МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению лабораторных работ
по дисциплине
«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск
2025

ВВЕДЕНИЕ

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Защита персональных данных в информационных системах» является 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».

2.Наименование лабораторных занятий

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
6 семестр			
1	Лабораторная работа №1. Разработка приказов об организации работ по обеспечению безопасности персональных данных	4	4
2	Лабораторная работа №2 Разработка перечней персональных данных, информационных систем персональных данных и применяемых средств защиты информации	4	4
3	Лабораторная работа №3 Разработка согласия субъекта персональных данных на обработку его персональных данных	2	4
4	Лабораторная работа №4 Разработка уведомительных документов об обработке персональных данных	4	4
5	Лабораторная работа № 5 Разработка частной модели угроз безопасности персональных данных при их обработке в информационной системе	2	4
6	Лабораторная работа №6 Разработка Политики информационной безопасности	4	2
7	Лабораторная работа № 7 Разработка плана мероприятий по обеспечению защиты персональных данных в информационных	4	2

	системах персональных данных		
8	Лабораторная работа № 8 Аттестация информационных систем персональных данных по требованиям безопасности информации	4	4
9	Лабораторная работа № 9. Разработка требований к информационной системе по обеспечению безопасности персональных данных	4	4
	Итого за 6 семестр	**32**	**32**
	Итого	**32**	**32**

СТРУКТУРА И СОДЕРЖАНИЕ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

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.

СОДЕРЖАНИЕ ЗАНЯТИЯ

Вступительная часть

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

Содержание занятия

Основные теоретические сведения.

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных (Приложение 2) 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 (Приложение 2) 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 (Приложение 2) 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 (Приложение 2):

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.

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 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.

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.

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.

***Варианты базового уровня*:**

1) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для дошкольной образовательной организации.

2) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для общеобразовательной организации.

3) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для профессиональной образовательной организации.

4) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для юридического агентства.

5) Разработать приказ о назначении ответственного за обработку персональных данных для дошкольной образовательной организации.

6) Разработать приказ о назначении ответственного за обработку персональных данных для общеобразовательной организации.

7) Разработать приказ о назначении ответственного за обработку персональных данных для профессиональной образовательной организации.

8) Разработать приказ о назначении ответственного за обработку персональных данных для агентства недвижимости.

9) Разработать приказ о назначении ответственного за обработку персональных данных для юридического агентства.

10) Разработать приказ о назначении ответственного за обработку персональных данных для администрации города.

11) Разработать приказ о назначении ответственного за обработку персональных данных для автотранспортного предприятия.

12) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для дошкольной образовательной организации.

13) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для общеобразовательной организации.

14) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для профессиональной образовательной организации.

15) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для агентства недвижимости.

16) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для юридического агентства.

17) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для администрации города.

18) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для автотранспортного предприятия.

***Варианты повышенного уровня*:**

1) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для образовательной организации высшего образования.

2) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для организации дополнительного профессионального образования.

3) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для городской поликлиники.

4) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для для городской детской поликлиники.

5) Разработать приказ о назначении ответственного за обработку персональных данных для образовательной организации высшего образования.

6) Разработать приказ о назначении ответственного за обработку персональных данных для организации дополнительного образования.

7) Разработать приказ о назначении ответственного за обработку персональных данных для организации дополнительного профессионального образования.

8) Разработать приказ о назначении ответственного за обработку персональных данных для городской поликлиники.

9) Разработать приказ о назначении ответственного за обработку персональных данных для городской детской поликлиники.

10) Разработать приказ о назначении ответственного за обработку персональных данных для министерства здравоохранения края.

11) Разработать приказ о назначении ответственного за обработку персональных данных для городской больницы.

12) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для образовательной организации высшего образования.

13) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для организации дополнительного образования.

14) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для организации дополнительного профессионального образования.

15) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для городской поликлиники.

16) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для городской детской поликлиники.

17) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для министерства здравоохранения края.

18) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для городской больницы.

ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ЛАБОРАТОРНОЙ РАБОТЕ

по учебной дисциплине

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»

для студентов направления подготовки
10.03.01 – «Информационная
безопасность»

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

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

5. 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.
6. Уметь разрабатывать уведомительные и организационно-распорядительные документы, необходимые для эффективной защиты персональных данных в соответствии с требованиями действующего законодательства.
7. Приобрести навыки разработки необходимых документов в интересах организации работ по обеспечению безопасности ИСПДн.
8. Приобрести навыки анализа и обобщения полученных результатов.

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, 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

2. По тестовым вопросам.

Содержание занятия

Основные теоретические сведения.

Материал лекции по теме 4. 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 (Приложение 1) 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 (Приложение 1) путем решения проблемных задач разработать перечень информационных систем персональных данных, в которых должна быть обеспечена безопасность информации.

Методические пояснения и рекомендации по выполнению третьего вопроса

В ходе отработки третьего вопроса, обучаемые должны для заданных исходных данных (Приложение 1) путем решения проблемных задач разработать перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним.

Отчетность за занятие

Отчет по лабораторной работе должен содержать разработанные для заданных исходных данных (Приложение 1):

4. Перечень персональных данных, подлежащих защите в информационных системах персональных данных.

5. Перечень перечня информационных систем персональных данных, в которых должна быть обеспечена безопасность информации

6. Перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним

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:

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

Приложение №1

***Варианты базового уровня*:**

1) Разработать перечень персональных данных, обрабатываемых в дошкольной образовательной организации.
2) Разработать перечень персональных данных, обрабатываемых в общеобразовательной организации.
3) Разработать перечень персональных данных, обрабатываемых в профессиональной образовательной организации.
4) Разработать перечень персональных данных, обрабатываемых в агентстве недвижимости.
5) Разработать перечень персональных данных, обрабатываемых в юридическом агентстве.
6) Разработать перечень персональных данных, обрабатываемых в администрации города.
7) Разработать перечень персональных данных, обрабатываемых в автотранспортном предприятии.
8) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для дошкольной образовательной организации.

9) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для общеобразовательной организации.

10) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для профессиональной образовательной организации.

11) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для агентства недвижимости.

12) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для юридического агентства.

13) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для администрации города.

14) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для автотранспортного предприятия.

***Варианты повышенного уровня*:**

1) Разработать перечень персональных данных, обрабатываемых в образовательной орга-низации высшего образования.

2) Разработать перечень персональных данных, обрабатываемых в организации дополни-тельного образования.

3) Разработать перечень персональных данных, обрабатываемых в организации дополни-тельного профессионального образования.

4) Разработать перечень персональных данных, обрабатываемых в городской поликлини-ке.

5) Разработать перечень персональных данных, обрабатываемых в городской детской поликлинике.

6) Разработать перечень персональных данных, обрабатываемых в министерстве здраво-охранения края.

7) Разработать перечень персональных данных, обрабатываемых в городской больнице.

8) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для образовательной организации высшего образования.

9) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для организации дополнительного образования.

10) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для организации дополнительного профессионального образования.

11) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для городской поликлиники.

12) Разработать информационных систем персональных данных и применяемых средств защиты информации для городской детской поликлиники.

13) Разработать перечень информационных систем персональных данных и применяемых

ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ЛАБОРАТОРНОЙ РАБОТЕ

по учебной дисциплине

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»

для студентов направления подготовки
10.03.01 – «Информационная безопасность»

Занятие № 3. Разработка согласия субъекта персональных данных на обработку его персональных данных

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

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

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

3. По тестовым вопросам.

Содержание занятия

Основные теоретические сведения.

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

Методические пояснения и рекомендации по выполнению второго третьего 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:

7. Согласие субъекта персональных данных на обработку его персональных данных.
8. Журнал учета согласий субъектов персональных данных

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.

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 регистра-

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 нали-чия оснований, указанных в **пунктах 2 - 11 части 1 статьи 6**, **части 2 статьи 10** и **части 2 ста-тьи 11** настоящего Федерального закона.

