Автономная некоммерческая организация
дополнительного профессионального образования
«ОРЕНБУРГСКАЯ БИЗНЕС-ШКОЛА»
«ORENBURG BUSINESS SCHOOL»
460018, г. Оренбург, пр-т Победы, 75, тел./факс: (3532) 30-50-08, 30-60-5, info@orenbs.ru

Утверждаю
Директор АНО ДПО
«Оренбургская бизнес-школа»
_____С.В. Анникова
«___» _____20___ г.

Дополнительная образовательная программа
повышения квалификации

«Обеспечение безопасности персональных данных»

Оренбург
2015

Введение

Настоящая учебная программа предназначена для повышения квалификации специалистов по технической защите информации и обеспечению безопасности информации на объектах информатизации государственных органов, организующих и осуществляющих обработку персональных данных.

1. Цель реализации образовательной программы:

Реализация программы повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации.

Формирование у слушателей знания и навыков, необходимых для обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

Формирование практических навыков в разработке нормативных документов, необходимых для эффективного функционирования комплексной системы защиты персональных данных, при их обработке в автоматизированных системах и без использования таковых.

Изучение организационно-правовых основ технической защиты конфиденциальной информации.

Изучение методов и процедур выявления угроз безопасности информации на объектах защиты.

Изучение методов оценки состояния технической защиты конфиденциальной информации.

Изучение методов и порядка осуществления работ по технической защите конфиденциальной информации и обеспечения безопасности персональных данных.

2. Планируемый результат обучения:

В результате прохождения повышения квалификации слушатель должен приобрести или (и) качественно повысить профессиональные компетенции, соответствующие видам деятельности. Слушатель должен:

иметь представление:

- о способах и средствах реализации угроз безопасности информации и их источниках;
- об используемых и перспективных способах и средствах обеспечения безопасности персональных данных.

знать:

- основные положения правовых и нормативно-методических документов по обеспечению безопасности в персональных данных;

- внешние и внутренние угрозы и уязвимости для персональных данных при их обработке в информационных системах и без использования средств автоматизации;
- методику проведения классификации информационных систем персональных данных;
- методы и порядок выявления угроз и уязвимостей безопасности персональных данных;
- основы работы с техническими и программными средствами выявления угроз безопасности информации и средствами защиты от этих угроз;
- методику разработки перечня актуальных угроз безопасности персональных данных;
- рекомендации и основные мероприятия по организации и техническому обеспечению безопасности персональных данных;
- основные положения лицензирования деятельности по технической защите конфиденциальной информации, сертификации и аттестации объектов информатизации по требованиям безопасности информации.

уметь:

- проводить классификацию информационных систем персональных данных;
- определять актуальные угрозы безопасности персональных данных;
- разрабатывать уведомительные и нормативные документы, необходимые для эффективной защиты персональных данных в соответствии с требованиями действующего законодательства;
- определять комплекс мероприятий по организации и техническому обеспечению безопасности персональных данных;
- грамотно оценивать и выбирать программные и технические средства защиты информации, которые могут быть использованы при создании (дооборудовании) и дальнейшей эксплуатации информационных систем персональных данных.

иметь навыки:

- работы с правовыми базами данных;
- работы с базами данных по объектам защиты и угрозам безопасности информации;
- разработка необходимых документов в интересах организации работ по конфиденциальной информации.

3. Содержание программы

3.1 Учебный план

№	Модули	Количество часов					
		Трудоемкость всего	Аудиторные занятия			Самостоятельная подготовка	Аттестация
			Всего	Лекции	Практические (лабораторные) занятия		
1	Введение	2	2	2			зачет
2	Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации	16	14	10	4	2	зачет
3	Основы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных	32	28	20	8	4	зачет
4	Порядок создания и эксплуатации информационных систем	20	18	10	8	2	зачет
	Итоговая аттестация.	2					зачет
	Итого:	**72**	**54**	**22**	**32**	**16**	

