пояснения и рекомендации по выполнению четвертого вопроса

В ходе отработки четвертого вопроса обучаемые должны, для заданных исходных данных разработать план внутренних проверок режима защиты персональных данных в информационных системах персональных данных.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанные в соответствии с требованиями руководящих документов план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных и план внутренних проверок режима защиты персональных данных в информационных системах персональных данных.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий, выставляется оценка.

Список рекомендуемой литературы

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Методическая литература:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

– http://fstec.ru/ - официальный сайт ФСТЭК РФ;
– http://www.fsb.ru/- официальный сайт ФСБ РФ;
– http://rkn.gov.ru//- официальный сайт Роскомнадзора;
– http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

– Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Лабораторная работа № 10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Формируемые компетенции: ОПК-2.3 (ИД-1)

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать особенности предварительного технико-экономического анализа проектных решений по обеспечению информационной безопасности.
2. Знать порядок разработки подсистемы управления информационной безопасностью.
3. Уметь анализировать исходные данные для проектирования подсистем и средств обеспечения информационной безопасности персональных данных.
4. Приобрести способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности.
5. Приобрести способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия.

Время 90 минут

Распределение времени занятия:

Вступительная часть.	- 5 мин
Проверка готовности студентов к занятию.	- 10 мин
Учебные вопросы занятия:	
1. Описание системы защиты персональных данных в ИСПДн	- 30 мин
2. Разработка проекта технического задания на разработку системы обеспечения безопасности информации объекта вычислительной техники	- 40 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить практические задания, связанные с разработкой требований к информационной системе по обеспечению безопасности персональных данных

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

Создание системы защиты персональных данных в соответствии с положениями Федерального закона «О персональных данных» и требованиями нормативных документов по защите персональных данных позволяет минимизировать правовые и репутационные риски, связанные с несоблюдением законодательства России в области автоматизированной обработки персональных данных.

Для эффективной защиты персональных данных в организации необходимо создание и внедрение системы безопасности, представляющей собой комплекс организационных, программно-технических и нормативно-методических мер, который, как правило, включает в себя следующие основные этапы работ:

1. Обследование информационной системы, обрабатывающей персональные данные, и оценка ее соответствия требованиям нормативных документов по защите персональных данных.
2. Классификация информационной системы, обрабатывающей персональные данные.
3. Разработка модели угроз безопасности персональных данных и модели нарушителя.
4. Разработка Технического задания на создание системы защиты персональных данных.
5. Макетирование и стендовые испытания средств защиты информации.
6. Разработка Технического проекта на создание системы защиты персональных данных.
7. Поставка и внедрение технических средств защиты информации.
8. Разработка проектов организационно-распорядительной документации.
9. Оценка соответствия информационной системы, обрабатывающей персональные данные требованиям по безопасности информации.

Такой подход позволяет разделить комплексный проект на несколько этапов, для выполнения которых отводится определенный срок и устанавливаются моменты контрольной отчетности.

Все работы проводятся на основе требований нормативных документов по защите персональных данных Российской Федерации.

Обследование информационной системы, обрабатывающей персональные данные, и оценка ее соответствия требованиям нормативных документов по защите персональных данных, включают в себя:

- анализ внутренних нормативных документов, регламентирующих порядок обработки и защиты персональных данных;
- определение используемых средств защиты персональных данных и оценка их соответствия требованиям нормативных документов РФ;
- определение перечня персональных данных, подлежащих защите;
- определение перечня элементов информационной системы персональных данных, обрабатывающих персональные данные;

– определение степени участия персонала в обработке персональных данных и режима доступа к ним.

По результатам этапа формируется отчет, в котором содержится описание текущего состояния защиты персональных данных, а также рекомендации по устранению выявленных недостатков и нарушений.

Классификация информационной системы, обрабатывающей персональные данные, осуществляется в соответствии с порядком проведения классификации, описанным в приказе Федеральной службы по техническому и экспортному контролю (ФСТЭК), Федеральной службы безопасности (ФСБ) и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20. Результаты классификации информационной системы, обрабатывающей персональные данные, оформляются соответствующим актом подписываемым руководителем предприятия.

Информационные системы, обрабатывающие персональные данные, классифицируются по уровням защищенности в зависимости от важности обрабатываемых персональных данных. Информационная система, обрабатывающая персональные данные, может относиться к классу типовых или специальных. К типовым информационным системам относятся системы, в которых требуется обеспечение только конфиденциальности персональных данных. Специальные информационные системы - системы, в которых дополнительно требуется обеспечить целостность или доступность персональных данных (ПДн). Для типовых информационных систем, обрабатывающих персональные данные (ИСПДн), определено четыре возможных класса: К1, К2, К3 и К4.

Разработка модели угроз безопасности персональных данных и модели нарушителя происходит на основе перечня угроз безопасности персональных данных при их обработке в ИСПДн, который содержится в «Базовой модели угроз безопасности ПДн при их обработке в ИСПДн», определённой ФСТЭК. При необходимости применения средств криптографических защиты разрабатывается **Модель нарушителя** в соответствии с нормативными документами ФСБ России. Именно модель угроз и модель нарушителя являются базовыми документами для дальнейшего проектирования системы защиты персональных данных (СЗПДн).

