ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «РОСТОВСКИЙ ЦЕНТР ПОВЫШЕНИЯ КВАЛИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ»

«УТВЕРЖДАЮ»
Директор
ЧОУ ДПО «РЦПК ИТС»

_____ С.Д. Мармоленко

05 мая 2022г.

Программа дополнительного профессионального образования

Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

Ростов-на-Дону

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая программа дополнительного образования Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных (далее - программа) разработана Частным образовательным учреждением дополнительного профессионального образования «Ростовский центр повышения квалификации в области информационных технологий и связи» (ЧОУ ДПО «РЦПК») с учётом требований: Федерального закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», «Доктрины информационной безопасности Российской Федерации», утвержденной Указом Президента РФ № 646 от 05.12.2016 г., Федерального закона от 28.12.2010 г. № 390-ФЗ «О безопасности», Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», приказа Минобрнауки Российской Федерации от 05.12.2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности», «Методических рекомендаций по разработке программ профессиональной переподготовке и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры. противодействия иностранным техническим разведкам и технической защите информации», утвержденных ФСТЭК России 04.04.2015 г. и примерной программы повышения квалификации, разработанной Минтруда Российской Федерации (письмо Минтруда РФ от 09.09.2013 г.).
Основой для разработки программы являются: Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 18.02.2013 г. № 17, «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18.02.2013 г. № 21, а также документы ФСТЭК России и ФСБ России, регламентирующие вопросы обеспечения безопасности персональных данных: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» и «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».

2 ЦЕЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ

Целью обучения по программе является освоение специалистами актуальных

изменений в вопросах профессиональной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах в условиях существования угроз безопасности информации.

Обучающиеся по программе повышения квалификации готовятся к осуществлению следующих профессиональной видов деятельности: организационно-управленческая и проектная.

Объектами профессиональной деятельности обучающихся являются:

объекты информатизации (ОИ), включающие автоматизированные (информационные) системы (ИС, АИС) различного уровня и назначения, средства и системы обработки информации и средства их обеспечения, а также помещения, предназначенные для ведения переговоров, содержащих ПДн (защищаемые помещения (ЗП));

технические каналы утечки информации (ТКУИ) на ОИ и угрозы безопасности информации в ИСПДн, на автоматизированных рабочих местах (АРМ) и в ЗП;

система нормативных правовых актов, методических документов, национальных и международных стандартов в области ТЗИ, содержащей ПДн;

способы и средства, используемые для обеспечения защиты ПДн.

Поставленная цель достигается решением следующих задач:

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

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

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

Задачами профессиональной деятельности обучающихся являются:

а) в организационно-управленческой деятельности:

планирование деятельности по обеспечению защиты ПДн (разработка документов, регламентирующих в организации политики (правила, процедуры) по обеспечению технической защиты ПДн);

организация внедрения и применения политик (правил, процедур) по обеспечению технической защиты ПДн в организации;

проведение контроля (мониторинга) и анализа применения политик (правил, процедур) по обеспечению технической защиты ПДн в организации;

поддержка и совершенствование деятельности по обеспечению технической защиты ПДн в организации;

б) в проектной деятельности:

определение ТКУИ на ОИ и угроз безопасности информации в ИСПДн, на АРМ и в ЗП;

формирование требований к обеспечению технической защиты ПДн на ОИ (формирование требований к системе защиты информации ОИ);

разработка способов и средств для обеспечения технической защиты ПДн на ОИ (разработка системы защиты информации (СЗИ));

внедрение способов и средств для обеспечения технической защиты ПДн на ОИ (внедрение СЗИ ОИ).

3 ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПОСТУПАЮЩЕГО НА ОБУЧЕНИЕ

Уровень образования лица, поступающего на обучение, - среднее/высшее образование по специальностям в области информационной безопасности, или профессиональная переподготовка для выполнения нового вида профессиональной деятельности - ТЗИ, или иное высшее образование и стаж работы в области ТЗИ.

4 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Знания, полученные в ходе изучения блока курсов по защите персональных данных, призваны помочь специалистам различных категорий, от руководителей предприятий и их структурных подразделений до лиц, связанных с организацией обработки персональных данных и непосредственно отвечающих за защиту информации, и ведение делопроизводства.

Процесс освоения слушателями данной программы направлен на совершенствование и (или) получение следующих компетенций:

- правовые и организационные основы защиты информации ограниченного доступа
- угрозы безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа
- мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- реализовывать типовые модели защищенных информационных систем обработки персональных данных.

