федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

УТВЕРЖДАЮ
_____
«__» _____ 20__ г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

Программа повышения квалификации

вид дополнительной профессиональной программы: программа повышения квалификации или программа профессиональной переподготовки

Наименование программы Информационная безопасность: практика подготовки к проверке Роскомнадзора за соответствием законодательству обработки персональных данных в организации

Категория слушателей: специалисты в области информационной безопасности или ответственных за организацию обработки персональных данных в организации и разработана в соответствии с актуальными требованиями регуляторов в области обработки и защиты персональных данных.

Уровень квалификации: без присвоения квалификации

Объем: 72 часа

Форма обучения: очная

Тольятти 2020 г.

Разработчик:
Власов Игорь Анатольевич, главный специалист по информационной безопасности Тольяттинского государственного университета.

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Нормативные правовые основания разработки программы

Нормативную правовую основу разработки программы составляют:

Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

приказ Минтруда России от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов»;

приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

Программа разработана на основе требований ФГОС 10.03.01 Информационная безопасность (уровень бакалавриата).

Программа разработана с учетом профессионального(ых) стандарта(ов) (квалификационных требований): Проект Приказа Министерства труда и социальной защиты РФ "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (подготовлен Минтрудом России 21.12.2015).

1.2. Срок освоения программы: 72 часа

1.3. Требования к слушателям: лица, желающие освоить программу повышения квалификации, должны иметь среднее профессиональное или высшее образование. Предназначена для специалистов в области информационной безопасности или ответственных за организацию обработки ПДн в организации Наличие допуска к государственной тайне определяется работодателем в соответствии с нормативными правовыми актами. Без предъявления требований к стажу работы.

1.4. Формы освоения программы (очная, очно-заочная, заочная) *очная*

1.5. Цель и планируемые результаты обучения

Целью реализации программы повышения квалификации является формирование у слушателей профессиональных компетенций в области разработки организационно-распорядительной документации (ОРД) по организации обработки и защиты персональных данных (ПДн) в соответствии с текущим законодательством и требованиями регуляторов.

Программа направлена на освоение (совершенствование) следующих профессиональных компетенций:

ПК 4 - способностью участвовать в работах по реализации политики информационной безопасности в области обработки и защиты персональных данных;

ПК 5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК 6 - способностью принимать участие в организации и проведении аудита информационных систем и уровня защищенности;
ПК 8 - способностью создавать схемы защиты информации с учетом действующих нормативных и методических документов, технических паспортов информационных систем;
ПК 10 - способностью проводить анализ информационной безопасности систем на соответствие требованиям стандартов в области информационной безопасности, составления моделей угроз безопасности информации;
ПК 13 - способностью принимать участие в формировании комплекса мер по обеспечению безопасности персональных данных при их обработке в информационных системах, управлять процессом их реализации;
ПК 15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Профессиональные компетенции	Соответствующая ОТФ, ТФ, ТД и др. профессионального стандарта	Практический опыт	Умения	Знания
1	2	3	4	5
ПК 4 - способностью участвовать в работах по реализации политики информационной безопасности в области обработки и защиты персональных данных; *«имеющиеся компетенции»*.	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации. Код В. Уровень квалификации 6.	- Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения защиты информации в автоматизированной системе. - Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации .	- Оценивать информационные риски в автоматизированных системах. - Классифицировать и оценивать угрозы безопасности информации. - Определять подлежащие защите информационные ресурсы автоматизированных систем. - Применять действующую законодательную базу в области обеспечения безопасности информации.	- Основные методы управления защитой информации. - Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах. - Основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) Основные положения
ПК 5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации; *«имеющиеся компетенции»*.				
ПК 6 - способностью принимать участие в организации и проведении аудита информационных систем и уровня защищенности;				

«имеющиеся компетенции».				
ПК 8 - способностью создавать схемы защиты информации с учетом действующих нормативных и методических документов, технических паспортов информационных систем; *«имеющиеся компетенции».*			- Пользоваться нормативными документами по противодействию технической разведке. - Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем. - Конфигурировать параметры системы защиты информации автоматизированных систем.	законодательства Российской Федерации в области защиты информации, отечественные и зарубежные стандарты в области информационной безопасности Правовые основы организации защиты государственной тайны и конфиденциальной информации Методы защиты информации в автоматизированных системах
ПК 10 - способностью проводить анализ информационной безопасности систем на соответствие требованиям стандартов в области информационной безопасности, составления моделей угроз безопасности информации; *«имеющиеся компетенции».*				
ПК 13 - способностью принимать участие в формировании комплекса мер по обеспечению безопасности персональных данных при их обработке в информационных системах, управлять процессом их реализации; *«осваиваемые компетенции».*				
ПК 15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими				

документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю *«осваиваемые компетенции».*				

II. УЧЕБНЫЙ ПЛАН

№ п/п	Результат (коды формируемых ПК)	Наименование учебных тем	Формы промежуточной аттестации	Контактные (аудиторные) учебные занятия		Самостоятельная работа обучающегося *(при наличии)*		Практика (стажировка) (час.)	Всего (час.)
				Всего (час.)	в т. ч. лабораторные и практические занятия (час.)	Всего (час.)	в т. ч. консультаций при выполнении самостоятельной работы *(при наличии)* (час.)		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1.	ПК 4; ПК 8; ПК 10; ПК 15	Модуль 1. Нормативная база	тестирование	8	2	-			8
2.	ПК 5; ПК 8; ПК 15	Модуль 2. Разработка ОРД	тестирование	36	6	2			38
3.	ПК 6; ПК 13	Модуль 3. Методика проведения оценки соответствия	тестирование	16	8	2			18
4.	ПК 15	Модуль 4. Методика проверки Роскомнадзора	тестирование	6	-	2			8
5.	ПК 4-6, 8, 10, 13, 15	Итоговая аттестация	зачет						

	Всего по программе:	64	*14*	8			**72**

III. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Образовательный процесс по программе может осуществляться в течение всего учебного года. Занятия проводятся по мере комплектования групп.

Учебные занятия проводятся 2 раз в неделю по 8 часов в день. Общая продолжительность обучения – 1 месяц.

IV. СОДЕРЖАНИЕ ПРОГРАММЫ (РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ ПРЕДМЕТОВ, КУРСОВ, ДИСЦИПЛИН (МОДУЛЕЙ)

Содержание учебного модуля 1 Нормативная база

Наименование разделов и тем	**Содержание учебного материала и формы организации деятельности обучающихся**		**Объем часов**
1	**2**		**3**
Тема 1. Законодательная база информационной безопасности по работе с персональными данными	**Содержание учебного материала** *(указывается перечень дидактических единиц темы)*	**Уровень освоения**	*2*
	1 Законодательство в области защиты персональных данных	*1*	
	2 Методика определения уровня защищенности	*1*	
	Информационные (лекционные) занятия *(при наличии, указываются темы)*		2
	Тема 1. Законодательство в области защиты персональных данных. Уровни защищенности и приказы ФСТЭК №№ 17, 21. 3. Методика определения уровня защищенности. Условия, допускающие обработку персональных данных Тенденции развития законодательной базы		
	Практические занятия, стажировка *(при наличии, указываются темы)*		
	Не предусмотрены		
	Самостоятельная работа обучающихся *(при наличии указывается тематика и содержание выполняемых работ, заданий)* Не предусмотрена		
Тема 2. Правоприменение. Уведомление в РКН	**Содержание учебного материала** *(указывается перечень дидактических единиц темы)*	**Уровень освоения**	*6*
	1 Правоприменение.	*2*	
	2 Уведомление в РКН	*2*	
	Информационные (лекционные) занятия *(при наличии, указываются темы)*		4
	Тема 2. Правоприменение. Актуальные комментарии к законодательству. Мнение и позиция РКН по некоторым вопросам законодательства. Облачные технологии хранения данных и соответствие текущему законодательству. Требования к сайту организации и практические вопросы оформления сайта		2
	Тема 3. Уведомления в РНК.		2

	Оформление и актуализация уведомления.	
	Практические занятия, стажировка *(при наличии, указываются темы)*	2
	Практическое занятие 1. Определение уровня защищенности. Оформление страниц сайта с формами, предусматривающими содержание ПДн	
	Самостоятельная работа обучающихся *(при наличии указывается тематика и содержание выполняемых работ, заданий)* Не предусмотрена	
	Всего:	*8 ч*

