АВТОНОМНОЕ УЧРЕЖДЕНИЕ
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ
«РЕГИОНАЛЬНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ»

СОГЛАСОВАНО

Протокол № 8 от 27 апреля 2024 г.
заседания учебно-методического совета

Председатель:

_____ Л. И. Красильникова
подпись расшифровка

«27» апреля 2024 года

УТВЕРЖДАЮ
Директор
автономного учреждения
Ханты-Мансийского
автономного округа – Югры
«Региональный институт управления»

_____ В. А. Аникин
подпись расшифровка

«27» апреля 2024 года

Дополнительная профессиональная программа
повышения квалификации

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Количество академических часов: 72.

Форма обучения: очная с применением
дистанционных образовательных технологий.

Разработчик:
АУ «Региональный институт управления»

Ханты-Мансийск
2024

Программу принял(а) эксперт Отдела ДПО _____ Т. В. Чанышева

СОДЕРЖАНИЕ

1	Аннотация программы…….	3
2	Пояснительная записка…….....	4
	2.1. Актуальность……..	4
	2.2. Цели, задачи……...	4
	2.3. Планируемые результаты обучения……	5
	2.4. Требования к квалификации поступающего на обучение…….	8
3	Содержание программы……...	9
	3.1. Учебный план…….	9
	3.2. Учебно-тематический план……...	10
	3.3. Календарный учебный график…….	13
	3.4. Тематическое содержание программы…….....	14
4	Организационно-педагогические условия…….	20
	4.1. Общие требования к организации образовательного процесса…….....	20
	4.2. Требования к информационным и учебно-методическим условиям.....	20
	4.3. Требования к материально-техническим условиям……...	20
5	Аттестация…….	21
	5.1. Входное тестирование……...	21
	5.2. Итоговая аттестация……..	27
6	Литература…….	36
	6.1. Основная литература…….	36
	6.2. Дополнительная литература…….	36

АННОТАЦИЯ

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность» направлена на формирование новых и совершенствование имеющихся у государственных гражданских служащих профессиональных компетенций в сфере обеспечения информационной безопасности органов власти, необходимых для повышения эффективности их профессиональной служебной деятельности. Содержание программы направлено на освоение и совершенствование компетенций в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти.

По результатам прохождения обучения слушатели должны обладать универсальными, общепрофессиональными и профессиональными компетенциями, необходимыми государственным гражданским служащим в области защиты персональных данных, а также обладать знаниями о современной практике применения нормативных правовых актов в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти.

Программа разработана в соответствии с положениями ФГОС ВО 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденный приказом Минобрнауки России от 17.11.2020 № 1427, и ФГОС ВО 10.04.01 Информационная безопасность (уровень магистратуры), утвержденный приказом Минобрнауки России от 26.11.2020 № 1455, а также с учетом квалификационных требований, указанных в квалификационном справочнике должностей руководителей, специалистов и других служащих, утвержденном постановлением Минтруда России от 21.08.1998 № 37, «Раздел I. Общеотраслевые квалификационные характеристики должностей работников, занятых на предприятиях, в учреждениях и организациях».

Разработчики программы: АУ «Региональный институт управления»

Категория обучающихся: государственные гражданские и муниципальные служащие.

Трудоемкость программы: 72 академических часа.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Актуальность программы заключается во всё возрастающем значении информационной безопасности для безопасности личности, общества, государства и всего мирового сообщества. Программа разработана с применением модульного и системно-деятельностного подхода, формирует у слушателей необходимые на практике компетенции для исполнения законодательства в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти и ориентирована на обучение лиц, замещающих государственные должности.

Программа повышения квалификации позволит совершенствовать и (или) получить новые компетенции, необходимые для профессиональной деятельности и повысить профессиональный уровень качества и эффективности безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти.

Данный курс повышения квалификации позволяет слушателю в достаточно краткий срок освоить и развить обозначенные в программе универсальные, общепрофессиональные и профессиональные компетенции.

Цели, задачи и планируемые результаты обучения

Цель программы – повышение профессионального уровня в рамках имеющейся квалификации в сфере информационной безопасности с формированием и (или) совершенствованием системных знаний и профессиональных компетенций, необходимых для выполнения нового вида профессиональной деятельности в указанной сфере, позволяющих принимать решения и оценивать их последствия, проводить мероприятия, направленные на повышение эффективности в сфере безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти.

Задачи:

1. Повысить эффективность профессиональной служебной деятельности обучающихся в организационно-управленческой области обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти.

2. Развить у обучающихся навыки:

– применения положений законодательства Российской Федерации и нормативных правовых актов, регулирующих вопросы планирования, организации и контроля мероприятий в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти;

– применения правоприменительной и судебной практики в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти;

– оценивания применения организационных мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти;

– обоснования выбора технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти;

– использования информационных ресурсов, содержащих сведения о нормативно-правовых актах в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти;

– осуществления мониторинга изменений в нормативно-правовых актах в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти;

– осуществления мониторинга инцидентов в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти.

Планируемые результаты обучения

Программа направлена на совершенствование ряда компетенций[1].

Информационная безопасность (УК):

УК-1(М). Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

УК-2(М). Способен управлять проектом на всех этапах его жизненного цикла;

УК-3(М). Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;

УК-4(М). Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия;

Общепрофессиональные компетенции (ОПК):

ОПК-1(Б). Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-2(Б). Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-5(Б). Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

ОПК-6(Б). Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-8(Б). Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

ОПК-9(Б). Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

ОПК-10(Б). Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.

[1] Перечень компетенций определен ФГОС ВО 10.03.01 Информационная безопасность (уровень бакалавриата (Б)), утвержденный приказом Минобрнауки России от 17.11.2020 № 1427, и ФГОС ВО 10.04.01 Информационная безопасность (уровень магистратуры (М)), утвержденный приказом Минобрнауки России от 26.11.2020 № 1455

Профессиональные компетенции (ПК):

Виды деятельности	Компетенции[2]	Знать	Уметь	Владеть
информационно-методическая деятельность	УК-4(М), ОПК-5(Б), ОПК-8(Б).	– нормативные правовые акты в области защиты информации; – национальные, межгосударственные и международные стандарты в области защиты информации; – методические документы уполномоченных федеральных органов исполнительной власти по защите информации.	– применять действующую нормативную базу в области обеспечения безопасности информации; – проводить инструктаж и обучение персонала по вопросам защиты персональных данных; – использовать различные технологии и методики реализации политики обеспечения информационной безопасности; – анализировать документы стратегического планирования в части отражения в них вопросов обеспечения информационной безопасности.	– современными методами получения, обработки и анализа информации в сфере обеспечения информационной безопасности; – способностью осуществлять подбор, изучение и обобщение нормативных и методических материалов; – составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.
организационно-регулирующая деятельность	УК-1(М), УК-3(М), ОПК-1(Б), ОПК-2(Б), ОПК-6(Б), ОПК-10(Б).	– организационные меры по защите информации; – принципы построения средств защиты информации от «утечки» по техническим каналам; – критерии оценки защищенности автоматизированной системы; – технические средства контроля эффективности мер защиты информации;	– разрабатывать организационно-распорядительную документацию по защите информации; – разрабатывать предложения по совершенствованию организационных и технических мероприятий по защите информации и оценке их эффективности,	– навыками разработки муниципальных программ (подпрограмм, блоков мероприятий) в рассматриваемой сфере; – навыками планирования мероприятий по обеспечению безопасности персональных данных; – навыками организации и проведения работ по защите информации;

[2] Перечень компетенций определен ФГОС ВО 10.03.01 Информационная безопасность (уровень бакалавриата (Б)), утвержденный приказом Минобрнауки России от 17.11.2020 № 1427, и ФГОС ВО 10.04.01 Информационная безопасность (уровень магистратуры (М)), утвержденный приказом Минобрнауки России от 26.11.2020 № 1455

		– основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах; – основные методы управления защитой информации; – обязательные и рекомендуемые мероприятия в сфере обеспечения информационной безопасности.	совершенствованию системы защиты информации; – классифицировать и оценивать угрозы безопасности информации; – применять технические средства контроля эффективности мер защиты информации; – осуществлять текущее планирование мероприятий в сфере обеспечения информационной безопасности.	
исполнительно-распорядительная деятельность	УК-2(М), ОПК-5(Б), ОПК-9(Б).	– нормативные правовые акты в области защиты информации; – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах; – основные методы управления защитой информации.	– применять уместно знания правых норм в сфере обеспечения информационной безопасности.	– приёмами выбора эффективных управленческих технологий в сфере обеспечения информационной безопасности.

