УТВЕРЖДАЮ
Генеральный директор
ООО «Новая Парадигма»
_____ Т.С. Белько
«22» января 2024 г.
М.П.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации
«Организация работы по защите персональных данных»

г. Москва
2024

АННОТАЦИЯ ПРОГРАММЫ

Дополнительная профессиональная программа повышения квалификации «**Организация работы по защите персональных данных**» (далее – «Программа») направлена на:

- совершенствование компетенции, необходимой для профессиональной деятельности в области защиты персональных данных;
- получение новой компетенции, необходимой для профессиональной деятельности в области защиты персональных данных;
- повышение профессионального уровня в рамках имеющейся квалификации в области защиты персональных данных.

Программа предназначена широкому кругу специалистов, участвующих в обработке и хранение персональных данных:

- руководителям и специалистам государственных, муниципальных органов и органов местного самоуправления;
- руководителям департаментов информационных технологий и информационной безопасности;
- специалистам, работающим в области информационной безопасности;
- специалистам, отвечающим за работу с персональными данными;
- юристам, юрисконсультам предприятий-операторов персональных данных;
- работникам кадровых отделов организаций и предприятий;
- иным категориям слушателей.

Нормативный срок освоения программы повышения квалификации **72 часа**, при заочной форме обучения с частичным отрывом от производства.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалиста, участвующего в обработке и хранение персональных данных.

Программа разработана в соответствии со следующими нормативными документами:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства образования и науки РФ от 01.07.2013 № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Профессиональный стандарт «Специалист по технической защите информации», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 09.08.2022 № 474н;
- Общероссийский классификатор занятий ОК 010-2014 (МСКЗ-08), (дата введения 01.07.2015).

Категория слушателей: специалисты предприятий и организаций, ответственные за обеспечение безопасности при работе с персональными данными.

Требования к имеющемуся уровню образования:

Лица, имеющие:

- Высшее образование (специалитет / бакалавриат / магистратура);
- Среднее профессиональное образование.
- Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

Форма обучения:

Заочная с применением дистанционных образовательных технологий и электронного обучения. В качестве инструмента дистанционного обучения используется система дистанционного обучения «Учи.Про» (sdo.uchi.pro). Логин и пароль для доступа в систему направляется слушателю (законному представителю слушателя) по указанному в заявке на обучение адресу электронной почты.

Сфера профессиональной деятельности освоивших Программу: связь, информационные и коммуникационные технологии, кадровое делопроизводство.

Лица, завершившие освоение Программу, должны обладать следующими профессиональными компетенциями:

- разработка и подготовка к утверждению проектов нормативных и методических документов, регламентирующих работу по технической защите информации, положений, инструкций и других организационно-распорядительных документов;
- руководство работами по составлению актов, предписаний на право эксплуатации и другой документации по технической защите информации и обеспечению безопасности информации на объектах информатизации;
- организация разработки организационно-распорядительных документов в области технической защиты информации;
- осуществление контроля выполнения требований нормативных правовых актов и иных документов по технической защите информации;
- руководство работами по выявлению угроз безопасности информации, определению возможностей технической разведки и проведению мероприятий технической защиты информации;
- участие в обследовании объектов информатизации, их категорировании и аттестации;
- осуществление проверки выполнения требований нормативных документов по технической защите информации.

Режим занятий:

Не более 40 часов в неделю, не более 8 часов в день.

Срок освоения Программы: 72 часа

Возможные наименования должностей, профессий лиц, окончивших Программу:

Освоение Программы (при наличии высшего образование в области информационной безопасности), предоставляет возможность занятия слушателем должностей:

- главный специалист по технической защите информации;
- руководитель структурного подразделения по технической защите информации;
- специалист по технической защите информации.

Выдаваемый документ об образовании: удостоверение о повышении квалификации.

1. ЦЕЛЬ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

1.1. Цель Программы

Целью данной Программы является совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалиста, участвующего в обработке и хранение персональных данных в следующих видах деятельности:

— проведение аттестации объектов информатизации на соответствие требованиям по защите информации;

— организация и проведение работ по защите информации в организации.