Приложение №2

***Варианты базового уровня*:**

1) Разработать согласие субъекта персональных данных и журнал учета согласий субъек-тов персональных данных на обработку его персональных данных для дошкольной образователь-ной организации.

2) Разработать согласие субъекта персональных данных и журнал учета согласий субъек-тов персональных данных на обработку его персональных данных для общеобразовательной орга-низации.

3) Разработать согласие субъекта персональных данных и журнал учета согласий субъек-тов персональных данных на обработку его персональных данных для профессиональной образо-вательной организации.

4) Разработать согласие субъекта персональных данных и журнал учета согласий субъек-тов персональных данных на обработку его персональных данных для агентства недвижимости.

5) Разработать согласие субъекта персональных данных и журнал учета согласий субъек-тов персональных данных на обработку его персональных данных для юридического агентства.

6) Разработать согласие субъекта персональных данных и журнал учета согласий субъек-тов персональных данных на обработку его персональных данных для администрации города.

7) Разработать согласие субъекта персональных данных и журнал учета согласий субъек-тов персональных данных на обработку его персональных данных для автотранспортного предприятия.

***Варианты повышенного уровня*:**

1) Разработать согласие субъекта персональных данных и журнал учета согласий субъ-ектов персональных данных на обработку его персональных данных для образовательной органи-зации высшего образования.

2) Разработать согласие субъекта персональных данных и журнал учета согласий субъ-ектов персональных данных на обработку его персональных данных для организации дополни-тельного образования.

3) Разработать согласие субъекта персональных данных и журнал учета согласий субъ-ектов персональных данных на обработку его персональных данных для организации дополни-тельного профессионального образования.

4) . Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для городской поликли-ники.

5) Разработать согласие субъекта персональных данных и журнал учета согласий субъ-ектов персональных данных на обработку его персональных данных для городской детской поликлиники.

6) Разработать согласие субъекта персональных данных и журнал учета согласий субъ-ектов персональных данных на обработку его персональных данных для министерства здравоохра-нения края.

7) Разработать согласие субъекта персональных данных и журнал учета согласий субъ-ектов персональных данных на обработку его персональных данных для городской больницы.

ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ЛАБОРАТОРНОЙ РАБОТЕ

по учебной дисциплине

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»

для студентов направления
подготовки 10.03.01 –
«Информационная безопасность»

Занятие № 4. Разработка уведомительных документов об обработке персо-нальных данных

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

13. Знать содержание и порядок разработки Уведомления об обработке персональных дан-ных.
14. Уметь разрабатывать уведомительные и организационно-распорядительные документы, необходимые для эффективной защиты персональных данных в соответствии с требовани-ями действующего законодательства.
15. Приобрести навыки разработки необходимых документов в интересах организации ра-бот по обеспечению безопасности ИСПДн.
16. Приобрести навыки анализа и обобщения полученных результатов.

СОДЕРЖАНИЕ ЗАНЯТИЯ

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связан-ные с разработкой Уведомления о намерении осуществлять обработку персональных данных, составлением Заявления об исключении сведений из реестра операторов, осуществляющих об-работку 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 дан-ных.

Проверка готовности студентов к занятию

4. По тестовым вопросам.

Содержание занятия

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 персо-нальных данных".

Образец формы уведомления об обработке (о намерении осуществлять обработку) пер-

Рекомендации

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

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

2. Уведомление оформляется на бланке Оператора (по **форме**, прилагаемой к настоя-щим 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 Рос-комнадзора).

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), осу-ществляющего 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) классификато-ров (**ОКВЭД**, ОКПО, **ОКОГУ**, ОКОП, **ОКФС**).

5. В **поле** "цель обработки персональных данных" указываются цели обработки персо-нальных 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 положе-ние, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту персональных данных).

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

6.3. Биометрические персональные данные (сведения, которые характеризуют физио-логические 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" указы-ваются 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 норма-
тивно-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, регулиру-ющие 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 состоя-ния" 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), отражает-ся только при наличии лицензии и (или) соответствующего пункта лицензионных условий.*

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

- неавтоматизированная обработка персональных данных;

- исключительно автоматизированная обработка персональных данных с передачей по-лученной 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 пер-сональных 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 информа-ции.

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, ответ-ственных за организацию обработки персональных данных, и номера их контактных теле-фонов, 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 утвер-ждении Порядка проведения классификации информационных систем персональных данных"; г) организационные и технические меры, применяемые для защиты персональных дан-ных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирова

ния, копирования, распространения персональных данных.

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

а) наименование, регистрационные номера и производителей используемых крип-тографических 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 дан-ных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра Федеральной службы безопас-ности Российской Федерации 21 февраля 2008 г. N 149/54-144.

11. В **поле** "сведения о наличии или об отсутствии трансграничной передачи персональ-ных данных" указываются сведения о наличии или об отсутствии трансграничной передачи пе-рсональных 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, уточ-нение (обновление, изменение), извлечение, использование, передачу (распространение, предо-ставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных дан-ных (фактическая дата начала обработки персональных данных).

14. В **поле** "срок или условие прекращения обработки персональных данных" указыва-ется конкретная дата (число, месяц, год) или основание (условие), наступление которого повле-чет прекращение обработки персональных данных.

*(1) Для юридических лиц с филиальной структурой указывается список субъектов Российской Федера-ции (с указанием кода субъекта - согласно **справочнику** "Коды регионов",

утвержденному **приказом** ФНС Рос-сии от 13.10.2006 года N САЭ-3-04/706@ "Об утверждении формы сведений о доходах физических лиц" (за-регистрированным Министерством юстиции Российской Федерации 17.11.2000 г., регистрационный номер 8507), на территории которых находятся филиалы (представительства) юридического лица и (или) где оператором произ-водится 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 поч-товый адреса (как юридического лица, так и его филиалов и представительств), где осуществляется непосред-ственная обработка персональных данных (все действия (операции) с персональными данными, включая сбор, си-стематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных). При этом, необходимо уточ-нить - 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 учреди-тельными 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 (Приложение 2) разработать и заполнить форму уведомления об обработке (о намерении осу-ществлять 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 (Приложение 2) составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных.

Методические пояснения и рекомендации по выполнению третьего вопроса

В ходе отработки третьего вопроса, обучаемые должны для заданных исходных данных (Приложение 2) составить заявление о предоставлении выписки из реестра операторов, осу-ществляющих обработку персональных данных.

Методические пояснения и рекомендации по выполнению четвертого вопроса

В ходе отработки четвертого вопроса обучаемые должны, для заданных исходных дан-ных (Приложение 2) 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:

9. Форму уведомления об обработке (о намерении осуществлять обработку) персональных данных.

10. Заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных.

11. Заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных.

12. Информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных

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:

Защита персональных данных в информационных системах: электрон-ный учебно-методический комплекс. Свидетельство о государственной регистра-ции 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: электрон-ный учебно-методический комплекс. Свидетельство о государственной регистра-ции 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 за-щите 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 пе-рсональных данных обработку персональных данных:

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

2) полученных оператором в связи с заключением договора, стороной которого является субъект персо-нальных 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 обра-батываемых 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 раскры-ваться 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 кото-рой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федераль-ными законами статус государственных автоматизированных информационных систем, а также в государствен-ные 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 обес-печению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных **законодательством** Российской Федерации о транспорт-ной 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 бумаж-ном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление долж-но 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 об-работки персональных данных;

7) описание мер, предусмотренных **статьями 18.1** и **19** настоящего Федерального закона, в том числе све-дения 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** настоя-щей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, со-держащиеся 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 персо-нальных 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 ста-тьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточ-нения 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 субъ-ектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Приложение №2

***Варианты базового уровня*:**

1) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для дошкольной образовательной организации.
2) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для дошкольной образовательной организации.
3) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для дошкольной образовательной организации.
4) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для дошкольной образовательной организации.
5) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для общеобразовательной организации.
6) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для общеобразовательной организации.
7) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для общеобразовательной организации.
8) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для общеобразовательной организа-ции.
9) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для профессиональной образовательной организации.
10) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для профессиональной образовательной организа-ции.
11) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для профессиональной образовательной организа-ции.
12) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для профессиональной образователь-ной организации.
13) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для агентства недвижимости.
14) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для агентства недвижимости.
15) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для агентства недвижимости.
16) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для агентства недвижимости.
17) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для юридического агентства.
18) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для юридического агентства.
19) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для юридического агентства.
20) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для юридического агентства.
21) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для администрации города.
22) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для администрации города.
23) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для администрации города.
24) Составить информационное письмо о внесении изменений в сведения в реестре опе-

раторов, осуществляющих обработку персональных данных для администрации города.