Требования к квалификации поступающего на обучение

К освоению данной программы повышения квалификации допускаются государственные служащие всех категорий и групп должностей, лица, замещающие муниципальные должности, муниципальные служащие, имеющие или получающие среднее профессиональное и (или) высшее образование.

СОДЕРЖАНИЕ ПРОГРАММЫ

(72 академических часа)

Учебный план

(1 академический час – 45 минут)

№	Раздел, модуль	Всего часов	Очное обучение		Дистанционное обучение		Форма контроля и аттестации	Формируемые компетенции
			Лекции	Практические занятия	Лекции	Практические занятия		
1.	Модуль 1. Правовое, нормативное и методическое обеспечение информационной безопасности органов власти	9	-	-	3	6	Входное тестирование, практикумы, изучение законодательства	УК-1(М) УК-4(М) ОПК-1(Б) ОПК-5(Б)
2.	Модуль 2. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти	25	2	3	6	14	Практикумы, разработка документов, дискуссия, разбор кейсов	УК-1(М) УК-2(М) УК-3(М) ОПК-1(Б) ОПК-6(Б) ОПК-8(Б) ОПК-10(Б)
3.	Модуль 3. Информационные системы	15,5	1	2,5	4	8	Практикумы, разработка документов, разбор кейсов	УК-1(М) УК- 4(М) ОПК-2(Б) ОПК-9(Б)
4.	Модуль 4. Система защиты информации	22,5	2	5,5	5	10	Практикумы, решение кейсов, разработка документов, круглый стол	УК-1(М) УК-2(М) УК-3(М) ОПК-1(Б) ОПК-2(Б) ОПК-5(Б) ОПК-6(Б) ОПК-9(Б)
ИТОГО		**72**	**5**	**11**	**18**	**38**		

Учебно-тематический план – 72 академических часа

№	Раздел, модуль	Всего часов	Очное обучение		Дистанционное обучение		Форма контроля и аттестации	Формируемые компетенц
			Лекции	Практические занятия	Лекции	Практические занятия		
1.	**Модуль 1. Правовое, нормативное и методическое обеспечение информационной безопасности органов власти**	**9**	**-**	**-**	**3**	**6**	**Входное тестирование (20 вопросов), практикумы, обмен опытом, решение задач, кейсов**	**УК-1(М) УК-4(М) ОПК-1(Б) ОПК-5(Б)**
1.1.	Тема 1.1. Основные понятия и принципы. Объекты и субъекты информационной безопасности в органах власти	3	-	-	1	2	Практикум, изучение законодательства	УК-1(М) ОПК-1(Б)
1.2.	Тема 1.2. Система нормативных правовых актов по вопросам информационной безопасности	3	-	-	1	2	Практикум, изучение законодательства	ОПК-5(Б)
1.3.	Тема 1.3. Методические документы и национальные стандарты в области защиты информации	3	-	-	1	2	Практикум, изучение законодательства	УК-4(М) ОПК-5(Б)
2.	**Модуль 2. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти**	**25**	**2**	**3**	**6**	**14**	**Практикумы, разработка документов, дискуссия, разбор кейсов**	**УК-1(М) УК-2(М) УК-3(М) ОПК-1(Б) ОПК-6(Б) ОПК-8(Б) ОПК-10(Б)**
2.1.	Тема 2.1. Персональные данные. Принципы и условия их обработки	6,5	-	0,5	2	4	Практикум, разработка документов, дискуссия	УК-1(М) ОПК-1(Б)
2.2.	Тема 2.2. Права субъекта персональных данных и обязанности оператора персональных данных	3,5	-	0,5	1	2	Практикум, разработка документов, разбор кейсов	УК-1(М) ОПК-10(Б)
2.3.	Тема 2.3. Требования по обеспечению	3,5	-	0,5	1	2	Практикум, разработка	УК-3(М) ОПК-6(Б)

	безопасности персональных данных						документов, разбор кейсов	
2.4.	Тема 2.4. Разработка локальных актов и иных документов оператора по вопросам обработки персональных данных	4,5	1	0,5	1	2	Практикум, разработка документов, разбор кейсов	УК-2(М) ОПК-8(Б)
2.5.	Тема 2.5. Контроль и надзор за обработкой персональных данных. Порядок проведения контрольных мероприятий регулятором	7	1	1	1	4	Практикум, разработка документов, разбор кейсов	УК-1(М) ОПК-1(Б)
3.	**Модуль 3. Информационные системы**	**15,5**	**1**	**2,5**	**4**	**8**	**Практикумы, разработка документов, разбор кейсов**	**УК-1(М) УК- 4(М) ОПК-2(Б) ОПК-9(Б)**
3.1	Тема 3.1. Угрозы безопасности информации. Модели угроз и нарушителя безопасности информации	7,5	0,5	1	2	4	Практикум, разработка документов, разбор кейсов	УК-1(М) ОПК-2(Б)
3.2	Тема 3.2. Государственные информационные системы: порядок создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации и дальнейшего хранения содержащейся в их базах данных информации	3,5	-	0,5	1	2	Практикум, разработка документов, разбор кейсов	УК- 4(М) ОПК-2(Б)
3.3	Тема 3.3. Классификация информационной системы по требованиям защиты информации	4,5	0,5	1	1	2	Практикум, разработка документов, разбор кейсов	УК-1(М) ОПК-9(Б)
4.	**Модуль 4. Система защиты информации**	**22,5**	**2**	**5,5**	**5**	**10**	**Практикумы, решение кейсов, разработка документов, круглый стол**	**УК-1(М) УК-2(М) УК-3(М) ОПК-1(Б) ОПК-2(Б) ОПК-5(Б) ОПК-6(Б) ОПК-9(Б)**

	Тема 4.1. Виды и типы средств защиты информации. Порядок применения средств защиты информации	3,5	-	0,5	1	2	Практикум, решение кейсов	УК-1(М) ОПК-9(Б)
	Тема 4.2. Разработка (проектирование) и внедрение системы защиты информации информационной системы	4,5	1	0,5	1	2	Практикум, разработка документов, разбор кейсов	УК-2(М) ОПК-2(Б)
	Тема 4.3. Требования к защите информации в информационной системе. Аттестация информационной системы. Сертификация средств защиты	3,5	-	0,5	1	2	Практикум, разработка документов, разбор кейсов	ОПК-6(Б) ОПК-9(Б)
	Тема 4.4. Порядок осуществления контроля за соблюдением требований к размещению технических средств информационных систем, используемых органами власти на территории Российской Федерации	5	1	1	1	2	Практикум, решение кейсов	УК-3(М) ОПК-5(Б)
	Тема 4.5. Обеспечение информационной безопасности при использовании государственными гражданскими и муниципальными служащими социальных сетей, почтовых и иных интернет-сервисов	4	-	1	1	2	Практикум, круглый стол	ОПК-1(Б) ОПК-5(Б)
	Итоговая аттестация	2		2			Итоговое тестирование (30 вопросов), решение итогового кейса	
ИТОГО		**72**	**5**	**11**	**18**	**38**		

Календарный учебный график

Общий объём программы – 72 академических часа. Занятия проводятся очно с применением дистанционных технологий в будние дни (16 дней), из них:

– с применением дистанционных технологий - 14 дней по 4 академических часов в день (итого 56 академических часов);

– очно - 2 дня по 8 академических часов в день (итого 16 академических часов).