1.2. Результаты обучения

Обучающийся в ходе освоения Программы **должен знать:**

— нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации;

— порядок аттестации объектов информатизации на соответствие требованиям по защите информации;

— основные требования, предъявляемые к организации и ведению работ по обеспечению безопасности персональных данных;

— права и обязанности оператора персональных данных;

— программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее;

— способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;

— основные виды угроз безопасности персональных данных;

— меры по предотвращению угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

— методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее;

— технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет

наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах;

- технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акусто-электромагнитные);
- технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных специальных электронных устройств перехвата информации в технические средства и (или) предметы интерьера помещения;
- способы и средства защиты информатизации от утечки за счет побочных электромагнитных излучений и наводок;
- способы и средства защиты акустической речевой информации от утечки по техническим каналам;
- нормативные правовые акты, методические документы в области защиты информации ограниченного доступа;
- организационно-распорядительную документацию по защите информации на объекте информатизации;
- эксплуатационную документацию на систему защиты информации;
- организационно-распорядительную документацию по защите информации на объекте информатизации;
- порядок создания автоматизированных систем в защищенном исполнении.

Обучающийся в ходе освоения программы должен уметь:

- применять государственные нормативные требования в области защиты информации ограниченного доступа и аттестации объектов информатизации при разработке локальных нормативных актов;
- применять нормативные правовые акты и нормативно-техническую документацию в части выделения в них требований, процедур, регламентов, рекомендаций для адаптации и внедрения в локальную нормативную документацию;
- анализировать изменения законодательства в сфере в области защиты информации ограниченного доступа и аттестации объектов информатизации;

— пользоваться справочными информационными базами данных, содержащими документы и материалы по в области защиты информации ограниченного доступа и аттестации объектов информатизации;
— определять перечень информации (сведений) ограниченного доступа, подлежащих защите в организации;
— организовывать работы по обеспечению безопасности персональных данных;
— определять возможные угрозы безопасности персональных данных;
— определять и внедрять оптимальные организационные и технические меры защиты информации в информационных системах персональных данных;
— разрабатывать техническое задание на создание системы защиты информации в организации;
— разрабатывать разрешительную систему доступа к информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации;
— разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации;
— анализировать данные о назначении, функциях, условиях функционирования основных технических средств и систем, установленных на объектах информатизации, и характере обрабатываемой на них информации;
— организовывать ввод системы защиты информации в эксплуатацию.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план Программы

№ п/п	Наименование модулей	Всего, час.	В том числе:	
			Лекции	Практические занятия
1.	**Модуль 1.** Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных	11	10,5	0,5
2.	**Модуль 2.** Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	11	10,5	0,5
3.	**Модуль 3.** Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	9	8,5	0,5
4.	**Модуль 4.** Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	16	9,5	6,5
5.	**Модуль 5.** Меры безопасности, применяемые при обработке персональных данных в информационных системах	9	8,5	0,5
6.	**Модуль 6.** Создание модели системы защиты персональных данных в организации	-	-	15
Итоговая аттестация		**1**	**-**	**1**
Итого		**72**	**47,5**	**24,5**

2.2. Календарный учебный график Программы

№ п/п	Наименование программы	Форма обучения	Месяцы/даты											
			январь	февраль	март	апрель	май	июнь	июль	август	сентябрь	октябрь	ноябрь	декабрь
1.	Дополнительная профессиональная программа (ДПП) повышения квалификации «Организация работы по защите персональных данных»	заочная с применением дистанционных технологий	По мере комплектования учебных групп в течение календарного года											

2.3. Учебно-тематический план Программы

№ п/п	Наименование разделов, модулей, тем	Всего часов	В том числе:		Формы контроля
			лекции	практические занятия	
Модуль 1.	Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных	**11**	**10,5**	**0,5**	
Тема 1.1.	Правовые основы технической защиты информации ограниченного доступа	3	3	-	Тестирование
Тема 1.2.	Организационные основы технической защиты информации ограниченного доступа	2	2	-	
Тема 1.3.	Организационные основы технической защиты информации ограниченного доступа в организации	2	2	-	
Тема 1.4.	Сертификация средств защиты и аттестация объектов информатизации	3,5	3,5	-	
Промежуточная аттестация	Тестирование по модулю «Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных»	0,5	-	0,5	
Модуль 2.	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	**11**	**10,5**	**0,5**	
Тема 2.1.	Выявление угроз безопасности информации на объектах информатизации	3	3	-	Тестирование
Тема 2.2.	Основные организационные меры защиты информации от несанкционированного доступа	4	4	-	
Тема 2.3.	Основные технические и программные средства защиты информации от несанкционированного доступа	3,5	3,5	-	