Разработка Технического задания на создание системы защиты персональных данных, как правило, определяет следующие разделы:

– обоснование разработки СЗПДн;

– исходные данные создаваемой ИСПДн в техническом, программном, информационном и организационном аспектах;

– класс ИСПДн;

– ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;

– мероприятия и требования к СЗПДн, которые определяются в соответствии с классом и типом ИСПДн на основе методических документов ФСТЭК России;

– перечень предполагаемых к использованию сертифицированных средств защиты информации;

– состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

Макетирование и стендовые испытания средств защиты информациипроводятся с учетом исходных данных, полученных на этапе обследования, а также требований, определенных Техническим заданием на СЗПДн. В рамках макетирования проводится анализ применимости, совместимости и внедряемости СЗИ в ИСПДн организации. В результате определяется состав технических средств защиты информации, удовлетворяющий требованиям по защите ПДн, а также позволяющий реализовать мероприятия по созданию СЗПДн. Проводятся стендовые испытания СЗИ. При необходимости производится уточнение Технического задания на СЗПДн.

Разработка Технического проекта на создание системы защиты персональных данных, который содержит детальное описание конкретных программно-технических решений для создания СЗПДн, осуществляется на основе технического задания и результатов стендовых испытаний средств защиты информации.

В состав комплексной системы защиты персональных данных (СЗПДн), как правило, входят следующие подсистемы:

– подсистема управления доступом, предназначенная для защиты от НСД к персональным данным (Панцирь, DeviceLock, eToken Windows Logon);

– подсистема регистрации и учета, обеспечивающая сбор и анализ информации о событиях безопасности (Панцирь);

– подсистема обеспечения целостности, предназначенная для защиты от внесения несанкционированных изменений в ИСПДн и СЗПДн (Adinf);

– подсистема антивирусной защиты, направленная на выявление вредоносных программ (Dr. Web + Kaspersky);

– подсистема межсетевого экранирования, предназначенная для фильтрации потенциально опасных пакетов данных (Cisco ASA);

– подсистема анализа защищенности, обеспечивающая выявление уязвимостей ИСПДн (XSpider, MaxPatrol);

– подсистема обнаружения вторжений, направленная на выявление сетевых атак на ресурсы ИСПДн (IBM Proventia);

– подсистема криптографической защиты, обеспечивающая конфиденциальность и контроль целостности ПДн в процессе их хранения и передачи (S-Terra, ViPNet, Aladdin SecretDisc);

– подсистема управления, предназначенная для централизованного мониторинга информации, поступающей от подсистем СЗПДн (ArcSight).

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных (Приложение 1) определить состав комплексной системы защиты персональных данных.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны, на основании данных первого вопроса разработать проект технического задания на разработку системы обеспечения безопасности информации объекта вычислительной техники.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанный в соответствии с требованиями руководящих документов проект технического задания на разработку системы обеспечения безопасности информации объекта вычислительной техники, обрабатывающий персональные данные.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий выставляется оценка.

Список рекомендуемой литературы

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Методическая литература:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

- http://fstec.ru/ - официальный сайт ФСТЭК РФ;
- http://www.fsb.ru/- официальный сайт ФСБ РФ;
- http://rkn.gov.ru//- официальный сайт Роскомнадзора;
- http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

– Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Лабораторная работа № 11. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

Формируемые компетенции: ОПК-2.3 (ИД-1).

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать нормативные правовые документы в области защиты персональных данных.
2. Знать правовые нормативные акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.
3. Приобрести способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности.
4. Приобрести способность формировать процедуры для управления информационной безопасностью.

Время 90 минут

Распределение времени занятия:

Вступительная часть.	- 5 мин
Проверка готовности студентов к занятию.	- 10 мин
Учебные вопросы занятия:	
1. Разработка инструкции администратора ИСПДн	- 20 мин
2. Разработка инструкции пользователя ИСПДн	- 20 мин
3. Разработка инструкции администратора безопасности при использовании ресурсов объекта вычислительной техники	- 10 мин
4. Разработка инструкции пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций	- 20 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить практические задания, связанные с разработкой инструкций по защите персональных данных в информационных системах

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны для заданных исходных данных разработать инструкцию администратора ИСПДн.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны для заданных исходных данных разработать инструкцию пользователя ИСПДн.

Методические пояснения и рекомендации по выполнению третьего вопроса

В ходе отработки третьего вопроса обучаемые должны для заданных исходных данных разработать инструкцию администратора безопасности при использовании ресурсов объекта вычислительной техники

Методические пояснения и рекомендации по выполнению четвертого вопроса

В ходе отработки четвертого вопроса обучаемые должны для заданных исходных данных разработать инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанные в соответствии с требованиями руководящих документов инструкции должностных лиц.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий, выставляется оценка.

Список рекомендуемой литературы

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Методическая литература:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

– http://fstec.ru/ - официальный сайт ФСТЭК РФ;
– http://www.fsb.ru/- официальный сайт ФСБ РФ;
– http://rkn.gov.ru//- официальный сайт Роскомнадзора;
– http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.
– Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Лабораторная работа № 12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации

Формируемые компетенции: ОПК-5 (ИД-1), ОПК-5 (ИД-2), ОПК-5 (ИД-3), ОПК-2.3. ИД-1

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

1. Знать нормативные правовые документы в области защиты персональных данных.
2. Знать правовые нормативные акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.
3. Уметь формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности.
4. Приобрести способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов.
5. Приобрести способность формировать процедуры для управления информационной безопасностью.

Время 90 минут

Распределение времени занятия:

Вступительная часть.	- 5 мин
Проверка готовности студентов к занятию.	- 10 мин
Учебные вопросы занятия:	
1. Подготовка заявки на аттестацию информационных систем персональных данных	- 30 мин
2. Подготовка необходимой организационно-распорядительной документации	- 40 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

Содержание занятия

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связанные с разработкой заявки на аттестацию информационных систем персональных данных

Проверка готовности студентов к занятию

1. По тестовым вопросам.

Основные теоретические сведения

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;
- предварительное ознакомление с аттестуемым объектом;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- разработка программы и методики аттестационных испытаний;
- заключение договоров на аттестацию;
- проведение аттестационных испытаний объекта информатизации;
- оформление, регистрация и выдача "Аттестата соответствия";
- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
- рассмотрение апелляций.