3.3 Учебно-тематический план

№	Перечень тем и их содержание	Количество часов						
		Трудоемкость всего	Аудиторные занятия					Самостоятельная подготовка
			Всего	Лекции	Семинары	Практические (лабораторные) занятия	Аттестация	
1.	**Введение**	**2**	**2**	**2**				
1.1.	Цель, задачи, структура и содержание курса. Основные понятия, термины и определения в области информационной		1	1				
1.2.	Актуальность проблемы защиты информации. Структура государственной системы защиты информации. Классификация угроз безопасности информации. Классификация каналов утечки		1	1				
2.	**Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации.**	**16**	**14**	**10**	**2**	**2**		**2**
2.1	Структура, задачи и основные функции органов государственной власти, отвечающих за организацию защиты персональных данных в		2	2				
2.2	Законодательная и нормативная база правового регулирования вопросов защиты персональных данных. Руководящие документы по защите персональных данных.		4	2	2			
2.3	Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях		2	2				

2.4	Порядок лицензирования операторов информационных систем персональных данных.		2	2				
2.5	Организационные и технические требования и рекомендации по технической защите информации ограниченного доступа в государственных, муниципальных органов и организаций.		4	2		2		
3.	**Основы обеспечения безопасности персональных данных при их обработке в информационных системах**	**32**	**28**	**20**	**4**	**4**		**4**
3.1	Понятие информационной системы персональных данных. Классификация информационных систем персональных данных. Порядок составления соответствующего акта.		2	2	2			
3.2	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.		2	2				
3.3	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.		2			2		
3.4	Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.		2			2		
3.5	Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных различных классов.		2	2				

3.6	Средства защиты информации, применяемые при защите информационных системах персональных данных.		2	2				
3.7	Оценка защищенности информационных систем персональных данных. Порядок принятия решения о		2	2				
3.8	Требования к подготовке к утилизации и порядок утилизации персональных данных и машиночитаемых носителей информации, используемых в обработке персональных данных.		4	2	2			
3.9	Защищенный электронный документооборот персональных данных. Использование электронной цифровой подписи в информационных системах персональных данных.		2	2				
3.10	Мероприятия по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств		2	2				
3.11	Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных		2	2				
4.	**Порядок создания и эксплуатации информационных систем персональных данных**	**20**	**18**	**10**		**8**		**2**
4.1	Общий порядок организации обеспечения безопасности персональных данных в информационных системах		2	2				

4.2	Разработка технического обоснования для создания системы защиты информационных систем персональных данных.		2			2		
4.3	Оформление технического (частного технического) задания на разработку системы (подсистемы) защиты		2			2		
4.4	Порядок внедрения средств обеспечения информационной безопасности в информационных системах персональных данных.		2	2				
4.5	Требования по аттестации информационных систем персональных данных.		2	2				
4.6	Техническое обслуживание и ремонт аттестованных информационных систем персональных данных.		2	2				
4.7	Периодичность и содержание работ по контролю обеспечения безопасности персональных данных.		2	2				
4.8	Контроль и оценка состояния технической защиты информации на объекте информатизации государственных, муниципальных органов и организаций.		4			4		
	Зачет	2						
	Итого	**72**	**62**	**42**	**6**	**14**		**10**

4. Форма аттестации и оценочные материалы:

4.1 Итоговая аттестация

Итоговая аттестация проводится в форме собеседования по следующим вопросам:

1. Основные понятия, термины и определения в области информационной безопасности.
2. Классификация угроз безопасности информации.
3. Основные направления защиты конфиденциальной информации.
4. Законодательная и нормативная база правового регулирования вопросов защиты информации ограниченного доступа.
5. Руководящие документы по защите информации от несанкционированного доступа.
6. Законодательная и нормативная база правового регулирования вопросов защиты персональных данных.
7. Руководящие документы по защите персональных данных.
8. Основные термины, определения и общие положения в области защиты персональных данных.
9. Понятие и классификация информационных систем персональных данных. Форма и содержание соответствующего акта.
10. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
11. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
12. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных.
13. Оформление технического (частного технического) задания на разработку системы (подсистемы) защиты персональных данных.
14. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных различных классов.
15. Оценка существующих мер защиты информации. Порядок принятия решения о необходимости дополнительных мер защиты.
16. Требования к подготовке к утилизации и порядок утилизации персональных данных и машиночитаемых носителей информации, используемых в обработке персональных данных.
17. Организация работы с персоналом, допущенных к обработке персональных данных.
18. Электронный документооборот персональных данных.
19. Использование электронной цифровой подписи в ИСПДн.
20. Периодичность и содержание контроля за обеспечением защищенности персональных данных.
21. Назначение, вид и цели создания объекта информатизации.