Слушатель по итогам обучение должен:

а) знать:

- Основные понятия и определения информационной безопасности;
- Нормативные документы в области информационной безопасности;
- Правовые аспекты обеспечения защиты ПДн;
- Возможные риски организаций и их последствия при утечке ПДн;
- Структура и направления деятельности системы ТЗИ.
- Основные принципы обеспечения безопасности персональных данных при их обработке;
- Основные требования и рекомендации по защите персональных;
- Оценка эффективности защиты персональных данных;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств;
- Анализ средств обеспечения безопасности персональных данных от физического доступа;
- Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов;
- Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных;
- Комплекс организационных и технических мероприятий;
- Пассивные и активные средства защиты персональных данных.

б) владеть навыками:

- Умение классифицировать угрозы безопасности в информационной системе;
- Умение определять технические каналы утечки информации;
- Умение составлять базовую модель угроз безопасности ПДн.
- Разработка нормативной документации необходимой для обработки ПДн в информационных системах;
- Разработка организационно-распорядительной документации;
- Планирование работ по контролю состояния защиты персональных данных.

5 ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Лабораторные базы ЧОУ ДПО «РЦПК» оснащены современным оборудованием, стендами, приборами, позволяющими изучать и исследовать аппаратуру, программно-аппаратные комплексы, специальное программное обеспечение, процессы обработки информации и технические СрЗИ в соответствии с реализуемой программой повышения квалификации.

Компьютерные классы с оборудованными АРМ для проведения учебных занятий, на которых присутствует речевая и видовая информация ОД1, аттестованы по требованиям безопасности информации. Количество АРМ в ЗП определяется из расчета одно рабочее место на одного обучающегося.

ЧОУ ДПО «РЦПК» имеет необходимый комплект лицензионного программного обеспечения и сертифицированных программных и аппаратных СрЗИ3.

Формирование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Программа повышения квалификации предусматривает проведение занятий в соответствии с целевыми установками программы, которые обеспечивают требуемый уровень усвоения учебного материала. Знания приобретаются путем прослушивания лекций в формате вебинаров и практической работы.

Помимо учебной литературы включены официальные, справочно-библиографические и специализированные периодические издания, в том числе правовые нормативные акты и нормативные методические документы (НМД) в области информационной безопасности.

Для обучающихся обеспечивается доступ к современным профессиональным базам данных, информационным справочным и поисковым системам по тематике информационной безопасности.

Изменения и дополнения вносятся в программу по мере необходимости в целях ее актуализации в случае изменений законодательной базы и осуществляются по распоряжению руководителя ЧОУ ДПО «РЦПК».

Создание блока курсов по защите персональных данных продиктовано необходимостью решения задач, поставленных перед всеми российскими компаниями и организациями в связи с принятием Федерального закона «О персональных данных». Главная цель обучения защите персональных данных – дать знания руководителям и специалистам организаций-операторов персональных данных (ПДн), необходимые для

соблюдения в организациях порядка обработки и защиты ПДн в соответствии с требованиями российского законодательства.

Особое внимание в программе курса уделено вопросам технической реализации требований законодательства по защите персональных данных. В ходе обучения по защите персональных данных слушатели получат прикладные знания о важных аспектах регулирования отношений между работником и работодателем. В рамках предлагаемых программ также рассматриваются вопросы государственного контроля и надзора в области защиты персональных данных, прав и обязанностей представителей надзорных органов и оператора при проведении проверок в соответствии с требованиями российских законов. Приводится перечень практических мер, которые должны быть реализованы предприятиями, организациями, физическими лицами, осуществляющими обработку персональных данных. Знания, полученные в ходе изучения блока курсов по защите персональных данных, призваны помочь специалистам различных категорий, от руководителей предприятий и их структурных подразделений до лиц, связанных с организацией обработки персональных данных и непосредственно отвечающих за защиту информации, и ведение делопроизводства.

В процессе изучения данной программы необходимо использовать действующие законодательные акты в области защиты персональных данных в информационных системах обработки персональных данных, технической защиты информации, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы ФСТЭК России, ФСБ России и Министерства информационных технологий и связи России, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите персональных данных в информационных системах обработки персональных данных. Часть лекций может излагаться проблемным методом с привлечением слушателей для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Для проведения практического занятия необходимо использовать методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями информационных систем персональных данных, и наборов конкретных действий, существенных для определённых категорий обучаемых объединенных в соответствующую подгруппу.