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, используя шаблон (Приложение 1) для заданных исходных данных с разбором конкретных ситуаций составить заявку на аттестацию информационных систем персональных данных.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны, на основании данных первого вопроса подготовить необходимую организационно-распорядительную документацию для проведения аттестации.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанный в соответствии с требованиями руководящих документов проект технического задания на разработку системы обеспечения безопасности информации объекта вычислительной техники, обрабатывающий персональные данные.

Отчет загрузить в СЭО для проверки преподавателем. Результаты работы должны быть защищены устно каждым студентом.

Заключение

Проводится собеседование по результатам работы с каждым студентом. Студентам, успешно завершившим выполнение всех практических заданий, выставляется оценка.

Список рекомендуемой литературы

1. Положения

1. «Положение по аттестации объектов информатизации по требованиям безопасности информации» (утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.);
2. «Положение о сертификации средств защиты информации по требованиям безопасности информации». Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
3. «Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации». Решение председателя Гостехкомиссии России от 25 ноября 1994 г.
4. «Типовое положение об испытательной лаборатории». Утверждено приказом председателя Гостехкомиссии России от 25 ноября 1994 г.

2. Специальные нормативные документы

1. Методические документы. Профили защиты средств антивирусной защиты. Утверждены ФСТЭК России 14 июня 2012 г.
2. Методические документы. Профили защиты систем обнаружения вторжений. Утверждены ФСТЭК России 6 марта 2012 г.
3. Методические документы. Утверждены ФСТЭК России 3 февраля 2012 г.
4. Профили защиты систем обнаружения вторжений
5. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Решение председателя Гостехкомиссии России от 25 июля 1997 г.
6. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

7. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 г.

8. Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. Гостехкомиссия России, 2003 г.

9. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003 г.

10. Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год

Методическая литература:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Интернет-ресурсы:

– http://fstec.ru/ - официальный сайт ФСТЭК РФ;
– http://www.fsb.ru/- официальный сайт ФСБ РФ;
– http://rkn.gov.ru//- официальный сайт Роскомнадзора;
– http://is.ncfu.ru/ - официальный сайт кафедры организации и технологии защиты информации СКФУ.

Программное обеспечение:

– Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

– Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.

Приложение 1

Кому:_____

(наименование органа по аттестации и его адрес)

З А Я В К А

на проведение аттестации объекта информатизации

1. *(наименование заявителя)* просит провести аттестацию *(наименование объекта информатизации)* на соответствие требованиям по безопасности информации:_____

2. Необходимые исходные данные по аттестуемому объекту информатизации прилагаются.

3. Заявитель готов предоставить необходимые документы и условия для проведения аттестации.

4. Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аттестации указанного в данной заявке объекта информатизации.

5. Дополнительные условия или сведения для договора:

5.1. Предварительное ознакомление с аттестуемым объектом предлагаю провести в период _____

5.2. Аттестационные испытания объекта информатики предлагаю провести в период _____

5.3. Испытания несертифицированных средств и систем информатизации *(наименование средств и систем)* предусмотрено провести в испытательных центрах (лабораториях) *(наименование испытательных центров)* в период _____ (или предлагается провести непосредственно на аттестуемом объекте в период _____)

Другие условия (предложения).

печать

Руководитель (органа заявителя)

(подпись, дата) (Фамилия, И.О.)

Приложение к форме "Заявки..."

Исходные данные по аттестуемому объекту информатизации готовятся на основе следующего перечня вопросов

1. Полное и точное наименование объекта информатизации и его назначение.

2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень секретности (конфиденциальности) обрабатываемой

информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия).

3. Организационная структура объекта информатизации.

4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация (расположенных в помещениях, где она циркулирует).

5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.

6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.

7. Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.

8. Наличие и характер взаимодействия с другими объектами информатизации.

9. Состав и структура системы защиты информации на аттестуемом объекте информатизации.

10. Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.

11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.

12. Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).

13. Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

14. Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Защита персональных данных в информационных системах»
для студентов направления подготовки
10.03.01 Информационная безопасность
Направленность (профиль)
«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»

Ставрополь
2026

СОДЕРЖАНИЕ

1. Общая характеристика самостоятельной работы студента при изучении дисциплины
2. Технологическая карта самостоятельной работы студента
3. Порядок выполнения самостоятельной работы
   3.1 Методические рекомендации по изучению теоретического материала
   3.2 Методические рекомендации по конспектированию первоисточников
   3.3 Методические рекомендации по подготовке к лабораторной работе
4. Список литературы

Введение

Цель освоения дисциплины - теоретическая и практическая подготовленность бакалавра для проведения работ по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах (ИС) в соответствии с современными требованиями, а также приобретение набора компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачи освоения дисциплины:

- формирование знаний нормативно-правовой документации в области персональных данных и умений работы с ней с использованием современных информационных технологий;
- формирование умений выявления угроз и уязвимостей безопасности персональных данных с подготовкой отчетов в цифровом или бумажном формате;
- формирование умений по разработке организационных и технических мер по обеспечению безопасности персональных данных;
- формирование навыков разработки организационно-распорядительных документов в области защиты персональных данных с использованием офисных приложений;
- формирование навыков самостоятельного изучения литературы в области обеспечения безопасности персональных данных с использованием инструментария электронных библиотечных систем, а также порталов регуляторов в области защиты информации.

1. Общая характеристика самостоятельной работы студента при изучении дисциплины

Самостоятельная работа включает те разделы курса, которые не получили достаточного освещения на лекциях по причине ограниченности лекционного времени и большого объема изучаемого материала.