22. Виды объектов информатизации. Защищаемое помещение. Объект вычислительной техники.
24. Порядок организации работ по созданию и эксплуатации объектов информатизации и систем защиты информации. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
25. Основные технические средства и системы. Вспомогательные технические средства и системы.
26. Средства вычислительной техники. Межсетевые экраны. Показатели защищенности от несанкционированного доступа к информации.
27. Автоматизированные системы. Классификация автоматизированных систем
и требования по защите информации.
28. Типы средств защиты информации от НСД. Сравнительные характеристики
СЗИ от НСД («Аккорд», «Secret Net», «Dallas Lock», «Блок Пост» и т. д.)

5. Организационно – педагогические условия

Обучение по программе проводится в очной форме.

Рекомендуемое количество обучающихся в группе – не более 8 человек.

Занятия проводятся в компьютерном классе, оснащенном программами «Консультант Плюс», или «Гарант», выходом в Интернет.

6. Список рекомендуемых источников

6.1 Основная литература

1. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности/ Учебное пособие. – СПб: НИУ ИТМО, 2012. 148 с.
2. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности, - СПб: СПбНИУИТМО, 2014. – 173 с.
3. Конституция Российской Федерации;
4. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001г. № 195-ФЗ Статья 13.11.
Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) Глава 13. Административные правонарушения в области связи и информации (ст.ст. 13.113.24). Раздел II. Особенная часть;
5. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197- ФЗ Глава 14 «Защита персональных данных работника» (ст. ст. 85-90);
6. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ.
Статья 137. Нарушение неприкосновенности частной жизни. Глава 19. Преступления против конституционных прав и свобод человека и гражданина (ст.ст. 136-149). Раздел VII. Преступления против

личности (ст.ст. 105-157). Особенная часть (ст.ст. 105-360) Статья 140. Отказ в предоставлении гражданину информации. Глава 19. Преступления против конституционных прав и свобод человека и гражданина (ст.ст. 136-149). Раздел VII. Преступления против личности (ст.ст. 105-157). Особенная часть (ст.ст. 105-360) Статья 272. Неправомерный доступ к компьютерной информации. Глава 28. Преступления в сфере компьютерной информации (ст.ст. 272-274). Раздел IX. Преступления против общественной безопасности и общественного порядка (ст.ст. 205-274). Особенная часть (ст.ст. 105-360);

7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
8. Федеральный закон от 8 августа 2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей»;
9. Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
11. Федеральный закон от 29 декабря 2006 г. № 256-ФЗ «О дополнительных мерах государственной поддержки семей, имеющих детей»;
12. Федеральный закон от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации» Глава 4. Хранение и учет архивных документов (ст.ст. 17- 19). Глава П. Государственные реестры ст.ст. 4 -7;
13. Основы законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 г. № 5487-1. Статья 61. Врачебная тайна Раздел X. Права и социальная поддержка медицинских и фармацевтических работников (ст.ст. 54 - 64);
14. Постановление Правительства РФ от 19 января 2005 г. № 30 «О Типовом регламенте взаимодействия федеральных органов исполнительной власти»;
15. Постановление Правительства РФ от 28 июля 2005 г. № 452 «О Типовом регламенте внутренней организации федеральных органов исполнительной власти»;
16. Постановление Правительства Российской Федерации от 30 декабря 2006 г. № 873 «О порядке выдачи государственного сертификата на материнский (семейный) капитал»;
17. Постановление Правительства Российской Федерации от 14 февраля 2007 г. № 94 «О государственной информационной системе миграционного учета»;
18. Постановление Правительства РФ от 6 июня 2007 г. № 353 «Вопросы Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия»;
19. Постановление Правительства РФ от 2 июня 2008г. №419 «О Федеральной службе по надзору в сфере связи и массовых

коммуникаций»;