Срок обучения	недели	1	2					3					4				
	дни	1	2	3	4	5	6	7	8	9	10	11	12	13	14	1	2
виды занятий, предусмотренные ДПП		ДО	ДО	ДО	ДО	ДО	ДО	ДО	ДО	ДО	ДО	ДО	ДО	ДО	ДО	А	А
количество часов		4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	4 ч.	8 ч.	8 ч.
Тема 1.1.		3															
Тема 1.2.		1	2														
Тема 1.3.			2	1													
Тема 2.1.				3	3											0,5	
Тема 2.2.					1	2										0,5	
Тема 2.3.						2	1									0,5	
Тема 2.4.							3									1,5	
Тема 2.5.								4	1							2	
Тема 3.1.									3	3						1,5	
Тема 3.2.										1	2					0,5	
Тема 3.3.											2	1				1	0,5
Тема 4.1.												3					0,5
Тема 4.2.													3				1,5
Тема 4.3.													1	2			0,5
Тема 4.4.														2	1		2
Тема 4.5.															3		1
																	И - 2

ДО – изучение материала и выполнение практических заданий в системе дистанционного обучения.

А – аудиторные занятия.

И – итоговая аттестация.

Тематическое содержание
дополнительной профессиональной программы повышения квалификации
«Информационная безопасность»

Модуль 1.
Правовое, нормативное и методическое обеспечение информационной безопасности органов власти – 9 академических часов (лекции – 3 академических часа, практическая работа – 6 академических часов)

Тема 1.1. Основные понятия и принципы. Объекты и субъекты информационной безопасности в органах власти – 3 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 2 часа (дистанционно).

Общие понятие «информационная безопасность» в законодательстве Российской Федерации и практика его применения в органах государственной власти и организациях независимо от формы их собственности. Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных в Российской Федерации. Основные положения ФЗ-152 «О персональных данных», на что обратить внимание.

Практическая работа – 2 академических часа (дистанционно):

1. Решение входного тестирования – 1 академический час.
2. Практикум. Изучите изменения в нормативных документах. Обратите внимание на Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» – 1 академический час.

Тема 1.2. Система нормативных правовых актов по вопросам информационной безопасности – 3 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 2 часа (дистанционно).

Конституция Российской Федерации. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ. Уголовная и административная ответственность за нарушение законодательства в информационной сфере.

Практическая работа – 2 академических часа (дистанционно):

Изучив нормативные документы, заполните таблицу.

Правовой документ	Год принятия	Объекты регулирования/ гарантии	Статьи, связанные с информационной безопасностью

Тема 1.3. Методические документы и национальные стандарты в области защиты информации – 3 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 2 часа (дистанционно).

Основные организационно-правовые и методические документы по обеспечению технической защиты информации в Российской Федерации. Федеральные законы РФ, постановления Правительства РФ, указы Президента РФ, руководящие документы ФСТЭК, ФСБ.

Практическая работа – 2 академических часа (дистанционно):

Изучите стандарты в сфере обеспечения информационной безопасности https://fstec.ru/dokumenty/vse-dokumenty/perechni/natsionalnye-standarty и заполните таблицу.

Название документа	Дата принятия	Объекты регулирования/ гарантии	Статьи, связанные с информационной безопасностью

Модуль 2.
Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в органах власти – 25 академических часов (лекции – 8 академических часов, практическая работа – 17 академических часов)

Тема 2.1. Персональные данные. Принципы и условия их обработки – 6,5 академических часа, из которых лекции – 2 часа (дистанционно), практическая работа – 4,5 часа (4 – дистанционно, 0,5 – очно).

Персональные данные (далее – ПДн). Классификация действий с ПДн. Обработка ПДн. Способы, принципы и условия обработки ПДн.

Практическая работа – 4,5 академических часа, из которых:

1. Определите перечень локальных документов, необходимых для обеспечения информационной безопасности в вашей организации. Составьте их проекты/шаблоны. Ответ на задание в свободной форме – 4 академических часа (дистанционно).
2. Дискуссия по теме «Персональные данные. Принципы и условия их обработки» – 0,5 академических часа (очно).

Тема 2.2. Права субъекта персональных данных и обязанности оператора персональных данных – 3,5 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 2,5 часа (2 – дистанционно, 0,5 – очно).

Права субъекта персональных данных. Обязанности оператора персональных данных. Обеспечение сохранности конфиденциальных сведений при их обработке. Действие федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Практическая работа – 2,5 академических часа, из которых:

1. Определите, в каких локальных документах должны быть закреплены права и обязанности субъектов и операторов персональных данных в вашей организации. Составьте их проекты/шаблоны. Ответ на задание в свободной форме – 2 академических часа (дистанционно).
2. Разбор кейсов по теме «Права субъекта персональных данных и обязанности оператора персональных данных» – 0,5 академических часа (очно).

Тема 2.3. Требования по обеспечению безопасности персональных данных – 3,5 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 2,5 часа (2 – дистанционно, 0,5 – очно).

Нормативно-правовая база по обеспечению безопасности персональных данных. Типичные угрозы, которые могут причинить вред гражданину при утечке ПДн. Уровни защищенности. Основные требования к защищенности. Основные этапы защиты ПДн.

Практическая работа – 2,5 академических часа, из которых:

1. Составьте пошаговый план защиты персональных данных в вашей организации. Ответ на задание в свободной форме – 2 академических часа (дистанционно).

2. Разбор кейсов по теме «Требования по обеспечению безопасности персональных данных» – 0,5 академических часа (очно).

Тема 2.4. Разработка локальных актов и иных документов оператора по вопросам обработки персональных данных – 4,5 академических часа, из которых лекции – 2 часа (1 – дистанционно, 1 – очно), практическая работа – 2,5 часа (2 – дистанционно, 0,5 – очно).

Нормативно-правовая база организации по обеспечению безопасности персональных данных. Перечень документов для надлежащей обработки персональных данных. Отчетная документация о защите ПДн.

Практическая работа – 2,5 академических часа, из которых:

1. Проанализируйте имеющиеся в вашей организации локальные акты и иные документы оператора по вопросам обработки персональных данных и разработайте проекты недостающих или требующих изменений документов – 2 академических часа (дистанционно).

2. Разбор кейсов по теме «Разработка локальных актов и иных документов оператора по вопросам обработки персональных данных» – 0,5 академический час (очно).

Тема 2.5. Контроль и надзор за обработкой персональных данных. Порядок проведения контрольных мероприятий регулятором – 7 академических часов, из которых лекции – 2 часа (1 – дистанционно, 1 – очно), практическая работа – 5 часов (4 – дистанционно, 1 – очно).