Методическое обеспечение самостоятельной работы по дисциплине состоит из:

1) Определения учебных вопросов, которые студенты должны изучить самостоятельно;

2) Подбора необходимой учебной литературы, обязательной для проработки и изучения;

3) Поиска дополнительной научной литературы, к которой студенты могут обращаться по желанию, если у них возникает интерес в данной теме;

4) Определения контрольных вопросов, позволяющих студентам самостоятельно проверить качество полученных знаний;

5) Организации консультаций преподавателя со студентами для разъяснения вопросов, вызвавших у обучающихся затруднения при самостоятельном освоении учебного материала.

Самостоятельная работа студента – это особым образом организованная деятельность, включающая в свою структуру такие компоненты, как:

- уяснение цели и поставленной учебной задачи;
- четкое и системное планирование самостоятельной работы;
- поиск необходимой учебной и научной информации;
- освоение собственной информации и ее логическая переработка;
- использование методов исследовательской, научно-исследовательской работы для решения поставленных задач;
- выработка собственной позиции по поводу полученной задачи;
- представление, обоснование и защита полученного решения;
- проведение самоанализа и самоконтроля

К основным видам самостоятельной работы студентов относится:

- работа с понятийным аппаратом;
- конспектирование первоисточников;
- самостоятельное изучение литературы;
- подготовка к лекциям;
- подготовка к лабораторным работам;

Контроль знаний студентов включает формы текущего и итогового контроля. Текущий контроль осуществляется в процессе изучения курса и включает в себя оценку работы студентов на практических занятиях (круглый стол, собеседование, групповые научные проекты, тестирование), а также подготовку домашнего задания.

2. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
6 семестр					
ОПК-5. ИД-2, ИД-3 ОПК-2.3. ИД-1	Подготовка к лекции	Собеседование	14.00	2.00	16.00
ОПК-5. ИД-2, ИД-3 ОПК-2.3. ИД-1	Подготовка к лабораторной работе	Собеседование	12.00	2.00	14.00
ОПК-5. ИД-2, ИД-3 ОПК-2.3. ИД-1	Самостоятельное изучение литературы и нормативных документов	Собеседование	12.00	2.00	14.00
Итого за 6 семестр			38.00	6.00	44.00
Итого			38.00	6.00	44.00

3. Порядок выполнения самостоятельной работы

3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Защита персональных данных в информационных системах» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения практических занятий, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям.

Работа с конспектом лекций

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

Выполнение лабораторных работ по дисциплине «Защита персональных данных в информационных системах»

На первом занятии получите у преподавателя индивидуальные задания по курсу, планы подготовки к лабораторным работам. Обзаведитесь всем необходимым методическим обеспечением.

Перед лабораторными работами изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью лабораторных работ является:

– формирование умений по разработке организационных и технических мер по обеспечению безопасности персональных данных;

– формирование умений выявления угроз и уязвимостей безопасности персональных данных с подготовкой отчетов в цифровом или бумажном формате;

– формирование навыков разработки организационно-распорядительных документов в области защиты персональных данных с использованием офисных приложений;

– восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

3.2 Методические рекомендации по конспектированию первоисточников

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материал, одной из обязательных форм организации умственного труда.

Планом удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

Тезисы предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.

5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

По форме *конспекты подразделяются* на формализованные и графические.

1. Формализованные (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

2. Графические (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

Плановый – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

Текстуальный – это конспект, созданный в основном из цитат.

Сводный конспект – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

Тематический – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

Способы конспектирования.

– ***Тезисы*** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

– ***Линейно-последовательная запись текста.*** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

– С***пособ «вопросов – ответов».*** Он заключается в том, что, поделив страницу тетради пополам вертикальной ***чертой***, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

– ***Схема с фрагментами*** **–** способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

– ***Простая схема*** **–** способ конспектирования, близкий к схеме с фрагментами, объяснений к которой ***конспектирующий*** не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

– ***Параллельный способ*** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

Однако лучше использовать разные способы конспектирования для записи одного и того же материала.

Комбинированный конспект – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

Принципы составления конспекта прочитанного.

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.

2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

1. Резюмирование.

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

2. Аннотация.

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуется изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

- тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)
- задачи, поставленные автором аннотируемого документа
- метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)
- принадлежность автора к определенной научной школе или направлению
- структуру аннотируемого документа
- предмет и тему произведения, основные положения и выводы автора
- характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

3.3 Методические рекомендации по подготовке к лабораторной работе

Задания и материалы к лабораторным работам выкладываются преподавателем в системе электронного обучения. Накануне проведения лабораторной работы студенту следует ознакомиться с программой проведения лабораторной работы, материалом лекций по теме лабораторной работы и изучить рекомендованную литературу. Перед началом цикла

лабораторных работ студенту необходимо выбрать исходные данные, которые будут использоваться во всех лабораторных работах.

После выполнения лабораторной работы по теме занятия, студент долен оформить результаты в виде рекомендованного отчета загрузить этот отчет для проверки преподавателем в систему электронного обучения и подготовить ответы на вопросы для устного собеседования.

Вопросы для собеседования по лабораторным работам

Лабораторная работа № 1. Разработка приказов об организации работ по обеспечению безопасности персональных данных

1. Поясните порядок разработки приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
2. Поясните порядок разработки приказа о назначении ответственного за обработку персональных данных
3. Поясните порядок разработки приказа о создании комиссии по организации и проведению работ по защите персональных данных
4. Поясните содержание приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
5. Поясните содержание приказа о назначении ответственного за обработку персональных данных
6. Поясните содержание приказа о создании комиссии по организации и проведению работ по защите персональных данных

Лабораторная работа № 2. Разработка перечней персональных данных, информационных систем персональных данных и применяемых средств защиты информации

1. Поясните порядок разработки перечня персональных данных, подлежащих защите в информационных системах персональных данных.
2. Поясните порядок разработки перечня информационных систем персональных данных, в которых должна быть обеспечена безопасность информации.
3. Поясните порядок разработки перечня применяемых средств защиты информации, эксплуатационной и технической документации к ним.
4. Поясните содержание перечня персональных данных, подлежащих защите в информационных системах персональных данных.
5. Поясните содержание перечня информационных систем персональных данных, в которых должна быть обеспечена безопасность информации.
6. Поясните содержание перечня применяемых средств защиты информации, эксплуатационной и технической документации к ним.