***Варианты повышенного уровня*:**

1) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для образовательной организации высшего образования.
2) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для образовательной организации высшего обра-зования.
3) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для образовательной организации высшего обра-зования.
4) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для образовательной организации высшего образования.
5) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для организации дополнительного образования.
6) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для организации дополнительного образования.
7) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для организации дополнительного образования.
8) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для организации дополнительного образования.
9) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для организации дополнительного профессионального образования.
10) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для организации дополнительного профессионального образования.
11) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для организации дополнительного профессионального образования.
12) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для организации дополнительного профессионального образования.
13) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для городской поликлиники.
14) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для городской поликлиники.
15) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для городской поликлиники.
16) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для городской поликлиники.
17) Разработать уведомление о намерении осуществлять обработку персональных дан-ных для министерства здравоохранения края.
18) Составить заявление об исключении сведений из реестра операторов, осуществляющих обработку персональных данных для министерства здравоохранения края. министерства здравоохранения края.
19) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных
20) Составить информационное письмо о внесении изменений в сведения в реестре опе-раторов, осуществляющих обработку персональных данных для министерства здравоохранения края.

ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ЛАБОРАТОРНОЙ РАБОТЕ

по учебной дисциплине

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»

для студентов направления подготовки
10.03.01 – «Информационная
безопасность»

Занятие № 5. Разработка частной модели угроз безопасности персональных данных при их обработке в информационной системе

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

17. Знать виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия.
18. Знать правовые нормативные акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.
19. Уметь формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности.
20. Уметь определять виды и формы информации, подверженной угрозам.
21. Приобрести навыки использования нормативных правовых документов в своей профессиональной деятельности.
22. Приобрести навыки анализа и обобщения полученных результатов.

СОДЕРЖАНИЕ ЗАНЯТИЯ

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, путем решения проблемных задач, связанные с разработкой частной модели угроз безопасности персональных данных при их обработке в информационной системе.

Проверка готовности студентов к занятию

5. По тестовым вопросам.

Содержание занятия

Основные теоретические сведения.

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исходных данных (Приложение 1) путем решения проблемных задач составить описание угроз безопасности персональных данных, обрабатываемых в ИСПДн.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса, обучаемые должны для заданных исходных данных (Приложение 1) путем решения проблемных задач выполнить определение актуальных угроз для информационной системы персональных данных и составить частную модель угроз.

Отчетность за занятие

Отчет по лабораторной работе должен содержать оформленную в соответствии с рекомендациями ФСТЭК частную модель угроз для заданных исходных данных (Приложение 1). с

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:

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

***Варианты базового уровня*:**

1) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для дошкольной образовательной организации.

2) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для дошкольной образовательной организации.

3) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для общеобразовательной организации.

4) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для общеобразовательной организации.

5) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для профессиональной образовательной органи-зации.

6) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для профессиональной образовательной организации.

7) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для агентства недвижимости.

8) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для агентства недвижимости.

9) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для юридического агентства.

10) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для юридического агентства.

11) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для администрации города.

12) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для администрации города.

13) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для автотранспортного предприятия.

14) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для автотранспортного предприятия.

***Варианты повышенного уровня*:**

1) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для образовательной организации высшего образования.

2) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для образовательной организации высшего образования.

3) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для организации дополнительного образования.

4) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для организации дополнительного образования.

5) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для организации дополнительного профессио-нального образования.

6) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для организации дополнительного профессионального обра-зования.

7) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для городской поликлиники.

8) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для городской поликлиники.

9) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для городской детской поликлиники.

10) Определить актуальные угрозы безопасности персональных данных в информацион-

ных системах персональных данных для городской детской поликлиники.

11) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для министерства здравоохранения края.

12) Определить актуальные угрозы безопасности персональных данных в информацион-ных системах персональных данных для министерства здравоохранения края.

ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ЛАБОРАТОРНОЙ РАБОТЕ

по учебной дисциплине

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»

для студентов направления подготовки
10.03.01 – «Информационная
безопасность»

Занятие № 6. Классификация автоматизированных и информационных систем персональных данных

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

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

СОДЕРЖАНИЕ ЗАНЯТИЯ

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить практические задания, связанные с классификацией автоматизированных систем и информационных систем персональных данных

Проверка готовности студентов к занятию

6. По тестовым вопросам.

Основные теоретические сведения

1. Классификация АС

1.1. Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

1.2. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

1.3. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

1.4. Основными этапами классификации АС являются:

разработка и анализ исходных данных;

выявление основных признаков АС, необходимых для классификации;

сравнение выявленных признаков АС с классифицируемыми;

присвоение АС соответствующего класса защиты информации от НСД.

1.5. Необходимыми исходными данными для проведения классификации конкретной АС являются:

перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;

матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

режим обработки данных в АС.

1.6. Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

1.7. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

наличие в АС информации различного уровня конфиденциальности;

уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС - коллективный или индивидуальный.

1.8. Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

1.9. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

2. Классификация информационных систем

3. Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

4. Проведение классификации информационных систем включает в себя следующие этапы:

сбор и анализ исходных данных по информационной системе;

присвоение информационной системе соответствующего класса и его документальное оформление.

5. При проведении классификации информационной системы учитываются следующие исходные данные:

категория обрабатываемых в информационной системе персональных данных - $X_{пд}$;

объем обрабатываемых персональных данных (количество субъектов персональных данных, персональных данные которых обрабатываются в информационной системе) – $X_{нпд}$;

заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;

структура информационной системы;

наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;

режим обработки персональных данных;

режим разграничения прав доступа пользователей информационной системы;

местонахождение технических средств информационной системы.

6. Определяются следующие категории обрабатываемых в информационной системе персональных данных ($X_{пд}$):

категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

категория 4 - обезличенные и (или) общедоступные персональные данные.

7. $X_{нпд}$ может принимать следующие значения:

1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

8. По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы - информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

9. По структуре информационные системы подразделяются:

на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);

на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

10. По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

11. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

12. По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

13. Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

14. По результатам анализа исходных данных типовой информационной си-стеме присваивается один из следующих классов:

класс 1 (К1) - информационные системы, для которых нарушение заданной

характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персо-нальных данных;

класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных дан-ных;

класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов пер-сональных данных;

класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

15. Класс типовой информационной системы определяется в соответствии с таблицей.

Хнпд Хпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

16. По результатам анализа исходных данных класс специальной информа-ционной системы определяется на основе модели угроз безопасности персональ-ных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопас-ности персональных данных при их обработке в информационных системах пер-сональных данных"

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданных исход-ных данных (Приложение 4) выполнить классификацию автоматизированной си-стемы и составить акт классификации автоматизированной системы. Форма акта классификации автоматизированной системы приведена в Приложении 1.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны, для заданных исход-ных данных (Приложение 4) выполнить классификацию информационной си-стемы и составить акт классификации информационной системы. Форма акта классификации информационной системы приведена в Приложении 2. Образец заполнения в Приложении 3.

Отчетность за занятие

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

13. Акт классификации автоматизированной системы.
14. Акт классификации информационной системы.