Государственный контроль за обработкой ПДн. Нормы ответственности нарушения требований обработки ПДН. Плановые и внеплановые проверки. Организация проведения проверок. Роскомнадзор – гарант соблюдения оператором требований законодательства об обработке персональных данных. Обязанности Роскомнадзора по проверке общих требований законодательства по защите персональных данных.

Практическая работа – 5 академических часа, из которых:

1. Проанализируйте имеющиеся в вашей организации локальные акты и иные документы оператора по вопросам обработки персональных данных, оцените их с позиции проверяющего и устраните выявленные недоработки – 4 академических часа (дистанционно).

2. Разбор кейсов по теме «Контроль и надзор за обработкой персональных данных» – 1 академических часа (очно).

Модуль 3.
Информационные системы – 15,5 академических часа
(лекции – 5 академических часов, практическая работа – 10,5 академических часа)

Тема 3.1. Угрозы безопасности информации. Модели угроз и нарушителя безопасности информации – 7,5 академических часа, из которых лекции – 2,5 часа (2 – дистанционно, 0,5 – очно), практическая работа – 5 часов (4 – дистанционно, 1 – очно).

Угрозы безопасности информации. Классификация нарушителей. Анализ вероятности реализации угрозы и ущерба от ее возникновения. Процесс анализа угроз информации. Источник риска. Зона риска. Гипотетический злоумышленник. Вероятность реализации риска. Степень ущерба от его реализации. Соотношение расходов, необходимых для минимизации риска, и убытка, причиняемого в случае его реализации.

Модели угроз и нарушителя безопасности информации.

Практическая работа – 5 академических часа, из которых:

1. Разработайте модель угроз информационной безопасности для вашей организации. Ответ на задание представьте в свободной форме – 4 академических часа (дистанционно).

2. Разбор кейсов по теме «Угрозы безопасности информации» – 1 академических часа (очно).

Тема 3.2. Государственные информационные системы: порядок создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации и дальнейшего хранения содержащейся в их базах данных информации – 3,5 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 2,5 часа (2 – дистанционно, 0,5 – очно).

Государственные информационные системы: порядок создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации и дальнейшего хранения содержащейся в их базах данных информации. Требования, которые должны осуществляться при создании, развитии, вводе в эксплуатацию, эксплуатации и выводе из эксплуатации ГИС. Требования регуляторов ФСБ и ФСТЭК. Требования к организации и мерам защиты информации, содержащейся в ГИС.

Практическая работа – 2,5 академических часа, из которых:

1. Изучите постановление Правительства РФ от 06.07.2015 № 676 «Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» – 2 академических часа (дистанционно).

2. Разбор кейсов по теме «Государственные информационные системы» – 0,5 академических часа (очно).

Тема 3.3. Классификация информационной системы по требованиям защиты информации – 4,5 академических часа, из которых лекции – 1,5 часа (1 – дистанционно, 0,5 – очно), практическая работа – 3 часа (2 – дистанционно, 1 – очно).

Государственные информационные системы. Типы информационных систем. Класс защищенности информационных систем. Автоматизированная система и ее классы защищенности.

Параметры определения класса защищённости. Масштаб (федеральный, региональный, объектовый). Уровень значимости. Определение степени ущерба от нарушения конфиденциальности, целостности, доступности.

Практическая работа – 3 академических часа, из которых:

1. Изучите и определите классы и уровни защищенности информационных систем в вашей организации. Ответ представьте в свободной форме – 2 академических часа (дистанционно).

2. Разбор кейсов по теме «Классификация информационной системы по требованиям защиты информации» – 1 академический час (очно).

Модуль 4.
Система защиты информации – 22,5 академических часа
(лекции – 7 академических часов, практическая работа – 15,5 академических часа)

Тема 4.1. Виды и типы средств защиты информации. Порядок применения средств защиты информации – 3,5 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 2,5 часа (2 – дистанционно, 0,5 – очно).

Средства защиты от несанкционированного доступа (СЗИ от НСД). Модуль доверенной загрузки. Межсетевые экраны (Файрволы, МЭ). Системы обнаружения вторжений (СОВ – IDS). Системы анализа уязвимостей (сканеры уязвимостей). Системы мониторинга безопасности (SIEM). Системы антивирусной защиты информации (САВЗ). Системы предотвращения утечек информации (DLP). Средства криптографической защиты информации (СКЗИ). Средства унифицированного управления угрозами (UTM).

Практическая работа – 2,5 академических часа, из которых:

1. Изучите процесс установки Secret Net Studio 8.8., определите преимущества и недостатки данной программы – 2 академических часа (дистанционно).
2. Разбор кейсов по теме «Виды и типы средств защиты информации» – 0,5 академических часа (очно).

Тема 4.2. Разработка (проектирование) и внедрение системы защиты информации информационной системы – 4,5 академических часов, из которых лекции – 2 часа (1 – дистанционно, 1 – очно), практическая работа – 2,5 часа (2 – дистанционно, 0,5 – очно).

Создания системы защиты информации. Формирование требований к системе защиты информации (предпроектный этап). Разработка системы защиты информации (этап проектирования). Внедрение системы защиты информации (этап установки, настройки, испытаний). Подтверждение соответствия системы защиты информации (этап оценки).

Практическая работа – 2,5 академических часа, из которых:

1. На примере вашей организации опишите поэтапное внедрение системы защиты информации информационной системы – 2 академических часа (дистанционно).
2. Разбор кейсов по теме «Внедрение системы защиты информации информационной системы» – 0,5 академических часа (очно).

Тема 4.3. Требования к защите информации в информационной системе. Аттестация информационной системы. Сертификация средств защиты – 3,5 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 2,5 часа (2 – дистанционно, 0,5 – очно).

Аттестация ГИС: подготовка, порядок действий, нововведения. Постановление Правительства РФ № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации». Сертификация средств защиты информации. Построение системы защиты информации в организации. Контроль состояния защиты информации.

Практическая работа – 2,5 академических часа, из которых:

1. Провести анализ процессов и соответствующих документов по сертификации средств защиты и аттестации информационных систем в вашей организации. Сформировать краткий отчет. Ответ представить в свободной форме – 2 академических часа (дистанционно).
2. Разбор кейсов по теме «Требования к защите информации в информационной системе» – 0,5 академических часа (очно).

Тема 4.4. Порядок осуществления контроля за соблюдением требований к размещению технических средств информационных систем, используемых органами власти на

территории Российской Федерации – 5 академических часов, из которых лекции – 2 часа (1 – дистанционно, 1 – очно), практическая работа – 3 часа (2 – дистанционно, 1 – очно).

Виды контроля состояния системы защиты информации. Оценка состояния защищенности локальной вычислительной сети. Оценка уязвимостей. Рекомендации по содержанию отчета по результатам тестирования на проникновение контроля.

Практическая работа – 3 академических часа, из которых:

1. Изучите, что такое контроль средств защиты информации и составьте проект методики программных испытаний для СЗИ в вашей организации – 2 академических часа (дистанционно).
2. Разбор кейсов по теме «Порядок осуществления контроля за соблюдением требований к размещению технических средств информационных систем, используемых органами власти на территории Российской Федерации» – 1 академический час (очно).

Тема 4.5. Обеспечение информационной безопасности при использовании государственными гражданскими и муниципальными служащими социальных сетей, почтовых и иных интернет-сервисов – 4 академических часа, из которых лекции – 1 час (дистанционно), практическая работа – 3 часа (2 – дистанционно, 1 – очно).