Лабораторная работа № 3. Разработка согласия субъекта персональных данных на обработку его персональных данных.

1. Поясните порядок разработки согласия субъекта персональных данных на обработку его персональных данных
2. Поясните содержание согласия субъекта персональных данных на обработку его персональных данных
3. В каких случаях обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных
4. В каких случаях согласие на обработку его персональных данных дает законный представитель субъекта персональных данных
5. Кто устанавливает требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения
6. На обработку каких категории персональных данных дается согласие субъекта персональных данных

Лабораторная работа № 4. Разработка уведомительных документов об обработке персональных данных

1. Поясните порядок разработки Уведомления об обработке персональных данных.
2. Поясните содержание Уведомления об обработке персональных данных.
3. Какие категории персональных данных, подлежащих обработке указываются в Уведомлении об обработке персональных данных?
4. Какие сведения случае использования Оператором, осуществляющим обработку персональных данных, шифровальных (криптографических) указываются в Уведомлении об обработке персональных данных?
5. Поясните порядок составления заявления об исключении сведений из реестра операторов, осуществляющих обработку персональных данных.
6. Поясните порядок составления о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных.
7. Поясните порядок составления информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.

Лабораторная работа № 5. Определение уровня защищенности персональных данных

1. В каком случае информационная система является информационной системой, обрабатывающей специальные категории персональных данных?

2. В каком случае информационная система является информационной системой, обрабатывающей биометрические персональные данные?
3. В каком случае информационная система является информационной системой, обрабатывающей общедоступные персональные данные?
4. В каком случае информационная система является информационной системой, обрабатывающей иные категории персональных данных?
5. В каком случае информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора?
6. Что понимается под актуальными угрозами безопасности персональных данных?
7. В каком случае для информационной системы актуальны угрозы 1-го типа?
8. В каком случае для информационной системы актуальны угрозы 2-го типа?
9. В каком случае для информационной системы актуальны угрозы 3-го типа?
10. Перечислите условия, при которых в информационной системе при обработке персональных данных устанавливается необходимость обеспечения 1-го уровня защищенности персональных данных (УЗ1)?
11. Перечислите условия, при которых в информационной системе при обработке персональных данных устанавливается необходимость обеспечения 2-го уровня защищенности персональных данных (УЗ2)?
12. Перечислите условия, при которых в информационной системе при обработке персональных данных устанавливается необходимость обеспечения 3-го уровня защищенности персональных данных (УЗ3)?
13. Перечислите условия, при которых в информационной системе при обработке персональных данных устанавливается необходимость обеспечения 4-го уровня защищенности персональных данных (УЗ4)?

Лабораторная работа № 6. Разработка модели угроз безопасности персональных данных при их обработке в информационных системах

1. Что определяет методика оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 г.?
2. Когда применяется методика оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 г.?
3. На оценку каких угроз ориентирована методика оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 г.?
4. Какие основные задачи решаются в ходе оценки угроз безопасности персональных данных?

5. Что является исходными данными для оценки угроз безопасности персональных данных?
6. Какие работы проводятся на этапе создания систем и сетей при оценке угроз безопасности персональных данных?
7. Какие работы проводятся в ходе эксплуатации систем и сетей при оценке угроз безопасности персональных данных?
8. На что должны быть направлены результаты оценки угроз безопасности персональных данных на этапе эксплуатации систем и сетей?
9. На что должны быть направлены результаты оценки угроз безопасности персональных данных на этапе создания систем и сетей?
10. Кто проводит оценку угроз безопасности персональных данных?
11. Какие знания и умения должны иметь специалистов привлекаемые для оценки угроз безопасности персональных данных?
12. С использованием какого метода безопасности проводится оценка угроз персональных данных?
13. Где отражаются результаты оценки угроз безопасности персональных данных?
14. В каких случаях осуществляется изменение модели угроз безопасности персональных данных?
15. Какие этапы включает оценка угроз безопасности персональных данных?
16. Что является исходными данными для определения негативных последствий от реализации угроз безопасности персональных данных?
17. Что является исходными данными для определения возможных объектов воздействия?
18. Какой порядок определения возможных объектов воздействия угроз безопасности персональных данных?
19. Какой порядок определения негативных последствий от реализации (возникновения) угроз безопасности персональных данных?
20. Какой порядок оценки возможности реализации (возникновения) угроз безопасности персональных данных и определение их актуальности?
21. Что является исходными данными для определения возможных актуальных нарушителей?
22. Какими являются основные виды нарушителей, подлежащих оценке при моделировании угроз?
23. Когда нарушители признаются актуальными для систем и сетей?
24. Как подразделяются нарушители в зависимости от уровня возможностей?
25. Какие нарушители относятся к внешним нарушителям?
26. Какие нарушители относятся к внутренним нарушителям?