20. Постановление Правительства Российской Федерации от 27 сентября 2007 г. № 612 «Об утверждении Правил продажи товаров дистанционным способом», Пункт 16;
21. Постановление Правительства Российской Федерации от 17 ноября 2007 года №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
22. Распоряжение Правительства Российской Федерации от 15 августа 2007 г. № 1055-р «Об утверждении Плана подготовки проектов нормативных правовых актов, необходимых для реализации Федерального закона «О персональных данных»;
23. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
24. Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 2 октября 2007г. №199 «Об утверждении Типового положения о территориальном органе Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия», (с изменениями от 18 января 2008 года);
25. Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28 марта 2008 г. № 154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных»;
26. Приказ Министерства природных ресурсов Российской Федерации от 5 сентября 2007 г. № 230 «О защите персональных данных государственных гражданских служащих Министерства природных ресурсов Российской Федерации, заместителей руководителей федеральных органов исполнительной власти, находящихся в ведении Министерства природных ресурсов Российской Федерации, руководителей их территориальных органов».
27. Федеральный закон Российской Федерации от 10 января 2002г. № 1-ФЗ «Об электронной цифровой подписи».
28. Федеральный закон Российской Федерации 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне».
29. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно телекоммуникационных сетей международного информационного обмена (Указ Президента Российской Федерации от 17.03.2008 г. №351).
30. Перечень сведений конфиденциального характера (Указ Президента Российской Федерации от 6 марта 1997 г. № 188).
31. О лицензировании деятельности по технической защите конфиденциальной информации. (Постановление Правительства РФ от 15.08.2006г. №504.).

32. О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации. (Постановление Правительства РФ от 31.08.2006г.).
33. Руководящий документ. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. (Председатель Гостехкомиссии России от 25.11.1994г.).
34. Руководящий документ. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. (Заместитель директора ФСТЭК от 15.02. 2008г.).
35. Руководящий документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Заместитель директора ФСТЭК от 15.02. 2008г.).
36. Руководящий документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Заместитель директора ФСТЭК от 15.02. 2008г.).
37. Руководящий документ. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. (Заместитель директора ФСТЭК от 15.02. 2008г.).
38. Руководящий документ. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (Руководитель 8 центра ФСБ России от 21 февраля 2008 года № 149/54-144)
39. Руководящий документ. 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. (Руководитель 8 центра ФСБ России от 21 февраля 2008 года № 149/54-144)

6.2 Информационно – справочные источнпики

1. Справочно – правовая система «Консультант Плюс»
2. Справочно – правовая систем «Гарант»

6.3 Нормативно – правовые источники

1. Алексенцев А.И. Защита информации: Словарь базовых терминов и определений. М: РГТУ,2000.
2. Герасименко В.А., Малюк А.А, Основы защиты информации. - М.: Изд-воМИФИ, 1997.
3. ГОСТ ИСО/МЭК 15408-1-2002. Информационная технология. Методы и

средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
4. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
5. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
6. ГОСТ Р 50739-95. СВТ. Защита от несанкционированного доступа к информации.
7. ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений приее обработке средствами вычислительной техники. Методы испытаний.
8. ГОСТ Р 50922-96. Защита информации. Основные термины определения.
9. ГОСТ Р 51624-2000. Автоматизированные системы в защищенном исполнении. Общие требования.
10. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.
11. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
12. ГОСТ Р 51583-2000. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
13. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования.
14. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на АС. Техническое задание на создание АС.
15. ГОСТ 28388-89. Система обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.
16. Грушо А.А., Тимоыина Е.Е. Теоретические основы защиты информации. - М.: Издательство Агентства «Яхтсмен», 1996.
17. Зима В.М., Ломако А.Г., Ростовцев Ю.Г. Технологии обеспечения информационно-компьютерной безопасности. Санкт-Петербург: ВИКУ им. А.Ф.Можайского. 2000.
18. Корнеев И.К. Информационное обеспечение управленческой деятельности. М,: Горячая линия - Телеком, 2000.
19. Кузнецов С.Л. Делопроизводство на компьютере. М.: ЗАО «Бизнес школа «Интелсинтез»»,1999.
20. Хорев А.А. Способы и средства защиты информации. Учебное пособие. М.: МО РФ. 2000 г.