Содержание учебного модуля 2 Разработка ОРД

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем часов
1	**2**		**3**
Тема 1. Разработка ОРД	**Содержание учебного материала** *(указывается перечень дидактических единиц темы)*	**Уровень освоения**	*33*
	1 Разработка положений и политик. Разработка инструкций и журналов.	*2*	
	2 Разработка планов и отчетов	*2*	
	Информационные (лекционные) занятия *(при наличии, указываются темы)*		26
	Тема 1.Разработка положений и политик. Политика ИБ. Политика в отношении обработки ПДн. Положение об обработке ПДн. Учредительные документы. Согласие на обработку ПДн. Положение о применимости базовых мер по обеспечению безопасности персональных данных. Необходимые приказы. Необходимые регламенты.		10
	Тема 2. Разработка инструкций и журналов. Инструкция администратора ИСПДн. Инструкция пользователя ИСПДн. Инструкция действий должностных лиц по обеспечению безопасности. Инструкция ответственному за организацию обработки персональных данных. Необходимые журналы		10
	Тема 3. Разработка планов и отчетов. Планы, отчеты о проведении внутренних проверок обеспечения защиты информационных систем персональных данных. Необходимые схемы.		6
	Практические занятия, стажировка *(при наличии, указываются темы)*		6
	Практическое занятие 1. Практическая разработка «Положение об обработке ПДн».		4
	Практическое занятие 2. Схема организации технической защиты ИСПДн.		2
	Самостоятельная работа обучающихся *(при наличии указывается тематика и содержание выполняемых работ, заданий)*		*1*

	Подготовка к тестированию по теме		
Тема 2. Обработка Пдн без использования средств автоматизации	**Содержание учебного материала** *(указывается перечень дидактических единиц темы)*	**Уровень освоения**	*5*
	1 Обработка Пдн без использования средств автоматизации	*2*	
	Информационные (лекционные) занятия *(при наличии, указываются темы)*		
	Тема 4. Обработка Пдн без использования средств автоматизации. Документы, необходимые в соответствии с ПП №687. Нетиповые формы, предполагающие наличие ПДн. Договор – поручение на обработку ПДн.		4
	Практические занятия, стажировка *(при наличии, указываются темы)*		
	Не предусмотрены.		
	Самостоятельная работа обучающихся *(при наличии указывается тематика и содержание выполняемых работ, заданий)* Подготовка к тестированию по теме		*1*
		Всего:	*38 ч*

Содержание учебного модуля 3 Методика проведения оценки соответствия

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем часов
1	**2**		**3**
Тема 1. Разработка модели угроз информационной системы	**Содержание учебного материала** *(указывается перечень дидактических единиц темы)*	**Уровень освоения**	*7*
	1 Угрозы информационных систем	*2*	
	Информационные (лекционные) занятия *(при наличии, указываются темы)*		
	Тема 1.Угрозы информационных систем Аудит состояния информационной безопасности в организации. Частная модель угроз		2
	Практические занятия, стажировка *(при наличии, указываются темы)*		
	Практическое занятие 1. Частная модель угроз.		4
	Самостоятельная работа обучающихся *(при наличии указывается тематика и содержание выполняемых работ, заданий)* Подготовка к тестированию по теме		*1*
Тема 2. Оценка соответствия информационных систем	**Содержание учебного материала** *(указывается перечень дидактических единиц темы)*	**Уровень освоения**	*11*
	1 Соответствие информационных систем требованиям безопасности информации	*2*	
	Информационные (лекционные) занятия *(при наличии, указываются темы)*		
	Тема 2. Оценка соответствия информационных систем требованиям безопасности.		6

требованиям безопасности информации	Требования по защите персональных данных при их обработке в информационные системы обработки персональных данных (ИСПДн) в соответствии с присвоенным классом. Модель обследования ИСПДн. Аттестация объекта информатизации по требованиям безопасности информации. Практические вопросы проведения оценки соответствия и разработки документации	
	Практические занятия, стажировка *(при наличии, указываются темы)*	
	Практическое занятие 2. Технический паспорт ИСПДн.	4
	Самостоятельная работа обучающихся *(при наличии указывается тематика и содержание выполняемых работ, заданий)* Подготовка к тестированию по теме	*1*
	Всего:	*18 ч*