27. Какие угрозы безопасности информации реализуют внешние нарушители
28. Какие угрозы безопасности информации реализуют внутренние нарушители
29. Что может являться основными факторами возникновения угроз безопасности информации, связанными с техногенными источниками?
30. Что должно быть определено по результатам определения источников угроз безопасности персональных данных?
31. Поясните каким образом осуществляется оценка способов реализации (возникновения) угроз безопасности персональных данных.
32. Что является исходными данными для определения актуальных способов реализации (возникновения) угроз безопасности персональных данных?
33. Назовите основные способы реализации (возникновения) угроз безопасности персональных данных?
34. Поясните каким образом осуществляется оценка актуальности угроз безопасности персональных данных.
35. Что является исходными данными для оценки актуальности угроз безопасности персональных данных?
36. Что такое сценарии реализации угроз безопасности персональных данных?
37. Что включает определение сценариев реализации угрозы на этапе эксплуатации систем и сетей?
38. Поясните рекомендуемую структуру модели угроз безопасности персональных данных.

Лабораторная работа № 7. Разработка Концепции информационной безопасности

1. Поясните порядок определение основных целей построения системы защиты персональных данных организации.
2. Поясните порядок определение задач защиты персональных данных организации.
3. Поясните порядок определение общей стратегии построения системы защиты персональных данных организации.
4. Что определяет Концепция обеспечения безопасности информации в автоматизированной системе организации?
5. Какие вопросы должны быть отражены В Концепции информационной безопасности?
6. На какие структурные подразделения организации распространяются основные положения и требования Концепции информационной безопасности?

Лабораторная работа № 8. Разработка Политики информационной безопасности

1. Что понимается под политикой информационной безопасности?
2. Какие направления защиты информационных систем персональных данных рассматриваются в политике информационной безопасности?
3. Какие этапы создания СЗИ должна описывать политика информационной безопасности?
4. Какими принципами целесообразно руководствоваться при разработке политики информационной безопасности?
5. Что является основой избирательной политики безопасности?
6. Что составляет основу полномочной политики безопасности?
7. Какое основное назначение полномочной политики безопасности?

Лабораторная работа № 9. Разработка плана мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных

1. На основании чего составляется план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных?
2. Какие категории мероприятий включаются в план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных?
3. На какие информационные системы персональных данных организации составляется план внутренних проверок?
4. Поясните порядок разработки плана мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных.

Лабораторная работа № 10. Разработка требований к информационной системе по обеспечению безопасности персональных данных

1. Перечислите основные этапы работ создания и внедрения системы по обеспечению безопасности персональных данных.
2. Что включают в себя обследование информационной системы, обрабатывающей персональные данные, и оценка ее соответствия требованиям нормативных документов по защите персональных данных?
3. Какие разделы должно содержать техническое задание на создание системы защиты персональных данных?
4. Каким образом проводятся макетирование и стендовые испытания средств защиты информации?
5. Какие подсистемы, как правило, входят в состав комплексной системы защиты персональных данных?

Лабораторная работа № 11. Разработка инструкций по защите персональных данных в информационных системах

1. Что должна содержать инструкция администратора ИСПДн?
2. Что должна содержать инструкция пользователя ИСПДн?
3. Что должна содержать инструкция администратора безопасности при использовании ресурсов объекта вычислительной техники?
4. Что должна содержать инструкция пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций?

Лабораторная работа № 12. Аттестация информационных систем персональных данных по требованиям безопасности информации

1. Что понимается под аттестацией объектов информатизации?
2. Какие действия включает проведение аттестации объектов информатизации по требованиям безопасности информации?
3. Поясните порядок разработки программы и методики аттестационных испытаний объектов информатизации.
4. Поясните порядок осуществления государственного контроля и надзора, инспекционного контроля за проведением аттестации объектов информатизации.
5. Поясните порядок осуществления государственного контроля и надзора, инспекционного контроля за эксплуатацией аттестованных объектов информатизации.
6. Поясните порядок испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте

Индивидуальное задание для самостоятельной работы студентов

Вопросы для собеседования.

1. В каких случаях обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных
2. В каких случаях осуществляется изменение модели угроз безопасности информации?
3. В каких случаях согласие на обработку его персональных данных дает законный представитель субъекта персональных данных
4. В каком случае для информационной системы актуальны угрозы 1-го типа?
5. В каком случае для информационной системы актуальны угрозы 2-го типа?
6. В каком случае для информационной системы актуальны угрозы 3-го типа?

7. В каком случае информационная система является информационной системой, обрабатывающей биометрические персональные данные?
8. В каком случае информационная система является информационной системой, обрабатывающей общедоступные персональные данные?
9. В каком случае информационная система является информационной системой, обрабатывающей иные категории персональных данных?
10. В каком случае информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора?
11. Где отражаются результаты оценки угроз безопасности информации?
12. Для чего предназначена подсистема анализа защищенности информационной системы по обеспечению безопасности персональных данных?
13. Для чего предназначена подсистема криптографической защиты информационной системы по обеспечению безопасности персональных данных?
14. Для чего предназначена подсистема регистрации и учета информационной системы по обеспечению безопасности персональных данных?
15. Для чего предназначена подсистема управления доступом, информационной системы по обеспечению безопасности персональных данных?
16. Для чего предназначена подсистема управления информационной системы по обеспечению безопасности персональных данных?
17. Как подразделяются нарушители в зависимости от уровня возможностей?
18. Какие вопросы должны быть отражены В Концепции информационной безопасности?
19. Какие действия включает проведение аттестации объектов информатизации по требованиям безопасности информации?
20. Какие знания и умения должны иметь специалистов привлекаемые для оценки угроз безопасности информации?
21. Какие категории мероприятий включаются в план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных?
22. Какие категории персональных данных, подлежащих обработке указываются в Уведомлении об обработке персональных данных?
23. Какие направления защиты информационных систем персональных данных рассматриваются в политике информационной безопасности?
24. Какие нарушители относятся к внешним нарушителям?
25. Какие нарушители относятся к внутренним нарушителям?
26. Какие основные задачи решаются в ходе оценки угроз безопасности информации?