С целью текущего контроля знаний в ходе практических занятий должны проводиться выборочные опросы и (или) использоваться различные приёмы тестирования.

Научно-педагогические работники, осуществляющие преподавание даннойпрограммы, имеют образование, соответствующее профилю преподаваемой дисциплины(отдельных модулей), конкретный опыт реализации разработок и иной формыпрактической деятельности в области информационной безопасности.

6 ФОРМЫ АТТЕСТАЦИИ И ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Контрольно-проверочные занятия включают входной контроль. Освоение обучающимися программы повышения квалификации завершается итоговой аттестацией в форме теста.

Перечень вопросов (тестов), используемых для проведения итоговой аттестации, полностью соответствует и отражает содержание лекционных и практических занятий по всем темам программы.

Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается директором ЧОУ ДПО «РЦПК».

Входной контроль охватывает всех обучаемых и проводится в форме тестирования. Целью его является определение уровня знаний обучаемых для корректировки и адаптации учебного процесса под конкретные потребности обучаемых, с учётом уровня освоения учебного материала, изученного ими ранее в рамках получения базового образования или на курсах повышения квалификации.

Оценочные средства, включают тесты, позволяющие оценить знания, умения и уровень приобретенных компетенций. В ходе тестирования используются современные способы и формы оценивания обучающихся.

Основными критериями оценки усвоения слушателями учебного материала при проведении текущего контроля в ходе практических занятий являются: полнота ответов на поставленные вопросы; правильность выполнения действий при отработке практических вопросов эксплуатации изучаемых средств защиты информации.

Конкретные формы и процедуры входного контроля знаний по каждой теме разрабатываются учебным заведением самостоятельно и доводятся до сведения обучающихся в течение первого дня обучения.

Для проведения контрольно-проверочных занятий образовательным учреждением разработаны тестовые задания, включающие вопросы для тестирования (не менее 25 вопросов для итогового теста).

Для успешного прохождения тестирования и получения оценки «зачтено» необходимо набрать не менее 70 баллов.

Ответ на вопрос считается правильным, если он является полным.

Тест включает в себя вопросы, направленные как на контроль знаний, так и на проверку полученных навыков работы. Во время тестирования запрещается пользоваться какой-либо литературой.

При проведении тестирования с использованием электронных форм контроля и оценки у каждого слушателя есть три попытки на прохождение тестирования. Время на одну попытку - 40 минут. По окончанию попытки слушатель может видеть результаты теста и полученные баллы. Также имеется возможность просмотра отчета, показывающего ошибки при прохождении теста. Оценка выставляется по последней попытке.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей образовательной программы создаются фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить знания, умения и уровень приобретенных компетенций. Фонды оценочных средств разрабатываются и утверждаются образовательным учреждением самостоятельно.

Лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдаются удостоверения о повышении квалификации.

Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы повышения квалификации и (или) отчисленным из организации, выдается справка об обучении или о периоде обучения, по установленному образцу.

Примерный список вопросов итоговой аттестации:

1. Какие нормативные акты (помимо ФЗ «О персональных данных») регулируют оборот персональных данных?
2. На кого распространяется закона «О персональных данных»?
3. Что такое персональные данные работника, какие сведения к ним относятся?
4. Какими нормативными актами, в том числе и международными, регулируются вопросы защиты персональных данных работника?
5. Назовите принципы обработки персональных данных.

6. Какие предусмотрены требования к обработке персональных данных?
7. Назовите права субъектов в области защиты персональных данных.
8. Дайте характеристику обязанностям работодателя при обработке персональных данных работника.
9. Какие установлены требования к передаче персональных данных работника?
10. Назовите виды ответственности за нарушение законодательства в области защиты персональных данных работника.
11. Какие технические меры необходимо применять при организации защиты персональных данных?
12. Какие технические меры необходимо применять при организации защиты персональных данных?
13. Вправе ли физическое лицо представлять персональные данные своих близких родственников?
14. Какие работы по защите ПДн могут оказываться только при наличии лицензии на осуществление деятельности по технической защите ПДн?
15. Каковы обязанности оператора по защите персональных данных?
16. Какова ответственность за несоблюдение требований закона «О персональных данных»?
17. Что такое аттестация объекта информатизации?
18. Является ли процедура аттестация объекта информатизации обязательной?
19. Кто осуществляет функции надзора и контроля за выполнением требований закона «О персональных данных»?