Обеспечение информационной безопасности при использовании государственными гражданскими и муниципальными служащими социальных сетей, почтовых и иных интернет-сервисов. Действие федерального закона от 29.12.2022 № 584-ФЗ. Список запрещенных на 1 марта 2023 года мессенджеров. Правила защиты от интернет-мошенничества. Правила безопасного пользования интернетом.

Практическая работа – 3 академических часа, из которых:

1. Составьте проект локального документа, закрепляющего правила по обеспечению информационной безопасности при использовании государственными гражданскими и муниципальными служащими социальных сетей, почтовых и иных интернет-сервисов с учетом действующих с 1 марта 2023 года ограничений Роскомнадзора – 2 академических часа

2. Круглый стол – 1 академический час (очно).

Итоговая аттестация – 2 академических часа (очно):
решение итогового кейса – 1 час,
решение итогового тестирования – 1 час.

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

1. Общие требования к организации образовательного процесса

Условия проведения.

Для дистанционной части курса необходимо:

а) разместить электронный учебно-методический комплекс курса в системе дистанционного обучения, доступный слушателям для копирования без каких-либо ограничений;

б) осуществлять эффективную коммуникацию слушателей с преподавателем, куратором курса. Доступ к ресурсу слушатели получают после регистрации и прохождении входного тестирования. Доступ к ресурсу закрывается по завершении курса.

Для очной части курса необходимы:

а) аудитория с учебными местами по количеству слушателей в группе, удовлетворяющая санитарно-гигиеническим требованиям, правилам пожарной безопасности и охраны здоровья слушателей;

б) питьевая вода (из расчета 0,5 л питьевой воды на 1 слушателя в день при проведении занятий);

в) блокноты и ручки для слушателей.

Образовательные технологии:

– ИКТ-технологии (система дистанционного обучения, презентации в PowerPoint на очной части курса, раздаточный материал на дисках);
– технологии группового обучения;
– технологии интерактивного и модульного обучения;
– тренинговые и игровые технологии обучения;
– кейс-стади технология;
тестирование.

2. Требования к информационным и учебно-методическим условиям

а) программное обеспечение и Интернет-ресурсы:
– PowerPoint, Word, Excel;
б) комплекты методических материалов на электронном носителе.

3. Требования к материально-техническим условиям

Перечень основного материально-технического обеспечения (ТСО и компьютерная техника, оборудование, приборы и т.п.):

а) для дистанционной части слушателю необходим компьютер, подключение к сети Интернет;

б) для очной части курса необходимы:

– ноутбук, подключенный к проектору;
– стулья по количеству участников;
– столы, которые возможно переставлять на усмотрение преподавателя;
– флип-чарт и маркеры;
– белая бумага А4.

Требования к аудитории (для очной части занятий: количество посадочных мест в помещении и пр.):

– аудитория с учебными местами по количеству слушателей в группе, удовлетворяющая санитарно-гигиеническим требованиям, правилам пожарной безопасности и охраны здоровья слушателей.

АТТЕСТАЦИЯ

Форма аттестации – тестирование. Аттестация заключается в прохождении двух видов тестирования – входного и итогового, и в решении итогового кейса.

Входное тестирование включает в себя 30 вопросов по теме курса, оценивает начальный уровень обучающегося. Обучающийся отвечает на 20 вопросов.

При прохождении входного тестирования:

Объект оценки	Показатели оценки	Критерии оценки
Результаты тестирования	Количество верных ответов	«зачтено» выставляется при наличии 50 % и более правильных ответов; «не зачтено» – при результате менее 50 %

Итоговое тестирование по всей тематике программы включает 40 вопросов по теме курса. Обучающийся отвечает на 30 тестовых вопросов.

При прохождении итогового тестирования:

Объект оценки	Показатели оценки	Критерии оценки
Результаты тестирования	Количество верных ответов	«отлично» выставляется при наличии 94 % и более правильных ответов; «хорошо» – при результате 84% и более; «удовлетворительно» – при результате 75% и более; «неудовлетворительно» – при результате менее 75%.

Процесс тестовых измерений предельно стандартизируется:

- заранее разработанная система подсчета баллов применяется ко всем слушателям одинаково;
- все слушатели отвечают на задания одинаковой сложности.

Слушателям, полностью прошедшим обучение, промежуточные и/или итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца по программе «Информационная безопасность».

ВХОДНОЕ ТЕСТИРОВАНИЕ

(обучающийся отвечает на 20 вопросов из 30)

1. Автоматизированная обработка персональных данных – это…

а) обработка персональных данных с использованием средств автоматизации;

б) обработка персональных данных с помощью средств вычислительной техники;

в) обработка персональных данных пользователя с применением компьютера.

2. Информация – это…

а) любые данные, представленные на материальном носителе;

б) сведения, принадлежащие кому-либо и защищаемые законом;

в) сведения (сообщения, данные), независимо от формы их представления.

3. Информационная система персональных данных – это…

а) пользователь, средства автоматизации, базы данных;

б) контролируемое пространство, в котором происходит обработка персональных данных;

в) совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4. Безопасность персональных данных – это…

а) состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

б) состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность персональных данных;

в) состояние защищенности персональных данных, характеризуемое способностью технических средств обеспечить конфиденциальность персональных данных.

5. Блокирование персональных данных – это…

а) временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

б) временное прекращение обработки персональных данных;

в) временное прекращение обработки персональных данных для уточнения персональных данных.

6. Доступ к информации – это…

а) возможность получения информации и ее использования;

б) возможность использования информации;

в) возможность доступа к информации;

г) возможность доступа к информации, но не ее использования.

7. Целью Федерального закона от 27.07.2006 № 152-ФЗ является…

а) контроль за обработкой персональных данных операторами персональных данных;

б) обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных;

в) соответствия законодательства РФ в сфере персональных данных Конвенции Совета Европы от 1981года.

8. Защищаемая информация – это…

а) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

б) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации;

в) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов;

г) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями Федерального закона «О защищаемой информации в Российской Федерации».

9. Что понимается под понятием «Конфиденциальность персональных данных»?

а) Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных;

б) Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом;

в) Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных или наличия иного законного основания.

10. Оператор при сборе персональных данных через свой официальный сайт обязан в соответствии с ч.2 ст.18.1 152-ФЗ на сайте опубликовать документы:

а) Политику в отношении обработки персональных данных;

б) Политику в отношении обработки персональных данных, Пользовательское соглашение;

в) Политику в отношении обработки персональных данных, Пользовательское соглашение, Согласие пользователя.

11. Общедоступные персональные данные – это…

а) персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных;

б) Пперсональные данные, доступ неограниченного круга лиц к которым предоставлен в соответствии с федеральными законами;

в) персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

12. Специальные категории персональных данных – это…

а) персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

б) персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни;

в) персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни;

г) персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости.

13. Трансграничная передача персональных данных – это…

а) передача персональных данных на территорию иностранного государства;

б) передача персональных данных на территорию другого субъекта РФ органу власти данного субъекта, физическому лицу или юридическому лицу данного субъекта РФ;

в) передача персональных данных на территорию иностранного государства или органу власти иностранного государства;

г) передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

14. Целостность информации – это…

а) состояние информации, при котором отсутствует любое ее изменение;

б) состояние информации, при котором изменение осуществляется только преднамеренно субъектами, имеющими на него право;

в) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

15. Что такое персональные данные?

а) Любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

б) Информация о частной жизни физического лица, доступ к которой он решил ограничить;

в) Сведения о религиозных убеждениях, политических взглядов, расовой и национальной принадлежности субъекта персональных данных;

г) Любые сведения независимо от формы их представления.

16. Оператор персональных данных – это…

а) государственный орган, осуществляющий автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке;

б) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

в) юридическое лицо, осуществляющее автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке;

г) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, но не определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

17. Обработка персональных данных – это…

а) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение,

уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных);

б) сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, осуществляемые с помощью средств вычислительной техники;

в) чтение, запись, сортировка, модификация, передача персональных данных в информационной системе.

18. Распространение персональных данных – это…

а) действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

б) действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

в) передача персональных данных оператору персональных данных.

19. Предоставление персональных данных – это…

а) действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

б) действия, направленные на раскрытие персональных данных по мотивированному запросу.

20. Уничтожение персональных данных – это…

а) действия, в результате которых становится невозможно определить субъекта персональных данных в информационной системе персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

в) удаление персональных данных из информационной системы персональных данных;

г) действия, направленные на уничтожение носителей персональных данных.

21. Обезличивание персональных данных – действия, в результате которых…

а) невозможно распространять персональные данные;

б) невозможно выполнять сбор персональных данных;

в) выполняется уничтожение персональных данных в информационной системе;

г) становится невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

22. Что такое биометрические персональные данные?

а) Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных;

б) Сведения, которые характеризуют физиологические особенности человека, на основании которых можно установить его личность;

в) Сведения, которые характеризуют биологические особенности человека, на основании которых можно установить его личность.

23. Законодательство Российской Федерации в области персональных данных состоит из:

а) ФЗ «О Государственной тайне»;

б) ФЗ «Об электронной цифровой подписи»;

в) ФЗ «О персональных данных»;

г) ФЗ, ПП и НПА уполномоченных органов государственной власти РФ в сфере информации и персональных данных.

24. Каким нормативно правовым актом Российской Федерации установлены «Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных»?

а) Постановлением Правительства РФ от 13 февраля 2019 г. № 146;

б) Приказом Минкомсвязи РФ от 21 января 2019 г. № 10;

в) Приказом Роскомнадзора от 30 октября 2018 г. № 159.

25. Какая статья Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» обязывает каждого оператора внести «сведения о месте нахождения базы данных, содержащих персональные данные» в Уведомление об обработке персональных данных?

а) п.10.1 ч.3 ст.22

б) ч.2 ст.18.1

26. В случае изменений сведений в Уведомлении, оператор обязан направить Информационное письмо об изменениях в Управление Роскомнадзора региона в течение…

а) 30 дней с даты изменений;

б) 10 дней с даты изменений.

27. На какие отношения не распространяется действие Федерального закона «О персональных данных»?

а) На отношения, возникающие при обработке персональных данных физическими лицами, исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

б) На отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

в) На организацию хранения, комплектования, учета и использования архивных документов в соответствии с законодательством об архивном деле в РФ

г) Не распространяется на все перечисленных варианта.

28. Оператор персональных данных (Несколько вариантов ответа):

а) Физическое лицо;

б) Юридическое лицо;

в) Муниципальный орган;

г) Государственный орган;

д) Гражданин;

е) Государственный служащий.

29. Перед кем оператор персональных данных несет ответственность?

а) Перед субъектом персональных данных;

б) Перед Роскомнадзором;

г) Перед вышестоящей организацией.

30. На какие отношения распространяется действие Федерального закона «О персональных данных»?

а) На отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

б) На отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

в) На отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами;

г) Распространяется на все перечисленные варианты.

ИТОГОВОЕ ТЕСТИРОВАНИЕ

(обучающийся отвечает на 30 вопросов из 40)

1. В какой орган нужно отправить Уведомление об обработке персональных данных?

а) Администрация города;

б) Департамент информационных технологий;

в) Управление Роскомнадзора;

г) Роскомнадзор РФ.

2. Перед передачей ПДн субъекта на территорию другого государства оператор…

а) получает согласие на передачу ПДн от субъекта;

б) принимает самостоятельно решение о передаче ПДн субъекта;

в) выясняет относится ли данная страна к государствам, обеспечивающим адекватную защиту персональных данных.

3. С какого времени базы данных с персональными данными должны храниться только на территории РФ?

а) с 1 января 2016 года

б) с 1 сентября 2015 года

в) с 1 июля 2015 года.

4. Какой срок в соответствии с ФЗ-152 предусмотрен для сообщения субъекту (его представителю) Оператором информации о наличии ПДн и предоставить возможность ознакомления с ними?

а) В течение 7 дней;

б) В течение 30 дней;

в) В течение 10 рабочих дней;

г) В течение 14 дней.

5. В течение какого времени со дня получения запроса Оператор обязан предоставить в Управление Роскомнадзора необходимую информацию?

а) В течение 10 дней;

б) В течение 7 рабочих дней;

в) В течение 10 рабочих дней;

г) Срок предоставления документов не ограничен.

6. В случае отзыва субъектом ПДн согласия на обработку своих ПДн, оператор обязан прекратить обработку ПДн, и, если сохранение ПДн более не требуется для целей обработки, уничтожить ПДн в срок, не превышающий с даты поступления указанного отзыва…

а) 10 рабочих дней;

б) 7 дней;

в) 20 дней;

г) 10 рабочих дней.

7. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором, оператор обязан прекратить неправомерную обработку ПДн с даты этого выявления в срок, не превышающий…

а) 7 рабочих дней;

б) 3 рабочих дней;

в) 10 рабочих дней;

г) 30 дней.

8. В случае достижения цели обработки ПДн оператор обязан прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий с даты достижения цели обработки ПДн…

а) 10 дней;

б) 30 дней;

в) 10 рабочих дней.

9. Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных…

а) в течение 3 рабочих дней после начала обработки ПДн;

б) в течение 4 рабочих дней после начала обработки ПДн;

в) до начала обработки ПДн;

г) в течение 7 рабочих дней после начала обработки ПДн.

10. Если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные в срок не превышающий…

а) 7 рабочих дней;

б) 10 рабочих дней;

в) 15 дней;

г) 30 рабочих дней.

11. Какие меры по обеспечению безопасности персональных данных при неавтоматизированной обработке являются обязательными в соответствии с постановлением Правительства РФ от 15.09.2008г. № 687?

а) Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

б) Использование средств контроля и управлении доступом;

в) Использование запираемых шкафов, сейфов и решеток на окнах;

г) Должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, устанавливаются оператором.

12. Государственный контроль и надзор в сфере персональных данных, в соответствии с постановлением Правительства № 146 проводится посредством: (вопрос с множественным выбором)

а) Плановых и внеплановых проверок;

б) Принятия мер по пресечению и устранению выявленных нарушений;

в) Проведения мероприятий по контролю без взаимодействия с операторами;

г) Проведения мероприятий по профилактике нарушений;

д) Проведением мероприятий по контролю за распространением ПДн.

13. Каким Федеральным законом и с какого времени контроль и надзор за обработкой персональных данных выведен из под 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного и муниципального контроля?

а) 149-ФЗ с 1 декабря 2016 г.;

б) 242-ФЗ с 1 сентября 2015 г.

14. В каком случае фотографию можно отнести к биометрическим персональным данным? (вопрос с множественным выбором)

а) В случае, если копия паспорта с фотографией находиться в личном деле сотрудника;

б) В случае если фотография зарегистрирована в СКУД (система контроля и управления доступом, т.е. проходная завода);

в) В случае если эта фотография сделана в публичном месте;

г) В случае, если гражданин проходит паспортный контроль в зелёной зоне аэропорта.