Промежуточная аттестация	Тестирование по модулю «Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа»	0,5	-	0,5	
Модуль 3.	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	**9**	**8,5**	**0,5**	
Тема 3.1.	Угрозы безопасности информации	2	2	-	Тестирование
Тема 3.2.	Утечка информации	2	2	-	
Тема 3.3.	Защита информации от утечки	4,5	4,5	-	
Промежуточная аттестация	Тестирование по модулю «Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных»	0,5	-	0,5	
Модуль 4.	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	**16**	**9,5**	**6,5**	
Тема 4.1.	Основные понятия обработки персональных данных	1	1	-	Выполнение практического задания, тестирование
Практическая работа по теме 4.1. «Основные понятия обработки персональных данных»		2	-	2	
Тема 4.2.	Субъект персональных данных	1	1	-	
Тема 4.3.	Оператор персональных данных	1	1	-	
Тема 4.4.	Меры по обеспечению безопасности персональных данных	2	2	-	
Тема 4.5.	Обработка персональных данных	3	3	-	
Практическая работа по теме 4.5. «Обработка персональных данных»		4	-	4	

Тема 4.6.	Нарушения законодательства РФ в области персональных данных	1,5	1,5	-	
Промежуточная аттестация	Тестирование по модулю «Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	0,5	-	0,5	
Модуль 5.	Меры безопасности, применяемые при обработке персональных данных в информационных системах	**9**	**8,5**	**0,5**	
Тема 5.1.	Типовые программно-технические средства защиты информации	2	2	-	Тестирование
Тема 5.2.	Организация защиты персональных данных в организации	3	3	-	
Тема 5.3.	Требования к защите, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	3,5	3,5	-	
Промежуточная аттестация	Тестирование по модулю «Меры безопасности, применяемые при обработке персональных данных в информационных системах»	0,5	-	0,5	
Модуль 6.	Создание модели системы защиты персональных данных в организации	**15**	**-**	**15**	
Практическая работа № 1. Определение условий функционирования системы обработки персональных данных в организации		2	-	2	Проверка практической работы
Практическая работа № 2. Определение актуальных угроз безопасности персональных данных в организации при их обработке в информационной системе		2	-	2	
Практическая работа № 3. Определение необходимого уровня защищенности персональных данных в организации		2	-	2	
Практическая работа № 4. Определение перечня нормативно-правовых актов при определении/описании создаваемой с учетом уже существующих средств защиты персональных данных в организации		3	-	3	

Практическая работа № 5. Определение перечня организационно-распорядительных документов, необходимых для регламентации защиты персональных данных в организации	3	-	3	
Практическая работа № 6. Определение на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующих актуальных угроз безопасности в организации	3	-	3	
Итоговая аттестация	1	-	1	**Итоговое тестирование**
Итого:	72	47,5	24,5	

2.4. РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА «ОРГАНИЗАЦИЯ РАБОТЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Курс состоит из 6 модулей:

Модуль 1. Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных;

Модуль 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа;

Модуль 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных;

Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

Модуль 5. Меры безопасности, применяемые при обработке персональных данных в информационных системах;

Модуль 6. Создание модели системы защиты персональных данных в организации.

2.4.1. РАБОЧАЯ ПРОГРАММА МОДУЛЯ 1 «Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных»

Целью освоения модуля является совершенствование компетенций, обеспечивающих готовность сформировать у слушателей основные знания и умение ориентироваться в современной нормативной правовой базе в сфере обработки и хранения персональных данных.

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения модуля 1:

- готовность осуществлять нормативное обеспечение обработки и хранения персональных данных;
- способность использовать правовые знания и умения в области обработки и хранения персональных данных.

Планируемые результаты обучения по модулю 1

По итогам освоения модуля слушатели должны

знать:

- нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации;
- нормативные правовые акты, методические документы в области защиты информации ограниченного доступа.