27. Какие подсистемы, как правило, входят в состав комплексной системы защиты персональных данных? На основании чего составляется план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных?
28. Какие работы проводятся в ходе эксплуатации систем и сетей при оценке угроз безопасности информации?
29. Какие работы проводятся на этапе создания систем и сетей при оценке угроз безопасности информации?
30. Какие разделы должно содержать техническое задание на создание системы защиты персональных данных?
31. Какие сведения случае использования Оператором, осуществляющим обработку персональных данных, шифровальных (криптографических) указываются в Уведомлении об обработке персональных данных?
32. Какие угрозы безопасности информации реализуют внешние нарушители
33. Какие угрозы безопасности информации реализуют внутренние нарушители
34. Какие этапы включает оценка угроз безопасности информации?
35. Какие этапы создания СЗИ должна описывать политика информационной безопасности?
36. Каким образом проводятся макетирование и стендовые испытания средств защиты информации?
37. Какими принципами целесообразно руководствоваться при разработке политики информационной безопасности?
38. Какими являются основные виды нарушителей, подлежащих оценке при моделировании угроз?
39. Какое основное назначение полномочной политики безопасности?В каком случае информационная система является информационной системой, обрабатывающей специальные категории персональных данных?
40. Какой порядок определения возможных объектов воздействия угроз безопасности информации?
41. Какой порядок определения негативных последствий от реализации (возникновения) угроз безопасности информации?
42. Какой порядок оценки возможности реализации (возникновения) угроз безопасности информации и определение их актуальности?
43. Когда нарушители признаются актуальными для систем и сетей?
44. Когда применяется методика оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 г.?
45. Кто проводит оценку угроз безопасности информации?
46. Кто устанавливает требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения

47. На какие информационные системы персональных данных организации составляется план внутренних проверок?
48. На какие структурные подразделения организации распространяются основные положения и требования Концепции информационной безопасности?
49. На обработку каких категории персональных данных дается согласие субъекта персональных данных
50. На оценку каких угроз ориентирована методика оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 г.?
51. На что должны быть направлены результаты оценки угроз безопасности информации на этапе эксплуатации систем и сетей?
52. На что должны быть направлены результаты оценки угроз безопасности информации на этапе создания систем и сетей?
53. Назовите основные способы реализации (возникновения) угроз безопасности информации?
54. Перечислите основные этапы работ создания и внедрения системы по обеспечению безопасности персональных данных.
55. Перечислите условия, при которых в информационной системе при обработке персональных данных устанавливается необходимость обеспечения 1-го уровня защищенности персональных данных (УЗ1)?
56. Перечислите условия, при которых в информационной системе при обработке персональных данных устанавливается необходимость обеспечения 2-го уровня защищенности персональных данных (УЗ2)?
57. Перечислите условия, при которых в информационной системе при обработке персональных данных устанавливается необходимость обеспечения 3-го уровня защищенности персональных данных (УЗ3)?
58. Перечислите условия, при которых в информационной системе при обработке персональных данных устанавливается необходимость обеспечения 4-го уровня защищенности персональных данных (УЗ4)? Поясните порядок разработки Уведомления об обработке персональных данных.
59. Поясните каким образом осуществляется оценка актуальности угроз безопасности информации.
60. Поясните каким образом осуществляется оценка способов реализации (возникновения) угроз безопасности информации.
61. Поясните порядок испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте
62. Поясните порядок определение задач защиты персональных данных организации.
63. Поясните порядок определение общей стратегии построения системы защиты персональных данных организации.
64. Поясните порядок определение основных целей построения системы защиты персональных данных организации.

65. Поясните порядок осуществления государственного контроля и надзора, инспекционного контроля за проведением аттестации объектов информатизации.
66. Поясните порядок осуществления государственного контроля и надзора, инспекционного контроля за эксплуатацией аттестованных объектов информатизации.
67. Поясните порядок разработки перечня информационных систем персональных данных, в которых должна быть обеспечена безопасность информации.
68. Поясните порядок разработки перечня персональных данных, подлежащих защите в информационных системах персональных данных.
69. Поясните порядок разработки перечня применяемых средств защиты информации, эксплуатационной и технической документации к ним.
70. Поясните порядок разработки плана мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных. Что понимается под политикой информационной безопасности?
71. Поясните порядок разработки приказа о назначении ответственного за обработку персональных данных
72. Поясните порядок разработки приказа о создании комиссии по организации и проведению работ по защите персональных данных
73. Поясните порядок разработки приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
74. Поясните порядок разработки программы и методики аттестационных испытаний объектов информатизации.
75. Поясните порядок составления заявления об исключении сведений из реестра операторов, осуществляющих обработку персональных данных.
76. Поясните порядок составления информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных. Поясните порядок разработки согласия субъекта персональных данных на обработку его персональных данных
77. Поясните порядок составления о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных.
78. Поясните рекомендуемую структуру модели угроз безопасности информации.
79. Поясните содержание перечня информационных систем персональных данных, в которых должна быть обеспечена безопасность информации.
80. Поясните содержание перечня персональных данных, подлежащих защите в информационных системах персональных данных.
81. Поясните содержание перечня применяемых средств защиты информации, эксплуатационной и технической документации к ним.