15. Подумайте, какие из перечисленных вариантов относятся к общедоступным персональным данным? Вопрос с множественным выбором (правильных здесь 8 ответов).

а) Объявление на сайте «Авито» с контактными данными продавца;

б) Контактные данные клиентов;

в) Доска почёта с лучшими работниками месяца в компании Газпром;

г) Паспортные данные гражданина;

д) Визитная карточка с ФИО, должностью, номером телефона руководителя;

е) Фамилия, имя, отчество;

ё) Фотография директора по качеству в магазине «Пятерочка»;

ж) Фотографии воспитанников на странице педагога в социальной сети «Вконтакте»;

з) Поздравление с Днем Рождения работника предприятия на стенде;

и) Фотография губернатора на дорожном щите.

16. Подумайте, какие ситуации из перечисленных относятся к неавтоматизированному виду обработки персональных данных? Ответ с множественным выбором (Правильных 5 ответов).

а) Выдача талона к врачу в регистратуре;

б) Трудовой договор в личном деле работника;

в) Распечатка бейджев участникам конференции;

г) Создание макета визиток для сотрудников компании в типографии;

д) Одноразовый пропуск в помещение;

е) Командировочные удостоверения сотрудников в папке на компьютере.

17. Какой размер штрафа установлен для организации по ст. 13.11.КоАП за не опубликование политики по обработке и защите персональных данных?

а) 10 000 – 15 000 рублей;

б) 15 000 – 30 000 рублей;

в) 20 000 – 50 000 рублей;

г) нет правильного ответа.

18. Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных в соответствии с постановлением Правительства РФ от 12.02.2019 г. № 146 определяют…

а) Порядок организации и проведения проверок операторов ПДн;

б) Порядок контроля и надзора за выполнением организационных и технических мер по обеспечению безопасности ПДн в ИСПДн, установленных в соответствии со ст.19.ФЗ-152;

в) нет правильного ответа.

19. Управление Роскомнадзора региона, в соответствии с постановлением Правительства РФ от 12.02.2019 г. № 146 согласует с органами прокуратуры внеплановые проверки…

а) по результатам обращения граждан, поступивших в Роскомнадзор;

б) в случае неисполнения оператором предписания Роскомнадзора;

в) по результатам проведения мероприятий по контролю без взаимодействия с оператором.

20. Управление Роскомнадзора региона, в соответствии с постановлением Правительства РФ от 12.02.2019 г. № 146 уведомляет оператора о проведении плановой проверки за…

а) 3 рабочих дня;

б) 7 рабочих дней;

в) 10 рабочих дней.

21. Управление Роскомнадзора региона, в соответствии с постановлением Правительства РФ от 12.02.2019 г. № 146 уведомляет оператора о проведении внеплановой проверки за…

а) 24 часа до начала проверки;

б) 48 часов до начала проверки;

в) 3 дня до начала проверки.

22. Управление Роскомнадзора региона, в соответствии с постановлением Правительства РФ от 12.02.2019 г. № 146 проводит проверку в отношении…

а) обработки ПДн с использованием и без использования средств автоматизации;

б) документов и принятых мер по ч.1 ст.18.1 ФЗ-152;

в) обработки ПДн в ИСПДн;

г) защиты ПДн в ИСПДн.

23. Кто получает Согласие на обработку персональных данных участников Всероссийской олимпиаде школьников?

а) Школа;

б) Управление образования района/города;

в) Организатор олимпиады.

24. Как поступить, если участковая поликлиника запрашивает по телефону у секретаря руководителя школы списки учащихся (студентов), не прошедших периодический медосмотр?

а) Предоставить список по телефону;

б) Переадресовать участковую поликлинику в медицинский кабинет;

в) Предложить направить на имя руководителя мотивированный запрос для передачи списка.

25. Что может размещать педагог школы, в личных аккаунтах «ВКонтакте», «Однокласснике» фотографии в виде:

а) групповая фотография своих учеников;

б) фотография коллеги;

в) групповая фотография коллег-педагогов.

26. При прохождении социально-психологического тестирования школьников Согласие дают…

а) самостоятельно дети, достигшие 14 летнего возраста

б) самостоятельно дети, достигшие 15 летнего возраста

в) родители детей, не достигших 18 летнего возраста

27. По приказу Управления образования, педагог школы назначен членом жюри (оргкомитета) городской олимпиады, которая проходит в Городском Учебно-методическом центре.

а) Педагог школы даёт Согласие на передачу ПДн в УМЦ;

б) Управление образования без Согласия педагога передаёт его ПДн в УМЦ.

28. При сопровождении учащихся на региональный этап олимпиады, педагог школы:

а) даёт Согласие на передачу его данных в региональный оргкомитет;

б) Согласие не обязательно.

29. Если банк направил в налоговую инспекцию запрос о подтверждении достоверности предоставленной заемщиком(гражданином) в банк справки о доходах:

а) Налоговая инспекция обязана предоставить информацию о гражданине;

б) Налоговая инспекция предоставит информацию банку о гражданине, если банк предоставит налоговой инспекции Согласие гражданина.

30. Управление образования направило в городскую больницу предписание (на основании Постановления Главы города) направить в Управление образования список родителей несовершеннолетних учащихся, кто отказался от прохождения медосмотров (оказания медицинской помощи).

а) Главный врач обязан предоставить запрашиваемую информацию;

б) Главный врач должен отказать Управлению образования в предоставлении информации, ввиду отсутствия Согласия родителей учащихся.

31. На классном родительском собрании отсутствовало трое родителей. Классный руководитель для информирования этих родителей:

а) Предоставит председателю родительского комитета класса номера мобильных телефонов отсутствующих родителей;

б) Не имеет права предоставлять номера мобильных телефонов отсутствующих родителей.

32. Инспектор по делам несовершеннолетних обратился к директору школы за предоставлением характеристики на школьника 8 класса:

а) Характеристика будет предоставлена по устному заявлению;

б) Характеристика будет предоставлена по письменному заявлению.

33. На школьном сайте решили разместить групповую фотографию трёх дипломантов городской предметной олимпиады и одиночную фотографию победителя городского конкурса.

а) Школа обязана получить согласия от четырех родителей;

б) Школа обязана получить согласие от родителя школьника – победителя конкурса;

в) Школа не обязана получать согласия так как фотографии без указаний фамилии и имени.

34. Электронный дневник в школе стал частью «Сетевого города» на портале госуслуг.

а) Школа обязана получить согласие родителей на размещение в системе данных учащихся;

б) Школа не обязана получать согласия родителей на размещение в системе ПДн учащихся.

35. Организацией доступа в здание лицея занимается частное охранное предприятие.

а) Лицей обязан получить письменные согласия от родителей и работников на предоставление персональных данных ЧОП;

б) Лицей не обязан получать согласия от родителей и работников, т.к. решение о договоре с ЧОП принималось на школьном собрании родителей.

36. Администрация города приняла решение о внедрении в городе транспортных карт для учащихся.

а) Школа обязана передать списки учащихся в Городское транспортное предприятие;

б) Школа передаст списки учащихся в Городское транспортное предприятие только после получения письменных согласий родителей.

37. Какой раздел в Уведомлении, которое подает образовательная организация в реестре операторов, осуществляющих обработку персональных данных, обязаны заполнять с 2018 года.

а) Сведения о месте нахождении базы данных информации, содержащей персональные данные граждан РФ;

б) Ответственный за обеспечение безопасности персональных данных.