уметь:

- применять государственные нормативные требования в области защиты информации ограниченного доступа и аттестации объектов информатизации при разработке локальных нормативных актов;
- применять нормативные правовые акты и нормативно-техническую документацию в части выделения в них требований, процедур, регламентов, рекомендаций для адаптации и внедрения в локальную нормативную документацию;
- анализировать изменения законодательства в сфере в области защиты информации ограниченного доступа и аттестации объектов информатизации;
- пользоваться справочными информационными базами данных, содержащими документы и материалы по в области защиты информации ограниченного доступа и аттестации объектов информатизации.

Учебно-тематический план модуля 1

№ п/п	Наименование разделов, модулей, тем	Всего часов	В том числе:		Формы контроля
			лекции	практические занятия	
Модуль 1.	Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных	**11**	**10,5**	**0,5**	
Тема 1.1.	Правовые основы технической защиты информации ограниченного доступа	3	3	-	Тестирование
Тема 1.2.	Организационные основы технической защиты информации ограниченного доступа	2	2	-	

Тема 1.3.	Организационные основы технической защиты информации ограниченного доступа в организации	2	2	-	
Тема 1.4.	Сертификация средств защиты и аттестация объектов информатизации	3,5	3,5	-	
Промежуточная аттестация	Тестирование по модулю «Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных»	0,5	-	0,5	

Содержание модуля 1

Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных

Тема 1.1. Правовые основы технической защиты информации ограниченного доступа

Основные понятия и определения в области защиты информации. Доктрина информационной безопасности Российской Федерации. Информационная безопасность как одно из стратегических направлений национальной безопасности Российской Федерации. Концептуальные вопросы защиты информации.

Тема 1.2. Организационные основы технической защиты информации ограниченного доступа

Силы обеспечения информационной безопасности. Задачи ФСБ России по обеспечению общей и информационной безопасности. Основные задачи ФСО России. Деятельность Минобороны России и МВД России по обеспечению информационной безопасности. Деятельность Минкомсвязи России в сфере информационной безопасности. Полномочия Роскомнадзора в сфере информационной безопасности. Полномочия ФСТЭК России. Задачи ФСТЭК России. Деятельность органов власти и местного самоуправления в сфере информационной безопасности РФ.

Тема 1.3. Организационные основы технической защиты информации ограниченного доступа в организации

Структура и функции органов и подразделений по технической защите информации в организации. Система обеспечения информационной безопасности. Лицензирование деятельности в области защиты информации.

Тема 1.4. Сертификация средств защиты и аттестация объектов информатизации

Нормативно-правовая база сертификации средств защиты и аттестации объектов информатизации. Формы подтверждения соответствия. Декларирование соответствия. Сертификат соответствия. Нормативно-правовая база сертификация средств защиты информации. Сертификация средств защиты информации (СЗИ). Электронная цифровая подпись. Аттестация объектов информатизации.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, ознакомления с материалами лекций, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд электронной библиотеки, интернет-ресурсы и профессиональные информационные сервисы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и пособий, разработанные конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения. Индивидуальные консультации проводятся посредством возможностей электронного учебного курса (форум с преподавателем).

№ темы	Наименование (содержание) темы, по которой предусмотрена самостоятельная работа	Формы и методы проведения
1.1	Правовые основы технической защиты информации ограниченного доступа	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
1.2	Организационные основы	Изучение основной и дополнительной

№ темы	Наименование (содержание) темы, по которой предусмотрена самостоятельная работа	Формы и методы проведения
	технической защиты информации ограниченного доступа	литературы по программе; работа с интернет-сервисами правовых систем
1.3	Организационные основы технической защиты информации ограниченного доступа в организации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
1.4	Сертификация средств защиты и аттестация объектов информатизации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к промежуточной аттестации

Задания для самостоятельной работы:

Слушателю предлагается изучить основополагающие законодательные акты в области организации работ в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.12.2002 №184-ФЗ «О техническом регулировании»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Закон РФ от 21.07.1993 № 5485-I «О государственной тайне»;
- Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

— Постановление Правительства РФ от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации»;
— Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»;
— Постановление Правительства РФ от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения и о внесении изменения в Положение о сертификации средств защиты информации»;
— Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
— Постановление Правительства РФ от 21.03.2012 № 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»;
— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения

установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;
— Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
— Приказ Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
— Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
— Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
— Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

— Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
— Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.).