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. Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

2. Порядок проведения классификации информационных систем персональных данных. Приказ от 13 февраля 2008 года. Федеральная служба по техническому и экспортному контролю № 55. Федеральная служба безопасности Российской Федерации № 86. Министерство информационных технологий и связи Российской Федерации № 20.

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.

52

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.

***Варианты базового уровня*:**

1) Выполнить классификацию автоматизированных систем и составить акты классификации для дошкольной образовательной организации.
2) Выполнить классификацию информационных систем персональных данных и составить акты классификации для дошкольной образовательной организации.
3) Выполнить классификацию автоматизированных систем и составить акты классификации для общеобразовательной организации.
4) Выполнить классификацию информационных систем персональных данных и составить акты классификации для общеобразовательной организации.
5) Выполнить классификацию автоматизированных систем и составить акты классификации для профессиональной образовательной организации.
6) Выполнить классификацию информационных систем персональных данных и составить акты классификации для профессиональной образовательной организации.
7) Выполнить классификацию автоматизированных систем и составить акты классификации для агентства недвижимости.

8) Выполнить классификацию информационных систем персональных данных и составить акты классификации для агентства недвижимости.

9) Выполнить классификацию автоматизированных систем и составить акты классификации для юридического агентства.

10) Выполнить классификацию информационных систем персональных данных и составить акты классификации для юридического агентства.

11) Выполнить классификацию автоматизированных систем и составить акты классификации для администрации города.

12) Выполнить классификацию информационных систем персональных данных и составить акты классификации для администрации города.

13) Выполнить классификацию автоматизированных систем и составить акты классификации для автотранспортного предприятия.

14) Выполнить классификацию информационных систем персональных данных и составить акты классификации для автотранспортного предприятия.

***Варианты повышенного уровня*:**

1) Выполнить классификацию автоматизированных систем и составить акты классификации для образовательной организации высшего образования.

2) Выполнить классификацию информационных систем персональных данных и составить акты классификации для образовательной организации высшего образования.

3) Выполнить классификацию автоматизированных систем и составить акты классификации для организации дополнительного образования.

4) Выполнить классификацию информационных систем персональных данных и составить акты классификации для организации дополнительного образования.

5) Выполнить классификацию автоматизированных систем и составить акты классификации для городской поликлиники.

6) Выполнить классификацию информационных систем персональных данных и составить акты классификации для городской поликлиники.

7) Выполнить классификацию автоматизированных систем и составить акты классификации для городской детской поликлиники.

8) Выполнить классификацию информационных систем персональных данных и составить акты классификации для городской детской поликлиники.

9) Выполнить классификацию автоматизированных систем и составить акты классификации для министерства здравоохранения края.

10) Выполнить классификацию информационных систем персональных данных и составить акты классификации для министерства здравоохранения края.

ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ЛАБОРАТОРНОЙ РАБОТЕ

по учебной дисциплине

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»

для студентов направления подготовки
10.03.01 – «Информационная безопасность»

Занятие № 7. Разработка Концепции информационной безопасности

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

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

Вступительная часть

На сегодняшней лабораторной работе Вам предлагается выполнить задания, связанные с классификацией автоматизированных систем и информационных систем персональных данных

Проверка готовности студентов к занятию

7. 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 автоматизи-рованная 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 самостоя-тельных направлений, объединенных единым замыслом: защита информации от утечки по техническим каналам и защита информации в автоматизированных си-стемах от несанкционированного доступа.

Отчетность за занятие

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

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:

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

***Варианты базового уровня*:**

1) Разработать Концепцию информационной безопасности для дошкольной образовательной организации.
2) Разработать Концепцию информационной безопасности для общеобразовательной организации.
3) Разработать Концепцию информационной безопасности для профессиональной обра-зовательной организации.
4) Разработать Концепцию информационной безопасности для агентства недвижимости.
5) Разработать Концепцию информационной безопасности для юридического агентства.
6) Разработать Концепцию информационной безопасности для администрации города.
7) Разработать Концепцию информационной безопасности для автотранспортного предприятия.

***Варианты повышенного уровня*:**

1) Разработать Концепцию информационной безопасности для образовательной органи-зации высшего образования.
2) Разработать Концепцию информационной безопасности для организации дополнительного профессионального образования.
3) Разработать Концепцию информационной безопасности для городской поликлиники.
4) Разработать Концепцию информационной безопасности для городской детской поликлиники.
5) Разработать Концепцию информационной безопасности для министерства здравоохра-нения края.
6) Разработать Концепцию информационной безопасности для городской больницы.

ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ЛАБОРАТОРНОЙ РАБОТЕ

по учебной дисциплине

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»

для студентов направления подготовки
10.03.01 – «Информационная
безопасность»

Занятие № 8. Разработка Политики информационной безопасности

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

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

СОДЕРЖАНИЕ ЗАНЯТИЯ

Вступительная часть

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

Проверка готовности студентов к занятию

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 (Приложение 1) 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 (Приложение 1) 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.

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:

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.

***Варианты базового уровня*:**

8) Разработать Политику информационной безопасности для дошкольной образователь-ной организации.

9) Разработать Политику информационной безопасности для общеобразовательной организации.

10) Разработать Политику информационной безопасности для профессиональной образо-вательной организации.

11) Разработать Политику информационной безопасности для агентства недвижимости.

12) Разработать Политику информационной безопасности для юридического агентства.

13) Разработать Политику информационной безопасности для администрации города.

14) Разработать Политику информационной безопасности для автотранспортного предприятия.

***Варианты повышенного уровня*:**

7) Разработать Политику информационной безопасности для образовательной организа-ции высшего образования.

8) Разработать Политику информационной безопасности для организации дополнитель-ного профессионального образования.

9) Разработать Политику информационной безопасности для городской поликлиники.

10) Разработать Политику информационной безопасности для городской детской поликлиники.

11) Разработать Политику информационной безопасности для министерства здравоохранения края.

12) Разработать Политику информационной безопасности для городской больницы.

ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ЛАБОРАТОРНОЙ РАБОТЕ

по учебной дисциплине

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»

для студентов направления подготовки
10.03.01 – «Информационная безопасность»

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

Учебные цели занятия:

В результате настоящего занятия и последующей самостоятельной работы Вы должны:

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

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

8. 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 (Приложение 1) 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 (Приложение 1) 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 (Приложение 1) 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 (Приложение 1) 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.

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:

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

***Варианты базового уровня*:**

1) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных дошкольной образовательной организации.
2) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных общеобразовательной организации.
3) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных профессиональной образовательной организа-ции.
4) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных агентства недвижимости.
5) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных юридического агентства.
6) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных администрации города.
7) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных автотранспортного предприятия.

***Варианты повышенного уровня*:**

1) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных образовательной организации высшего образо-вания.
2) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных организации дополнительного образования.
3) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных организации дополнительного профессиональ-ного образования.
4) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных городской поликлиники.
5) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных городской детской поликлиники.
6) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных министерства здравоохранения края.
7) Разработать план мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных городской больницы.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Рекомендуемая литература

Основная литература:

1. Баймакова И.А., Новиков А.В., Рогачев А.И., Хыдыров А.Х. Обеспе-чение защиты персональных данных. –М.: Издательство "1С-Паблишинг", 2013. 215 с.

2. Защита персональных данных в информационных системах: Учебное пособие. – Ставрополь: Изд-во СГУ, 2014г. -272с.