Содержание учебного модуля 4 Методика проверки Роскомнадзора

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем часов
1	**2**		**3**
Тема 1. Содержание проверки РКН	**Содержание учебного материала** *(указывается перечень дидактических единиц темы)*	**Уровень освоения**	*6*
	1 Содержание проверки РКН	*3*	
	Информационные (лекционные) занятия *(при наличии, указываются темы)*		5
	Тема 1. Содержание проверки РКН. Проверка соответствия сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности. Проверка места нахождения базы данных. Проверка наличия условий, допускающих обработку ПДн. Проверка наличия обработки биометрических и специальных категорий ПДн. Проверка соблюдения условий трансграничной передачи ПДн. Согласия. Соблюдение установленных требований при поручении обработки персональных данных третьему лицу. Проверка соблюдения требований по уничтожению персональных данных. Проверка выполнения требований конфиденциальности при обработке персональных данных. Проверка принятия мер, необходимых и достаточных для обеспечения выполнений обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных. Проверка выполнения требований по информированию лиц о факте обработки ими персональных данных. Проверка соблюдения требований, предъявляемых к типовым формам документов. Соблюдение требований в части определения мест хранения персональных данных. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ. Проверка соблюдения требований, установленных законодательством Российской Федерации, при обработке персональных данных работников.		5

	Практические занятия, стажировка *(при наличии, указываются темы)*		
	Не предусмотрена		
	Самостоятельная работа обучающихся *(при наличии указывается тематика и содержание выполняемых работ, заданий)* Подготовка к тестированию по теме		*1*
Тема 2. Порядок составления справки в РКН	**Содержание учебного материала** *(указывается перечень дидактических единиц темы)*	**Уровень освоения**	*2*
	1 Справка в РКН	*3*	
	Информационные (лекционные) занятия *(при наличии, указываются темы)*		1
	Тема 2. Порядок составления справки в РКН. Содержание вопросов, отражаемых в справке.		1
	Практические занятия, стажировка *(при наличии, указываются темы)*		
	Не предусмотрена		
	Самостоятельная работа обучающихся *(при наличии указывается тематика и содержание выполняемых работ, заданий)* Подготовка к тестированию по теме		*1*
		Всего:	*8 ч*

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

V. ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

5.1. Формы аттестации

Промежуточная аттестация проводится по модулям 1-4 в форме компьютерного тестирования.

Итоговая аттестация производится в виде зачета.

Возможные варианты вопросов к зачету перечислены в Приложении А.

Лицам, успешно освоившим программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации

5.2. Оценочные средства

Основные показатели оценки планируемых результатов

Результаты освоения программы (освоенные умения, усвоенные знания)	Критерии оценки результатов освоения программы
ПК 4 - способностью участвовать в работах по реализации политики информационной безопасности в области обработки и защиты персональных данных;	Выполнение практической работы по темам: - Определение уровня защищенности. - Оформление страниц сайта с формами, предусматривающими содержание ПДн
ПК 5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;	Разработка «Положение об обработке ПДн». Разработка «Схема организации технической защиты ИСПДн.
ПК 6 - способностью принимать участие в организации и проведении аудита информационных систем и уровня защищенности;	Определение частной модели угроз. Разработка «Технический паспорт ИСПДн».
ПК 8 - способностью создавать схемы защиты информации с учетом действующих нормативных и методических документов, технических паспортов информационных систем.	Выполнение практической работы по темам: - Определение уровня защищенности. - Оформление страниц сайта с формами, предусматривающими содержание ПДн Разработка «Положение об обработке ПДн». Разработка «Схема организации технической защиты ИСПДн.
ПК 10 - способностью проводить анализ информационной безопасности систем на соответствие требованиям стандартов в области информационной безопасности, составления моделей угроз безопасности информации;	Выполнение практической работы по темам: - Определение уровня защищенности. - Оформление страниц сайта с формами, предусматривающими содержание ПДн

ПК 13 - способностью принимать участие в формировании комплекса мер по обеспечению безопасности персональных данных при их обработке в информационных системах, управлять процессом их реализации;	Определение частной модели угроз. Разработка «Технический паспорт ИСПДн».
ПК 15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Выполнение практической работы по темам: - Определение уровня защищенности. - Оформление страниц сайта с формами, предусматривающими содержание ПДн. Разработка «Положение об обработке ПДн». Разработка «Схема организации технической защиты ИСПДн.

Примерный перечень вопросов к зачету представлен в Приложении А.

VI. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

6.1. Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса.
Образовательный процесс по дисциплинам (модулям) обеспечивается научно-педагогическими кадрами, имеющими базовое образование, соответствующее профилю дисциплины (модулю), и ученую степень или опыт деятельности в соответствующей профессиональной сфере и систематически занимающимися научной и/или научно-методической деятельностью.

