

**Учебный план программы курса повышения квалификации по направлению
«Защита персональных данных. Построение модели угроз безопасности
информации систем и сетей»**

№ п/п	Разделы и темы	Всего часов	Аудиторные занятия, час.		Самост. работа
			Лекции	Практ. занятия	
1.	<i>Введение. Основы компьютерной безопасности, источники и носители конфиденциальной информации.</i>	6	2	2	2
1.1.	Понятие и принципы компьютерной безопасности	3	1	1	1
1.2	Источники и носители конфиденциальной информации, защищаемые техническими средствами	3	1	1	1
2.	<i>Основные направления деятельности в области защиты персональных данных. Обзор нормативно-правовой базы в области защиты ПДн.</i>	7	1	2	4
2.1.	Основные направления деятельности в области защиты персональных данных. Общие представления о защищаемой информации. Обзор нормативно-правовой базы в области защиты ПДн, Федеральный закон №152 «О персональных данных» от 27.07.2006, Обезличивание ПДн. Общие вопросы. Определение уровней защищенности в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	7	1	2	4
3.	<i>Построение модели угроз безопасности информации систем и сетей</i>	32	6	11	14
3.1.	Вводная лекция. Определение что такое модель угроз. Цели и задачи. Какие НПА включают в себя необходимость разработки модели угроз на объекте (Приказ ФСТЭК № 21 от 18 февраля 2013 с изменениями 23 марта 2017 года, Приказ ФСТЭК № 17 от 11 февраля 2013 с изменениями 15 февраля 2017 года, Правительственное постановление № 1119 от 01.11.2012 г., Федеральный закон № 152 ст.19 ч.2, Приказы ФСТЭК № 239 от 25.12.2017 г. и 31 от 14.03.2014 г.) Обзор документа методики оценки угроз безопасности информации (ФСТЭК, 2021), структура по разделам документа и приложениям, положительные и негативные аспекты.	4	1	1	2
3.2.	БДУ ФСТЭК. Банк данных угроз ФСТЭК, описание автоматизированного раздела, порядок работы.	4	1	1	2

№ п/п	Разделы и темы	Всего часов	Аудиторные занятия, час.		Самост. работа
			Лекции	Практ. занятия	
3.3.	Построение модели угроз. Описание ИС объекта. Определение пользователей ИС	4	1	1	2
3.4.	Построение модели угроз. Определение потенциальных нарушителей для объекта и их возможности. Определение актуальных для каждой конкретной ИС нарушителей с указанием возможных видов воздействия и способов их реализации, а также видов негативных последствий.	5	1	2	2
3.5.	Построение модели угроз. Моделирование действий нарушителя при реализации УБИ. Построение модели угроз. Определение актуальности угроз.	9	1	4	4
3.6	МУ как функциональная система в динамике. Описание рабочих подходов, которые можно встроить в практическую деятельность для выявления угроз и нарушителей.	5	1	2	2
4.	Популярные тактики злоумышленников, технические аспекты противодействия актуальным угрозам информационной безопасности	4	1	1	2
4.1	Наиболее популярные техники у злоумышленников, наиболее опасные техники и уязвимости, матрица Mitre Att&ck, порядок предотвращения продвижения злоумышленника в системе, особенности проведения пентеста.	4	1	1	2
5.	Психологический портрет нарушителя	3	1	-	2
5.1.	Выявление характерологических признаков и составление психологического портрета возможного нарушителя и лояльного сотрудника в сфере информационной безопасности	3	1	-	2
6.	Разработка организационно-распорядительных документов по защите персональных данных. Риски ИБ	7	1	2	4
6.1.	Основы разработки ОРД по защите ПДн. Основы оценки рисков информационной безопасности, страхование рисков.	7	1	2	4
7.	Фишинг	3	1	1	1
7.1.	Фишинг - как вид интернет-мошенничества, позволяющий получить доступ к персональным данным	3	1	1	1
8.	Основы криптографической защиты персональных данных	3	1	1	1
8.1	Основы криптографической защиты персональных данных	3	1	1	1

№ п/п	Разделы и темы	Всего часов	Аудиторные занятия, час.		Самост. работа
			Лекции	Практ. занятия	
9.	<i>Аттестация объекта информатизации (относительно персональных данных)</i>	4	1	1	2
9.1	Аттестация объекта информатизации (относительно персональных данных)	4	1	1	2
10.	<i>Особенности защиты объектов КИИ, на которых происходит обработка персональных данных</i>	3	1	1	1
10.1	Особенности защиты объектов КИИ, на которых происходит обработка персональных данных	3	1	1	1
	Всего:	72	17	22	33