14.1.2. Дополнительная литература:

1. Положение о методах и способах защиты информации в информаци-онных системах персональных данных. Утверждено приказом ФСТЭК России № 58 от 5 февраля 2015 г.
2. Федеральный закон Российской Федерации «Об электронной циф-ровой подписи». Принят Государственной Думой 13 декабря 2015 г. Одобрен Советом Федерации декабря 2016 года (в ред. Федерального закона от 08.11.2014
№ 258-ФЗ).
3. Положение об особенностях обработки персональных данных, осу-ществляемой без использования средств автоматизации. Утверждено постановле-нием Правительства РФ от 15 сентября 2013 г. № 687.
4. Порядок проведения классификации информационных систем персо-нальных данных. Приказ от 13 февраля 2008 года. Федеральная служба по техни-ческому и экспортному контролю № 55. Федеральная служба безопасности Рос-сийской Федерации № 86. Министерство информационных технологий и связи Российской Федерации № 20.
5. Автоматизированные системы. Защита от несанкционированного до-ступа к информации Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Утверждено решением предсе-дателя Государственной технической комиссии при Президенте Российской Фе-дерации от 30 марта 1992 г.
6. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 15408-1-2008. "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение
и общая модель" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. N 519-ст).
7. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 15408-2-2008 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. "Функцио-нальные требования безопасности" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. N 520-ст).
8. ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения без-опасности. Системы менеджмента информационной безопасности.
9. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от

несанкционированного до-ступа к информации. Руководящий документ. Утверждено решением председате-ля Государственной технической комиссии при Президенте Российской Федера-ции от 30 марта 1992 г.

10. Требования к материальным носителям биометрических персональ-ных данных и технологиям хранения таких данных вне информационных систем персональных данных. Утверждено постановлением Правительства РФ от 6 июля 2008 г. № 512.

Дополнительная литература:

1. 1. Аверченков, В. И.; Защита персональных данных в организации Электронный ресурс : Монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. - Брянск : Брянский государственный технический университет, 2012. - 124 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 5-89838-382-4
2. Административно-правовое регулирование правоохранительной деятельности: теория и практика : материалы Всерос. научно-практ. конференции, посвященной 35-летию со дня осн. Краснодар. ун-та МВД России (25 мая 2012 г.) : [в 2 т.] / М-во внутренних дел Рос. Федерации, Краснодар. ун-т, Всерос. науч.-исслед. ин-т, Т. 1. - Краснодар: КрУ МВД России, 2012. - 236 с. - ISBN 978-5-9266-0476-1

Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Защита персональных данных в информационных системах».
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Защита персональных данных в информационных системах».

Интернет-ресурсы:

1. www.intuit.ru – национальный открытый университет «ИНТУИТ»;
2. www.window.edu.ru –единое окно доступа к образовательным ресурсам;
3. www.citforum.ru – сервер информационных технологий.
4. http://biblioclub.ru
5. http://elibrary.ru/

Программное обеспечение:

1	Альт Рабочая станция 10
2	Альт Рабочая станция K
3	Альт «Сервер»
4	Пакет офисных программ - Р7-Офис

Материально-техническое обеспечение

1. Лабораторные и практические занятия проводятся в компьютерных классах, в которых установлено вышеперечисленное программное обеспечение.

2. Лекционный курс проводится в аудиториях, оснащенных проектором.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы
по дисциплине **«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ»**
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2025

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- написание докладов;
- подготовка к семинарам, практическим и лабораторным работам, их оформление;
- составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
- выполнение учебно-исследовательских работ, проектная деятельность;
- подготовка практических разработок и рекомендаций по решению проблемной ситуации;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;
- компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;
- выполнение курсовых работ (проектов) в рамках дисциплин;
- выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

2.Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование универсальных компетенций.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3.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-6(ИД-1 ИД-2ИД-3) ОПК-11(ИД-1 ИД-2ИД-3)	Самостоятельное изучение литературы	Собеседование	21,96	2,44	24,4
ОПК-6(ИД-1 ИД-2ИД-3) ОПК-11(ИД-1 ИД-2ИД-3)	Изучение лекций	Собеседование	2,88	0,32	3,2
ОПК-6(ИД-1 ИД-2ИД-3) ОПК-11(ИД-1 ИД-2ИД-3)	Подготовка к лабораторным занятиям	Собеседование	5,76	6,4	6,4
ОПК-6(ИД-1 ИД-2ИД-3) ОПК-11(ИД-1 ИД-2ИД-3)	Подготовка доклада	Доклад	9	1	10
Итого за 6 семестр			39,6	4,4	44

4.Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.
2. Выделите главное, составьте план.
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим занятиям

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа

данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение отвечать на вопросы для собеседования.

Вопросы для собеседования

1. Тема 2. Разработка приказов об организации работ по обеспечению безопасности персональных данных.

***Типовые задачи*:**
***Задания базового уровня*:**

1. Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для дошкольной образовательной организации.
2. Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для общеобразовательной организации.
3. Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для профессиональной образовательной организации.
4. Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для юридического агентства.
5. Разработать приказ о назначении ответственного за обработку персо-нальных данных для дошкольной образовательной организации.
6. Разработать приказ о назначении ответственного за обработку персо-нальных данных для общеобразовательной организации.
7. Разработать приказ о назначении ответственного за обработку персо-нальных данных для профессиональной образовательной организации.
8. Разработать приказ о назначении ответственного за обработку персо-нальных данных для агентства недвижимости.

9. Разработать приказ о назначении ответственного за обработку персо-нальных данных для юридического агентства.

10. Разработать приказ о назначении ответственного за обработку персо-нальных данных для администрации города.

11. Разработать приказ о назначении ответственного за обработку персо-нальных данных для автотранспортного предприятия.

12. Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для дошкольной образовательной организа-

ции.

13. Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для общеобразовательной организации.

14. Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для профессиональной образовательной организации.

15. Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для агентства недвижимости.

16. Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для юридического агентства.

17. Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для администрации города.

18. Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для автотранспортного предприятия.

***Задания повышенного уровня*:**

19) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для образовательной организации высшего образования.

20) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для организации дополнительного профессионального образования.

21) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для городской поликлиники.

22) Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для для городской детской поликлиники.

23) Разработать приказ о назначении ответственного за обработку персо-нальных данных для образовательной организации высшего образования.

24) Разработать приказ о назначении ответственного за обработку персо-нальных данных для организации дополнительного образования.

25) Разработать приказ о назначении ответственного за обработку персо-нальных данных для организации дополнительного профессионального образова-ния.

26) Разработать приказ о назначении ответственного за обработку персо-нальных данных для городской поликлиники.

27) Разработать приказ о назначении ответственного за обработку персо-нальных данных для городской детской поликлиники.

28) Разработать приказ о назначении ответственного за обработку персо-нальных данных для министерства здравоохранения края.

29) Разработать приказ о назначении ответственного за обработку персо-нальных данных для городской больницы.

30) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для образовательной организации высшего образования.

31) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для организации дополнительного образова-ния.

32) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для организации дополнительного профес-сионального образования.

33) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для городской поликлиники.

34) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для городской детской поликлиники.

35) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для министерства здравоохранения края.

36) Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для городской больницы.

2. Тема 5. Разработка перечней персональных данных, информацион-ных систем персональных данных и применяемых средств защиты информации.

***Типовые задачи*:**
***Задания базового уровня*:**

15) Разработать перечень персональных данных, обрабатываемых в дошкольной образовательной организации.

16) Разработать перечень персональных данных, обрабатываемых в общеобра-зовательной организации.

17) Разработать перечень персональных данных, обрабатываемых в професси-ональной образовательной организации.

18) Разработать перечень персональных данных, обрабатываемых в агентстве недвижимости.

19) Разработать перечень персональных данных, обрабатываемых в юриди-ческом агентстве.

20) Разработать перечень персональных данных, обрабатываемых в адми-нистрации города.

21) Разработать перечень персональных данных, обрабатываемых в автотранспортном предприятии.

22) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для дошкольной образовательной организации.

23) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для общеобразовательной организации.

24) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для профессиональной образовательной организации.

25) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для агентства недвижимости.

26) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для юридического агентства.

27) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для администрации города.

28) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для автотранспортного предприятия.

***Задания повышенного уровня*:**

15) Разработать перечень персональных данных, обрабатываемых в образовательной организации высшего образования.