6.2. Требования к материально-техническим условиям
Реализация программы модуля предполагает наличие компьютерных классов корпус УЛК, ауд. № 918.
Учебный процесс обеспечивается необходимым комплектом лицензионного программного обеспечения MS Windows и MS Office.
Оборудование учебного кабинета и рабочих мест кабинета УЛК №918: 23 ПК, интерактивная доска.
Оборудование и технологическое оснащение рабочих мест: ПК с выходом в интернет, наушники, веб-камеры, интерактивная доска.

6.3. Требованиям к информационным и учебно-методическим условиям
Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы
Основные источники:

1. Исаев А.С. Правовые основы организации защиты персональных данных [Электронный ресурс] : учебное пособие / А.С. Исаев, Е.А. Хлюпина. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2014. — 106 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67564.html
2. Кухаренко Т.А. Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (3-е издание переработанное и дополненное) [Электронный ресурс] / Т.А. Кухаренко, Н.А. Захарова. — Электрон. текстовые данные. — Саратов: Ай Пи Эр Медиа, 2016. — 151 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/49154.html
3. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 121 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52153.html
4. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.html

Дополнительные источники:

1. Аверченков В.И. Защита персональных данных в организации [Электронный ресурс] : монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 124 c. — 5-89838-382-4. — Режим доступа: http://www.iprbookshop.ru/6993.html
2. Макаров А.М. Организация защиты персональных данных [Электронный ресурс] : лабораторный практикум / А.М. Макаров, И.В. Калиберда, К.О. Бондаренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 92 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62971.html
3. Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Защита персональных данных [Электронный ресурс] : учебное пособие / М.И. Шубинский. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2013. — 77 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/68654.html
4. Петрыкина Н.И. Правовое регулирование оборота персональных данных [Электронный ресурс] : теория и практика / Н.И. Петрыкина. — Электрон. текстовые данные. — М. : Статут, 2011. — 135 c. — 978-5-8354-0771-2. — Режим доступа: http://www.iprbookshop.ru/28992.html

Электронные источники:

1. Портал РКН. Режим доступа: [https://63.rkn.gov.ru]

После каждого наименования печатного издания обязательно указываются издательство и год издания (в соответствии с ГОСТом).

6.4. Общие требования к организации образовательного процесса

Программа курса ориентирована на формирование у слушателей активной профессиональной позиции в отношении соблюдения законодательства в сфере защиты персональных данных.

В процессе освоения программы используются активные формы проведения занятий. При реализации учебного процесса используются аудиторные и сетевые формы образовательного взаимодействия. Занятия проводятся в компьютерном классе.

Практическая работа организовывается на основе системы заданий для индивидуальной работы. Результаты, полученные в процессе выполнения заданий, обсуждаются и анализируются на практических занятиях. По согласованию со слушателями, выполненные задания размещаются в открытом доступе, что позволяет сформировать банк дидактических и учебно-методических материалов, которыми могут пользоваться все желающие.

Приложение А.

Примерный перечень вопросов к зачету

1. Нормативная база обработки ПДн.
2. Перечень учредительных документов.
3. Принципы обработки ПДн.
4. Условия, допускающие обработку персональных данных.
5. Категории персональных данных.
6. Реагирование на запросы субъекта персональных данных.
7. Требования ФСТЭК России по защите персональных данных.
8. Обязанности оператора ИСПДн.
9. Обеспечение безопасности ПДн при их обработке.
10. Классификация ПДн.
11. Перечень журналов по ПДн в организации.
12. Содержание уведомления.
13. Что должно быть отражено в Положении об обработке ПДн.
14. Где размещается Политика в отношении обработки персональных данных.
15. Частная модель угроз безопасности ПДн.
16. Порядок уничтожения ПДн.
17. Сроки хранения ПДн.
18. Порядок передачи ПДн третьим лицам.
19. Что такое трансграничная передача ПДн.
20. Порядок разработки нетиповой формы, предполагающей включение ПДн
21. Определение уровней защищённости информационных систем персональных данных.
22. Требования к формам на страницах сайта, предполагающих ввод ПДн.
23. Где определяются общедоступные Пдн.
24. На кого из операторов распространяется действие 378 приказа ФСБ.
25. Какие документы представляются для подтверждения мест хранения баз данных.
26. Каков порядок одноразового пропуска на территорию организации.
27. В каких случаях не требуется согласие в договорных отношениях.

28. К чему предъявляются требования раздельного хранения.
29. В каких случаях назначаются проверки регулятора.
30. Штрафные санкции за нарушения законодательства по ПДн.