38. Какой период хранения в архиве организации договоров о повышении квалификации работников в соответствии с Приказом Минкультуры России от 25.08.2010 № 558?

а) 3 года;

б) 5 лет.

39. Какой период хранения в архиве организации графика предоставления отпусков с Приказом Минкультуры России от 25.08.2010 № 558?

а) 3 года;

б) 1 год.

40. Директор лицея получил из ИФНС района Уведомление о задолженности по налогам и сборам работников организации с предложением провести беседы с работниками.

а) Директор лицея обязан, в соответствии с Налоговым Кодексом, провести беседу с работником;

б) Директор лицея проведет беседу с работником в случае наличия в Уведомлении только информации о наличии задолженности.

ИТОГОВЫЙ КЕЙС

Ответ задачу

Управлением Роскомнадзора на основании задания, утвержденного руководителем Управления Роскомнадзора, было проведено мероприятие по контролю без взаимодействия с организацией (контролируемым лицом), посредством просмотра разделов сайта - https://kassa.ru/ в сети «Интернет» и анализа их содержания на предмет соответствия требованиям законодательства Российской Федерации в области персональных данных.

В ходе анализа сайта - https://kassa.ru/ установлено, что осуществляется сбор персональных данных в разделах: «Главная/Заказать звонок»; «Главная/Контакты»; «Главная/Подать заявку»; «Главная/Юридическая помощь», но на сайте не опубликован документ, определяющий политику в отношении обработки персональных данных и сведений о реализуемых требованиях к защите персональных данных.

ЗАДАНИЕ:

1. Выявлены признаки нарушения обязательных требований законодательства в области обработки персональных данных. Какая статья и какого закона нарушена, дать развернутый ответ по (ч. 0 ст. 00.0 ФЗ № 000 «……»)?

2. Совершено административное правонарушение. Какая административная статьи может быть применена в данной ситуации, дать развернутый ответ по (ч. 0 ст. 00.00 КоАП РФ)?

Эталонные ответы

Количество баллов	Примерное содержание ответа
9 – 10	В соответствии с требованиями ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети «Интернет», с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети. Управлением Роскомнадзора в ходе анализа разделов сайта в сети «Интернет» установлено, что осуществляет сбор персональных данных с использованием сайта https://kassa.ru/ (разделы: «Главная/Заказать звонок» (фамилия, имя, отчество, номер телефона); «Главная/Контакты» (фамилия, имя, отчество, номер телефона); «Главная/Подать заявку» (e-mail, фамилия, имя, отчество, номер телефона, название организации, сайт организации); «Главная/Юридическая помощь» (e-mail, фамилия, имя, отчество, номер телефона). При этом на сайте https://kassa.ru/ не опубликованы документ,

Ответ задача

	определяющий политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных. Совершено административное правонарушение, предусмотренное ч. 3 ст. 13.11 КоАП РФ, а именно невыполнение предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию документа, определяющего политику в отношении обработки персональных данных, и сведений о реализуемых требованиях к защите персональных данных, в части неисполнения требования ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Невыполнение предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию документа, определяющего политику оператора в отношении обработки персональных данных, и сведений о реализуемых требованиях к защите персональных данных, образует состав административного правонарушения, предусмотренного ч. 3 ст. 13.11 Кодекса Российской Федерации об административных правонарушениях. В случае, если на все вопросы даны правильные развернутые ответы с верно указанными ссылками на законодательство. Балл может быть снижен за несущественную неточность.
7 – 8	В случае, если на вопросы даны правильные развернутые ответы с верно указанными ссылками на законодательство. Балл может быть снижен за лаконичные ответы, отсутствие или ошибку в ссылке на законодательство в одном из ответов.
5 – 6	В случае, если на вопросы даны правильные развернутые ответы с верно указанными ссылками на законодательство. Балл может быть снижен за лаконичные ответы, отсутствие или ошибку в ссылке на законодательство в одном из ответов.
3 – 4	В случае, если на 1 вопрос дан правильный ответ с верно указанными ссылками на законодательство. Балл может быть снижен за лаконичные ответы, отсутствие или существенные ошибки в ссылках на законодательство.
0 – 2	В случае, если на все вопросы даны неправильные ответы, либо ответы содержат существенные ошибки (например, ошибки в ссылках на законодательство).

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Основная литература

1. В.В. Беспалов / Информационные технологии / – Томск: Изд-во Томского политехнического университета, 2012. – 134 стр.
2. В.В. Сухостат / Основы информационной безопасности / – СПб.: Изд-во СПбГЭУ, 2019. – 103 стр.
3. С.И. Макаренко / Информационная безопасность: учебное пособие. /– Ставрополь, 2009 г. – 372 стр.
4. Комплексное обеспечение информационной безопасности автоматизированных систем: учеб. пособие / В.А. Челухин. - Комсомольск-на-Амуре: ФГБОУ ВПО "КнАГТУ", 2014. - 207 с.
5. Ясенев В.Н. / Информационная безопасность / – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2006. – 253 стр.

Дополнительная литература

6. Е.В. Вострецова / Основы информационной безопасности / — Екатеринбург : Изд-во Урал. ун-та, 2019 г. — 204 стр.
7. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.
8. Ю. Ю. Громов / Информационные технологии / – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2015 г. – 260 стр.
9. Келдыш Н.В. Информационная безопасность. Защита информации на объектах информатизации. Учебное пособие – М.: Мир науки, 2022.
10. А.М. Кенин / Самоучитель системного администратора / Санкт-Петербург 2019 г. - 608 стр.
11. Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке) / Под общ. ред. А. В. Крутских. — М.: Издательство «Аспект Пресс», 2019.— 784 с.
12. Информационное право России: Учеб. пособие для студентов, обучающихся по специальностям (направлениям) «Юриспруденция» и «Прикладная информатика в юриспруденции». – Саратов: Изд-во Сарат. ун-та, 2010. – 196 с

Нормативно-правовые акты:

Конституция Российской Федерации;

Трудовый кодекс Российской Федерации; Гражданский кодекс Российской Федерации;

Федеральный закон от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

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

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Федеральный закон от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;

Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

Федерального закона от 2 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации»;

Постановление Правительства РФ от 6 июля 2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановление Правительства РФ от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

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».

Электронные ресурсы

1. http://www.inside-zi.ru — сайт журнала «Защита информации»
2. http://www.inside-zi.ru — сайт журнала «Инсайд»
3. http://www.xakep.ru — сайт журнала «Хакер»
4. http://garant.ru — Гарант: законодательство РФ
5. http://www.consultant.ru — Консультант +: законодательство РФ
6. http://fstec.ru/ — официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)
7. http://www.scrf.gov.ru/ — официальный сайт Совета безопасности Российской Федерации
8. http://fsb.ru — официальный сайт Федеральной службы безопасно- сти Российской Федерации (ФСБ России)
9. http://www.saferinternet.ru/ Безопасный интернет - специальный портал, созданный по вопросам безопасного использования сети Интернет. Документы, материалы и многое другое
10. http://saferinternet.ru/ Портал Российского Оргкомитета по проведению Года Безопасного Интернета (ресурсы, ссылки, документы, материалы по проблематике)

11. http://www.infoforum.ru/ Национальный форум информационной безопасности "ИНФОФОРУМ" – электронное периодическое издание по вопросам информационной безопасности
12. http://saferunet.ru/ Центр Безопасного Интернета в России посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Вопросы Интернет-угроз, технологий, способов эффективного противодействия им в отношении пользователей.