16) Разработать перечень персональных данных, обрабатываемых в организа-ции дополнительного образования.

17) Разработать перечень персональных данных, обрабатываемых в организа-ции дополнительного профессионального образования.

18) Разработать перечень персональных данных, обрабатываемых в городской поликлинике.

19) Разработать перечень персональных данных, обрабатываемых в городской детской поликлинике.

20) Разработать перечень персональных данных, обрабатываемых в министерстве здравоохранения края.

21) Разработать перечень персональных данных, обрабатываемых в городской больнице.

22) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для образовательной организации высшего образования.

23) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для организации дополнительного образования.

24) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для организации дополнительного про-фессионального образования.

25) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для городской поликлиники.

26) Разработать информационных систем персональных данных и применяемых средств защиты информации для городской детской поликлиники.

27) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для министерства здравоохранения края.

28) Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для городской больницы.

3. Тема 6. Разработка согласия субъекта персональных данных на обработку его персональных данных.

***Типовые задачи*:**
***Задания базового уровня*:**

8) Разработать согласие субъекта персональных данных и журнал учета согла-

сий субъектов персональных данных на обработку его персональных данных для дошкольной образовательной организации.

9) Разработать согласие субъекта персональных данных и журнал учета согла-сий субъектов персональных данных на обработку его персональных данных для общеобразовательной организации.

10) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для профессиональной образовательной организации.

11) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для агентства недвижимости.

12) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для юридического агентства.

13) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для администрации города.

14) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для автотранспортного предприятия.

***Задания повышенного уровня*:**

8) Разработать согласие субъекта персональных данных и журнал учета согла-сий субъектов персональных данных на обработку его персональных данных для образовательной организации высшего образования.

9) Разработать согласие субъекта персональных данных и журнал учета согла-сий субъектов персональных данных на обработку его персональных данных для организации дополнительного образования.

10) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для организации дополнительного профессионального образования.

11) . Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для городской поликлиники.

12) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для городской детской поликлиники.

15) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для министерства здравоохранения края.

13) Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для городской больницы.

4. Тема 7. Разработка уведомительных документов об обработке персо-нальных данных.

***Типовые задачи*:**

***Задания базового уровня*:**

25) Разработать уведомление о намерении осуществлять обработку персональ-ных данных для дошкольной образовательной организации.

26) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для дошкольной образовательной организации.

27) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для дошкольной образователь-ной организации.

28) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для до-школьной образовательной организации.

29) Разработать уведомление о намерении осуществлять обработку персональ-ных данных для общеобразовательной организации.

30) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для общеобразовательной организа-ции.

31) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для общеобразовательной орга-низации.

32) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для обще-образовательной организации.

33) Разработать уведомление о намерении осуществлять обработку персональ-ных данных для профессиональной образовательной организации.

34) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для профессиональной образо-вательной организации.

35) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для профессиональной образо-вательной организации.

36) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для профес-сиональной образовательной организации.

37) Разработать уведомление о намерении осуществлять обработку персональ-ных данных для агентства недвижимости.

38) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для агентства недвижимости.

39) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для агентства недвижимости.

40) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для агент-ства недвижимости.

41) Разработать уведомление о намерении осуществлять обработку персональных данных для юридического агентства.

42) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для юридического агентства.

43) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для юридического агентства.

44) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для юриди-ческого агентства.

45) Разработать уведомление о намерении осуществлять обработку персональ-ных данных для администрации города.

46) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для администрации города.

47) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для администрации города.

48) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для адми-нистрации города.

***Задания повышенного уровня*:**

21) Разработать уведомление о намерении осуществлять обработку персональ-ных данных для образовательной организации высшего образования.

22) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для образовательной организации высшего образования.

23) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для образовательной организа-ции высшего образования.

24) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для образо-вательной организации высшего образования.

25) Разработать уведомление о намерении осуществлять обработку персо-нальных данных для организации дополнительного образования.

26) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для организации дополнительного образования.

27) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для организации дополнитель-ного образования.

28) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для органи-зации дополнительного образования.

29) Разработать уведомление о намерении осуществлять обработку персо-нальных данных для организации дополнительного профессионального образова-ния.

30) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для организации дополнительного профессионального образования.

31) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для организации дополнитель-ного профессионального образования.

32) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для органи-зации дополнительного профессионального образования.

33) Разработать уведомление о намерении осуществлять обработку персональ-ных данных для городской поликлиники.

34) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для городской поликлиники.

35) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для городской поликлиники.

36) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для город-ской поликлиники.

37) Разработать уведомление о намерении осуществлять обработку персональ-ных данных для министерства здравоохранения края.

38) Составить заявление об исключении сведений из реестра операторов, осу-ществляющих обработку персональных данных для министерства здравоохране-ния края. министерства здравоохранения края.

39) Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных

40) Составить информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных для ми-нистерства здравоохранения края.

5. Тема 10. Разработка частной модели угроз безопасности персональных данных при их обработке в информационной системе.

***Типовые задачи*:**
***Задания базового уровня*:**

15) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для дошкольной обра-зовательной организации.

16) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для дошкольной образовательной организации.

17) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для общеобразователь-ной организации.

18) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для общеобразовательной орга-низации.

19) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для профессиональной образовательной организации.

20) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для профессиональной образо-вательной организации.

21) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для агентства не-движимости.

22) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для агентства недвижимости.

23) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для юридического агентства.

24) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для юридического агентства.

25) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для администрации го-рода.

26) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для администрации города.

27) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для автотранспортного предприятия.

28) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для автотранспортного предприя-тия.

***Задания повышенного уровня*:**

13) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для образовательной организации высшего образования.

14) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для образовательной организа-ции высшего образования.

15) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для организации допол-нительного образования.

16) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для организации дополнитель-ного образования.

17) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для организации до-полнительного профессионального образования.

18) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для организации дополнитель-ного профессионального образования.

19) Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для городской поликлиники. Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для городской поликлиники.

20) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для городской детской поликлиники.

21) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для городской детской поликли-ники.

22) Разработать перечень угроз безопасности персональных данных при их об-работке в информационных системах персональных данных для министерства здравоохранения края.

23) Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для министерства здравоохране-ния края.

6. Тема 11. Классификация автоматизированных и информационных си-стем персональных данных.

***Типовые задачи*:**
***Задания базового уровня*:**

15) Выполнить классификацию автоматизированных систем и составить акты классификации для дошкольной образовательной организации.

16) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для дошкольной образовательной организа-ции.

17) Выполнить классификацию автоматизированных систем и составить акты классификации для общеобразовательной организации.

18) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для общеобразовательной организации.

19) Выполнить классификацию автоматизированных систем и составить акты классификации для профессиональной образовательной организации.

20) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для профессиональной образовательной орга-низации.

21) Выполнить классификацию автоматизированных систем и составить акты классификации для агентства недвижимости.

22) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для агентства недвижимости.

23) Выполнить классификацию автоматизированных систем и составить акты классификации для юридического агентства.

24) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для юридического агентства.

25) Выполнить классификацию автоматизированных систем и составить акты классификации для администрации города.

26) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для администрации города.

27) Выполнить классификацию автоматизированных систем и составить акты классификации для автотранспортного предприятия.

28) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для автотранспортного предприятия.

***Задания повышенного уровня*:**

11) Выполнить классификацию автоматизированных систем и составить акты классификации для образовательной организации высшего образования.

12) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для образовательной организации высшего образования.

13) Выполнить классификацию автоматизированных систем и составить акты классификации для организации дополнительного образования.

14) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для организации дополнительного образова-ния.

15) Выполнить классификацию автоматизированных систем и составить акты классификации для городской поликлиники.

16) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для городской поликлиники.

17) Выполнить классификацию автоматизированных систем и составить акты классификации для городской детской поликлиники.

18) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для городской детской поликлиники.