7 УЧЕБНЫЙ ПЛАН ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

7.1 специалисты ОГВ и ОМСУ, организаций и учреждений по защите информации, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных.

7.2 Форма обучения: очная

7.3 Продолжительность обучения: 72 часа

7.4 План учебного процесса.

№ п/п	Наименование учебных модулей, тем	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11
1.	**Базовая часть**[2]	**72**	**58**	**46**		**12**			**14**	-
	Входное тестирование	**-**	**-**							
1.1.	**Учебный модуль № 1.** Общие вопросы технической защиты информации**.**	**16**								
1.1.1.	**Тема № 1.** Правовые и организационные основы защиты информации ограниченного доступа.			8						
1.1.2.	**Тема № 2.** Угрозы безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа.			8						
1.2.	**Учебный модуль № 2.** Организационно-технические основы обеспечения безопасности персональных данных в информационных системах персональных данных.	**26**								
1.2.1.	**Тема № 1.** Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в			9						

	информационных системах персональных данных.									
1.2.2.	**Тема № 2.** Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.			9						
1.2.3	**Тема № 3.** Практические реализации типовых моделей защищенных информационных систем обработки персональных данных.					8				
1.3.	**Учебный модель № 3.** Практические методы реализации защиты персональных данных при их обработке в информационных системах. Организация защиты информации средствами ViPNet.	**16**		12		4				
1.4.	**Учебный модуль № 4.** Темы для самостоятельного изучения	**14**							14	
2.	**Итоговая аттестация**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**Тестирование**
2.1.	Итоговое тестирование	-	-	-	-	-	-	-	-	-
	Итого:	**72**	**58**	**46**		**12**			**14**	

7.6 Сводные данные по бюджету времени

Общий объем времени, отводимого на освоение программы (календарных дней/часов)			**Распределение учебного времени (количество часов)**					
Всего	**Из них**		**Всего часов учебных занятий**	**В том числе**		**Время на самостоя-тельную работу**	**Итоговая аттестация**	**Резерв учебного времени**
	Выходные, праздничные дни	**Учебное время**		**Учебные занятия по расписанию**	**Практики**			
		38	38	32	6	-	Зачет	-

8 КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Сроки проведения занятий	Количество рабочих недель	Количество занятий в неделю	Количество занятий в курсе	Продолжительность занятия (в часах)	Сроки итоговой аттестации
Устанавливаются решением руководителя учреждения по мере формирования групп	2	5	9	8	в конце 2-й недели

9 РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА

9.1 Содержание учебных модулей, тем.

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

Учебный модуль № 1. Общие вопросы технической защиты информации.

Цель модуля - получение знаний в области организации технической защиты информации, обрабатываемой в автоматизированных системах.

Тема № 1. Правовые и организационные основы защиты информации ограниченного доступа.

Основные понятия в области защиты информации. Стратегия национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ИБ. Система документов по ЗИ и краткая характеристика ее основных составляющих.

Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Задачи, полномочия и права Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

Основные нормативно-методические документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Возможные риски организаций и их последствия при утечки ПДн.

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

Тема № 2. Угрозы безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа.

Особенности информационного элемента информационной системы персональных данных.

Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы», «атаки». Целостность, конфиденциальность и доступность информации.

Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Уровни защищённости ПДн.

Классификация угроз безопасности информации и их общая характеристика.

Технические каналы утечки информации (ТКУИ) и их классификация. Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации.

Характеристика основных угроз утечки информации по техническим каналам. Угрозы утечки акустической (речевой) информации. Угрозы утечки видовой информации. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Характеристика основных угроз несанкционированного доступа к информации в информационных системах персональных данных. Общая характеристика источников угроз несанкционированного доступа в информационных системах персональных данных. Основныеуязвимости в информационных системах персональных данных.

Результат освоения модуля:

Знания:

- Основные понятия и определения информационной безопасности;
- Нормативные документы в области информационной безопасности;
- Правовые аспекты обеспечения защиты ПДн;
- Возможные риски организаций и их последствия при утечке ПДн;
- Структура и направления деятельности системы ТЗИ.