82. Поясните содержание приказа о назначении ответственного за обработку персональных данных
83. Поясните содержание приказа о создании комиссии по организации и проведению работ по защите персональных данных.
84. Поясните содержание приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
85. Поясните содержание согласия субъекта персональных данных на обработку его персональных данных
86. Поясните содержание Уведомления об обработке персональных данных.
87. С использованием какого метода безопасности проводится оценка угроз информации?
88. Что включает определение сценариев реализации угрозы на этапе эксплуатации систем и сетей?
89. Что включают в себя обследование информационной системы, обрабатывающей персональные данные, и оценка ее соответствия требованиям нормативных документов по защите персональных данных?
90. Что должно быть определено по результатам определения источников угроз безопасности информации?
91. Что может являться основными факторами возникновения угроз безопасности информации, связанными с техногенными источниками?
92. Что определяет Концепция обеспечения безопасности информации в автоматизированной системе организации?
93. Что определяет методика оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 г.?
94. Что понимается под актуальными угрозами безопасности персональных данных?
95. Что понимается под аттестацией объектов информатизации?
96. Что составляет основу полномочной политики безопасности?
97. Что такое сценарии реализации угроз безопасности информации?
98. Что является исходными данными для определения актуальных способов реализации (возникновения) угроз безопасности информации?
99. Что является исходными данными для определения возможных актуальных нарушителей?
100. Что является исходными данными для определения возможных объектов воздействия?
101. Что является исходными данными для определения негативных последствий от реализации угроз безопасности информации?
102. Что является исходными данными для оценки актуальности угроз безопасности информации?
103. Что является исходными данными для оценки угроз безопасности информации?

104. Что является основой избирательной политики безопасности?

4. Список литературы

Основная литература:

1. Петренко, В. И. Защита персональных данных в информационных системах: учебное пособие / В. И. Петренко. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 201 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/66023.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

2. Петренко, В. И. Защита персональных данных в информационных системах: лабораторный практикум / В. И. Петренко, И. В. Мандрица. — Ставрополь : Северо-Кавказский федеральный университет, 2018. — 118 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/83198.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

3. Технические средства и методы защиты информации: учебное пособие / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков, И. В. Голубятников. — Москва: Горячая линия-Телеком, 2012. — 616 с. — ISBN 978-5-9912-0084-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/5154 (дата обращения: 18.10.2022).

Дополнительная литература:

1. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 222 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/63138.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. Пользователей

2. Петренко, В. И. Защита персональных данных в информационных системах. Практикум / В. И. Петренко, И. В. Мандрица. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-507-45301-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/264242 (дата обращения: 04.03.2023). — Режим доступа: для авториз. пользователей.

3. Воробьев, Е. Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных : учебное пособие / Е. Г. Воробьев. — Санкт-Петербург : Интермедия, 2017. — 432 с. — ISBN 978-5-4383-0120-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/66796.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. Пользователей

4. Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-

Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 121 c. — ISBN 978-5-4497-0334-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89449.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

5. Голембиовская, О. М. Формализация подходов к обеспечению защиты персональных данных : монография / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков. — Саратов : Ай Пи Эр Медиа, 2019. — 198 c. — ISBN 978-5-4486-0726-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/81851.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. Пользователей

6. Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных : монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. — Москва : Ай Пи Ар Медиа, 2020. — 236 c. — ISBN 978-5-4497-0535-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95150.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

7. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.: ил

Методическая литература:

1. Методические указания к выполнению лабораторных работ по дисциплине «Защита персональных данных в информационных системах» для студентов направления подготовки 10.03.01 «Информационная безопасность» (электронная версия).

2. Международные документы:
   a. Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS от 28.01.1981 № 108
   b. Директива 97/66/ЕС Европейского парламента и Совета Европейского Союза от 15 декабря 1997 г., касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций.
   c. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

3. Указы Президента РФ:
   a. Стратегия национальной безопасности Российской Федерации. Указ Президента Российской Федерации от 02.07.2021 г. № 400

b. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 05.12.2016 г. № 646

4. Федеральные законы:
   a. Федеральный закон "О персональных данных" от 27.07.2006 г. №152-ФЗ
   b. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 г. № 149-ФЗ
5. Постановления Правительства РФ:
   a. Постановление от 6 июля 2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"
   b. Постановление от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"
   c. Постановление от 1 ноября 2012 года №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
   d. Постановление от 23 октября 2021 № 1815 "Об утверждении перечня случаев осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных ... "
   e. Постановление Правительства РФ от 29.06.2021 № 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных"
   f. Постановление Правительства РФ от 11.10.2021 № 1729 "Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере идентификации и (или) аутентификации"
   g. Постановление Правительства РФ от 20.10.2021 № 1799 "Об аккредитации организаций, владеющих информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающих услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц"
6. Документы ФСТЭК:
   a. Приказ ФСТЭК России от 18 февраля 2013 г. N 21. "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных

данных при их обработке в информационных системах персональных данных"

b. Приказ ФСТЭК России от 30 июля 2018 г. N 131. "Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий"
c. Государственный реестр сертифицированных средств защиты информации

7. Документы ФСБ:

a. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Утверждены руководством 8 Центра ФСБ России 31 марта 2015 года №149/7/2/6-432.
b. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности. Приказ от 10 июля 2014г. №378
c. Выписка из перечня средств защиты информации, сертифицированных ФСБ России. http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_15.04.2022.doc

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). http://rkn.gov.ru//
2. Официальный сайт ФСТЭК РФ. http://fstec.ru/
3. Официальный сайт ФСБ РФ. http://www.fsb.ru/
4. Консорциум сетевых электронных библиотек ЭБС «Лань». https://e.lanbook.com/
5. ЭБС «Университетская библиотека ОНЛАЙН». http://biblioclub.ru
6. ЭБС IPRbooks. http://www.iprbookshop.ru
7. ЭБС «Biblio-online.ru». http://biblio-online.ru/

8. Цифровая платформа «East View». https://dlib.eastview.com/browse/udb/12

Программное обеспечение:

Класс персональных ЭВМ, электронная доска, маркеры. Программное обеспечение в комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.

Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных №2012620913. Зарегистрировано 11.09.2012. Заявка №2012620729 от 16.07.2012.