19) Выполнить классификацию автоматизированных систем и составить акты классификации для министерства здравоохранения края.

20) Выполнить классификацию информационных систем персональных дан-ных и составить акты классификации для министерства здравоохранения края.

7. Тема 13. Разработка Концепции информационной безопасности. *Типовые задачи*:

***Задания базового уровня*:**

15) Разработать Концепцию информационной безопасности для дошкольной

образовательной организации.

16) Разработать Концепцию информационной безопасности для общеобразо-вательной организации.

17) Разработать Концепцию информационной безопасности для профессио-нальной образовательной организации.

18) Разработать Концепцию информационной безопасности для агентства не-движимости.

19) Разработать Концепцию информационной безопасности для юридиче-ского агентства.

20) Разработать Концепцию информационной безопасности для администра-ции города.

автотранспортного предприятия.

***Задания повышенного уровня*:**

13) Разработать Концепцию информационной безопасности для образователь-ной организации высшего образования.

14) Разработать Концепцию информационной безопасности для организации дополнительного профессионального образования.

15) Разработать Концепцию информационной безопасности для городской поликлиники.

16) Разработать Концепцию информационной безопасности для городской детской поликлиники.

17) Разработать Концепцию информационной безопасности для министерства здравоохранения края.

18) Разработать Концепцию информационной безопасности для городской больницы.

8. Тема 14. Разработка Политики информационной безопасности. *Типовые задачи*:

***Задания базового уровня*:**

1. Разработать Политику информационной безопасности для дошкольной

образовательной организации.

2. Разработать Политику информационной безопасности для общеобразо-вательной организации.

3. Разработать Политику информационной безопасности для профессиональ-ной образовательной организации.

4. Разработать Политику информационной безопасности для агентства не-движимости.

5. Разработать Политику информационной безопасности для юридического агентства.

6. Разработать Политику информационной безопасности для администрации

города.

7. Разработать Политику информационной безопасности для автотранспорт-ного предприятия.

***Задания повышенного уровня*:**

1. Разработать Политику информационной безопасности для образователь-ной организации высшего образования.
2. Разработать Политику информационной безопасности для организации до-полнительного профессионального образования.
3. Разработать Политику информационной безопасности для городской поликлиники.
4. Разработать Политику информационной безопасности для городской дет-ской поликлиники.
5. Разработать Политику информационной безопасности для министерства здравоохранения края.
6. Разработать Политику информационной безопасности для городской больницы.

9. Тема 17. Разработка плана мероприятий по обеспечению защиты пер-сональных данных в информационных системах персональных данных.

***Типовые задачи*:**
***Задания базового уровня*:**

8) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных дошкольной образователь-ной организации.

9) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных общеобразовательной организации.

10) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных профессиональной образо-вательной организации.

11) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных агентства недвижимости.

12) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных юридического агентства.

13) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных администрации города.

14) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных автотранспортного предприятия.

***Задания повышенного уровня*:**

8) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных образовательной организа-ции высшего образования.

9) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных организации дополнитель-ного образования.

10) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных организации дополнитель-ного профессионального образования.

11) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных городской поликлиники.

12) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных городской детской поликлиники.

13) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных министерства здравоохра-нения края.

14) Разработать план мероприятий по обеспечению защиты персональных дан-ных в информационных системах персональных данных городской больницы.

10. Тема 18. Разработка положения по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн

***Типовые задачи*:**

***Задания базового уровня*:**

9) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных дошкольной образовательной организации.

10) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных общеобразовательной организации.

11) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных профессиональной образовательной организации.

12) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных агентства недвижимости.

13) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных юридического агентства.

14) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных администрации города.

15) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных автотранспортного предприятия.

16) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных гостиничного комплекса.

17) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных автотехцентра.

***Задания повышенного уровня*:**

15) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных образовательной организации высшего образования.

16) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных организации дополнительного образования.

17) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных организации дополнительного профессиональ-ного образования.

18) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных системах персональных данных городской поликлиники.

19) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных городской детской поликлиники.

20) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных министерства здравоохранения края.

21) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных городской больницы.

22) Разработать положение по организации и проведению работ по обеспече-нию безопасности персональных данных при их обработке в информационных си-стемах персональных данных стоматологической поликлиники.

11. Тема 21. Разработка требований к информационной системе по обес-печению безопасности персональных данных.

***Типовые задачи*:**
***Задания базового уровня*:**

9) Разработать требования к мерам защиты информации, содержащейся в информационной системе дошкольной образовательной организации.

10) Разработать требования к мерам защиты информации, содержащейся в информационной системе общеобразовательной организации.

11) Разработать требования к мерам защиты информации, содержащейся в информационной системе профессиональной образовательной организации.

12) Разработать требования к мерам защиты информации, содержащейся в информационной системе агентства недвижимости.

13) Разработать требования к мерам защиты информации, содержащейся в информационной системе юридического агентства.

14) Разработать требования к мерам защиты информации, содержащейся в информационной системе администрации города.

15) Разработать требования к мерам защиты информации, содержащейся в информационной системе автотранспортного предприятия.

16) Разработать требования к мерам защиты информации, содержащейся в информационной системе гостиничного комплекса.

***Задания повышенного уровня*:**

1. Разработать требования к мерам защиты информации, содержащейся в информационной системе образовательной организации высшего образования.
2. Разработать требования к мерам защиты информации, содержащейся в информационной системе организации дополнительного образования.
3. Разработать требования к мерам защиты информации, содержащейся в информационной системе организации дополнительного профессионального обра-зования.
4. Разработать требования к мерам защиты информации, содержащейся в информационной системе городской поликлиники.
5. Разработать требования к мерам защиты информации, содержащейся в информационной системе городской детской поликлиники.
6. Разработать требования к мерам защиты информации, содержащейся в информационной системе министерства здравоохранения края.

12. Тема 22. Разработка инструкций по защите персональных данных в информационных системах.

***Типовые задачи*:**
***Задания базового уровня*:**

19) Разработать инструкцию администратора информационной системы пер-сональных данных для дошкольной образовательной организации.

20) Разработать инструкцию пользователя информационной системы персо-нальных данных для дошкольной образовательной организации.

21) Разработать инструкцию администратора безопасности при использова-нии ресурсов объекта вычислительной техники для дошкольной образовательной организации.

22) Разработать инструкцию администратора информационной системы пер-сональных данных профессиональной образовательной организации.

23) Разработать инструкцию пользователя информационной системы персо-нальных данных профессиональной образовательной организации.

24) Разработать инструкцию администратора безопасности при использова-нии ресурсов объекта вычислительной техники профессиональной образователь-ной организации.

25) Разработать инструкцию администратора информационной системы пер-сональных данных агентства недвижимости.

26) Разработать инструкцию пользователя информационной системы персо-нальных данных агентства недвижимости.

27) Разработать инструкцию администратора безопасности при использова-нии ресурсов объекта вычислительной техники агентства недвижимости.

28) Разработать инструкцию администратора информационной системы пер-сональных данных юридического агентства.

29) Разработать инструкцию пользователя информационной системы персо-нальных данных юридического агентства.

30) Разработать инструкцию администратора безопасности при использова-нии ресурсов объекта вычислительной техники юридического агентства.

31) Разработать инструкцию администратора информационной системы пер-сональных данных администрации города.

32) Разработать инструкцию пользователя информационной системы персо-нальных данных администрации города.

33) Разработать инструкцию администратора безопасности при использова-нии ресурсов объекта вычислительной техники администрации города.

34) Разработать инструкцию администратора информационной системы пер-сональных данных гостиничного комплекса.

35) Разработать инструкцию пользователя информационной системы персональных данных гостиничного комплекса.

36) Разработать инструкцию администратора безопасности при использова-нии ресурсов объекта вычислительной техники гостиничного комплекса.