Умения:

- Умение классифицировать угрозы безопасности в информационной системе;
- Умение определять технические каналы утечки информации;
- Умение составлять базовую модель угроз безопасности ПДн.

Учебный модуль № 2. Организационно-технические основы обеспечения безопасности персональных данных в информационных системах персональных данных.

Цель модуля – получение знаний в области организационно-технического обеспечения ПДн.

Тема № 1. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Обследование информационных систем персональных данных с целью выявления фактов обработки персональных данных, форм представления персональных данных, целей и законности обработки, способов, сроков и объёмов их обработки, источников получения и др. Формирование перечня персональных данных.

Разработка модели угроз и нарушителя безопасности информации в информационных системах персональных данных. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Порядок создания систем защиты информации в информационных системах персональных данных.

Основные принципы обеспечения безопасности персональных данных при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности,

самозащиты, многоуровневости, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

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

Основные требования и рекомендации по защите персональных данных от утечки по каналам ПЭМИН.

Оценка эффективности защиты персональных данных, обрабатываемых основными техническими средствами и системами, от утечки через ТКУИ.

Основные требования и рекомендации по защите информации в информационных системах персональных данных от несанкционированного доступа. Программно-аппаратные средства защиты персональных данных при их обработке в информационных системах персональных данных.

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну.

Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных.

Анализ технических средств несанкционированного съема информации. Анализ технических средств защиты от утечки информации.

Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии.

Анализ средств обеспечения безопасности персональных данных от физического доступа. Биометрические персональные данные способы их использования.

Тема № 2. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

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

Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.

Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.

Обязанности оператора, осуществляющего обработку персональных данных. Порядок и условия обработки персональных данных без средств автоматизации. Порядок и методы обезличивания персональных данных и их обезличивания. Особенности обработки персональных данных в условиях государственной гражданской службы и муниципальной службы. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

Тема № 3. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных.

Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или модернизации. Основное содержание этапов организации обеспечения безопасности персональных данных.

Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации.

Аттестация объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации информационной системы персональных данных по требованиям безопасности информации.

Разработка нормативной документации необходимой для обработки ПДн в информационных системах.

Разработка организационно-распорядительной документации, регламентирующей вопросы организации обеспечения безопасности персональных данных и эксплуатации средств защиты информации в информационных системах персональных данных.

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

Пассивные и активные средства защиты персональных данных.

Результат освоения модуля:

Знания:

- Основные принципы обеспечения безопасности персональных данных при их обработке;
- Основные требования и рекомендации по защите персональных;
- Оценка эффективности защиты персональных данных;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств;
- Анализ средств обеспечения безопасности персональных данных от физического доступа;
- Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов;
- Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных;
- Комплекс организационных и технических мероприятий;
- Пассивные и активные средства защиты персональных данных.

Умения:

- Разработка нормативной документации необходимой для обработки ПДн в информационных системах;
- Разработка организационно-распорядительной документации;
- Планирование работ по контролю состояния защиты персональных данных;

Учебный модуль № 3. ***Практические методы реализации защиты персональных данных при их обработке в информационных системах. Организация защиты информации средствами ViPNet.***

В модуле рассматриваются теоретические и практические вопросы, связанные с обеспечением информационной безопасности и организацией защищенных

компьютерных сетей, позволяет овладеть навыками работы в защищенной сети, знакомит с основными особенностями работы с системой защиты информации ViPNet.

Содержание модуля:

- общие положения об информационной безопасности для телекоммуникационных систем;
- основные компоненты системы защиты информации;
- VPN: определение, состав, характеристики, требования;
- система защиты информации ViPNet: общие сведения;
- технология ViPNet — концепция защиты и разграничения доступа;
- программный комплекс ViPNet;
- ViPNet Client;
- «Деловая почта», автопроцессинг, ЭЦП;
- типовые схемы применения ПО ViPNet;
- дополнительные модули ПО ViPNet.

После изучения модуля слушатель сможет:

- разбираться в компонентах информационной безопасности;
- использовать основные компоненты системы защиты информации;
- применять методы организации защищенных сетей ViPNet;
- устанавливать и настраивать ПО ViPNet Client;
- протоколировать события при помощи журнала IP-пакетов;
- настраивать и работать с транспортным модулем MFTP;
- использовать прикладное шифрование писем;
- настраивать автоматический документооборот;
- работать со службами реального времени;
- работать с программой «Деловая почта».