***Задания повышенного уровня*:**

9) Разработать инструкцию пользователя по обеспечению безопасности обра-ботки персональных данных при возникновении внештатных ситуаций образо-вательной организации высшего образования.

10) Разработать инструкцию ответственного за организацию резервирования

и восстановления программного обеспечения и баз персональных данных образо-вательной организации высшего образования.

11) Разработать инструкцию пользователя по обеспечению безопасности об-работки персональных данных при возникновении внештатных ситуаций организа-ции дополнительного профессионального образования.

12) Разработать инструкцию ответственного за организацию резервирования

и восстановления программного обеспечения и баз персональных данных организа-ции дополнительного профессионального образования.

13) Разработать инструкцию пользователя по обеспечению безопасности об-работки персональных данных при возникновении внештатных ситуаций городской поликлиники.

14) Разработать инструкцию ответственного за организацию резервирования

и восстановления программного обеспечения и баз персональных данных город-ской поликлиники.

15) Разработать инструкцию пользователя по обеспечению безопасности об-работки персональных данных при возникновении внештатных ситуаций ми-нистерства здравоохранения края.

16) Разработать инструкцию ответственного за организацию резервирования

и восстановления программного обеспечения и баз персональных данных ми-нистерства здравоохранения края.

13. Тема 24. Аттестация информационных систем персональных данных по требованиям безопасности информации. *Типовые задачи*:

***Задания базового уровня*:**

10) Подготовить заявки на аттестацию информационных систем персональ-ных данных дошкольной образовательной организации.

11) Подготовить заявки на аттестацию информационных систем персональ-ных данных общеобразовательной организации.

12) Подготовить заявки на аттестацию информационных систем персональ-ных данных профессиональной образовательной организации.

13) Подготовить заявки на аттестацию информационных систем персональ-ных данных агентства недвижимости.

14) Подготовить заявки на аттестацию информационных систем персональ-ных данных юридического агентства.

15) Подготовить заявки на аттестацию информационных систем персональ-

16) Подготовить заявки на аттестацию информационных систем персональ-ных данных автотранспортного предприятия.

17) Подготовить заявки на аттестацию информационных систем персональ-ных данных гостиничного комплекса.

18) Подготовить заявки на аттестацию информационных систем персональ-ных данных автотехцентра.

***Задания повышенного уровня*:**

10) Подготовить заявки на аттестацию информационных систем персональ-ных данных образовательной организации высшего образования.

11) Подготовить заявки на аттестацию информационных систем персональ-ных данных организации дополнительного профессионального образования.

12) Подготовить заявки на аттестацию информационных систем персональ-ных данных городской поликлиники.

13) Подготовить заявки на аттестацию информационных систем персональ-ных данных городской детской поликлиники.

14) Подготовить заявки на аттестацию информационных систем персональ-ных данных министерства здравоохранения края.

15) Подготовить заявки на аттестацию информационных систем персональ-ных данных городской больницы.

16) Подготовить необходимую организационно-распорядительную документацию на аттестацию информационных систем персональных данных го-родской больницы.

17) Подготовить необходимую организационно-распорядительную документацию на аттестацию информационных систем персональных данных образовательной организации высшего образования.

18) Подготовить необходимую организационно-распорядительную документацию на аттестацию информационных систем персональных данных го-родской детской поликлиники.

4.2 Вопросы для собеседования по практическим занятиям По дисциплине «защита персональных данных в информационных си-стемах»

1. Актуальность проблемы защиты персональных данных в информацион-ных системах
2. Основные понятия информационной безопасности
3. Международное право в области защиты ПДн
4. Общие положения закона
5. Принципы и условия обработки персональных данных
6. Категории персональных данных
7. Права субъекта персональных данных
8. Основные принципы моделирования угроз с использованием методиче-ских документов ФСТЭК и ФСБ
9. Угрозы информационной безопасности
10. Анализ сетевого трафика
11. Сканирование сети
12. Угроза выявления пароля
13. Подмена доверенного объекта сети и передача по каналам связи со-общений от его имени с присвоением его прав доступа
14. Навязывание ложного маршрута сети
15. Общие принципы
16. Методология формирования модели угроз верхнего уровня
17. Методология формирования детализированной модели угроз
18. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных
19. Оценка обстановки и формирование замысла защиты персональных данных
20. Мероприятия от утечки по техническим каналам утечки информации
21. Методы и способы защиты персональных данных от НСД
22. Основные этапы при построении системы защиты персональных дан-

ных

23. Комплекс организационных и технических мероприятий в рамках СЗПДн
24. Общая характеристика подсистем
25. Подсистема антивирусной защиты

26. Подсистема обнаружения вторжений
27. Сертификация средств защиты персональных данных
28. Требования законодательства к средствам защиты персональных данных
29. Требования законодательства к ИСПДн
30. Угроза выявления пароля в информационной системе

4.4. Методические рекомендации по написанию научных текстов (докладов, рефератов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление.

Структура доклада:

Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

Приложение (при необходимости).

Требования к оформлению:

текст с одной стороны листа;

- шрифт Times New Roman;
- кегль шрифта 14;
- межстрочное расстояние 1,5;
- поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
- реферат должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Доклад оценивается по следующим критериям: соблюдение требований к его оформлению; необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации; умение студента свободно излагать основные идеи, отраженные в докладе; способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

4.5. Методические рекомендации по подготовке к зачетам

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра

обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет (Sзач) при различных рейтинговых баллах по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре (*Rсем*)	**Количество баллов за зачет (*S*зач)**
$50 \leq Rсем \leq 60$	**40**
$39 \leq Rсем < 50$	**35**
$33 \leq Rсем < 39$	**27**
***Rсем*< 33**	**0**

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка выполнения доклада и его презентации.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Астахова А.В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД [Электронный ресурс]: учебное пособие/ Астахова А.В.— Электрон. текстовые данные.— СПб.: Троицкий мост, 2014.— 216 c.— Режим доступа: http://www.iprbookshop.ru/40860.— ЭБС «IPRbooks», по паролю

2. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - М. : Издательский дом Высшей школы экономики, 2015. - 574 с. : ил. - Библ. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=440285.

Дополнительная литература:

1. Аверченков, В. И.; Защита персональных данных в организации Электронный ресурс : Монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. - Брянск : Брянский государственный технический университет, 2012. - 124 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 5-89838-382-4

2. Административно-правовое регулирование правоохранительной деятельности: теория и практика : материалы Всерос. научно-практ. конференции, посвященной 35-летию со дня осн. Краснодар. ун-та МВД России (25 мая 2012 г.) : [в 2 т.] / М-во внутренних дел Рос. Федерации, Краснодар. ун-т, Всерос. науч.-исслед. ин-т, Т. 1. - Краснодар: КрУ МВД России, 2012. - 236 с. - ISBN 978-5-9266-0476-1

Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Защита персональных данных в информационных системах».

2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Защита персональных данных в

информационных системах».

Интернет-ресурсы:

1. www.intuit.ru – национальный открытый университет «ИНТУИТ»;
2. www.window.edu.ru –единое окно доступа к образовательным ресурсам;
3. www.citforum.ru – сервер информационных технологий.
4. http://biblioclub.ru
5. http://elibrary.ru/

Программное обеспечение:

1	Альт Рабочая станция 10
2	Альт Рабочая станция K
3	Альт «Сервер»
4	Пакет офисных программ - Р7-Офис

1. Защита персональных данных в информационных системах: электрон-ный учебно-методический комплекс. Свидетельство о государственной регистра-ции базы данных №2012620964. Зарегистрировано 19.09.2012. Заявка №2012620799 от 26.07.2012.
2. 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;
3. Программа тестового контроля «Айрен».

Материально-техническое обеспечение

1. Лабораторные и практические занятия проводятся в компьютерных классах, в которых установлено вышеперечисленное программное обеспечение.
2. Лекционный курс проводится в аудиториях, оснащенных проектором.