Перечень основной и дополнительной учебной литературы, необходимой для освоения модуля 1

Основная литература

— Правовое регулирование информационных отношений в области государственной и коммерческой тайны, персональных данных: учебное пособие: / О. В. Ахрамеева, И. Ф. Дедюхина, О. В. Жданова [и др.]; Ставропольский государственный аграрный университет, Кафедра государственного и муниципального управления и права. – Ставрополь: Ставропольский государственный аграрный университет (СтГАУ), 2015. – 59 с. –URL: https://biblioclub.ru/index.php?page=book&id=438603.
— Защита интеллектуальной собственности: учебник / И. К. Ларионов, М. А. Гуреева, В. В. Овчинников [и др.] ; под ред. И. К. Ларионова, М. А. Гуреевой, В. В. Овчинникова. – 5-е изд., стер. – Москва: Дашков и К°, 2023. – 256 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=710103 – Библиогр. в кн. – ISBN 978-5-394-05367-2.

Дополнительная литература

— Мансуров, Г. З. Право цифровой безопасности: учебник: / Г. З. Мансуров. – Москва: Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – DOI 10.23681/687364.
— Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. –

ISBN 978-5-238-02857-6.

— Корнилова, А. А. Защита персональных данных: учебное пособие: / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2020. – 119 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн.

— Прохорова, О. В. Информационная безопасность и защита информации: учебник: / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.: табл., схем., ил. – URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн. – ISBN 978-5-9585-0603-3.

Электронные ресурсы:

1. Электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/.
2. Российская государственная библиотека https://www.rsl.ru/.

2.4.2. РАБОЧАЯ ПРОГРАММА МОДУЛЯ 2 «Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа»

Целью освоения модуля является совершенствование компетенций, обеспечивающих формирование у слушателей целостного представления, расширение теоретико-методологических знаний и закрепление профессиональных навыков в выявлении угроз безопасности информации на объектах информатизации, определении основных средств защиты информации от несанкционированного доступа.

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения модуля 2:

— способность формировать, внедрять и обеспечивать функционирование системы обработки и хранения персональных данных в организации;

— способность распределять полномочия, ответственность, обязанности по вопросам обработки и хранения персональных данных и обосновывать ресурсное обеспечение.

Планируемые результаты обучения по модулю 2

По итогам освоения модуля слушатели должны

знать:

- порядок аттестации объектов информатизации на соответствие требованиям по защите информации;
- программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее;
- способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;
- методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее;
- организационно-распорядительную документацию по защите информации на объекте информатизации;
- методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее.

уметь:

- определять перечень информации (сведений) ограниченного доступа, подлежащих защите в организации;
- разрабатывать техническое задание на создание системы защиты информации в организации.

Учебно-тематический план модуля 2

№ п/п	Наименование разделов, модулей, тем	Всего часов	В том числе:		Формы контроля
			лекции	практические занятия	
Модуль 2.	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	**11**	**10,5**	**0,5**	
Тема 2.1.	Выявление угроз безопасности информации на объектах информатизации	3	3	-	Тестирование
Тема 2.2.	Основные организационные меры защиты информации от несанкционированного доступа	4	4	-	

Тема 2.3.	Основные технические и программные средства защиты информации от несанкционированного доступа	3,5	3,5	-	
Промежуточная аттестация	Тестирование по модулю «Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа»	0,5	-	0,5	

Содержание модуля 2

Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

Тема 2.1. Выявление угроз безопасности информации на объектах информатизации

Угрозы информационной безопасности. Классификация угроз информационной безопасности

Классификация источников угроз. Уязвимости безопасности информации.

Тема 2.2. Основные организационные меры защиты информации от несанкционированного доступа

Аттестация объектов информатизации. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Разработка программы и методики аттестационных испытаний. Заключение договоров на аттестацию. Заключение по результатам аттестации. Рассмотрение апелляций. Аттестат соответствия. Аттестация объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.

Тема 2.3. Основные технические и программные средства защиты информации от несанкционированного доступа

Особенности программно-математического воздействия в сетях общего пользования. Защита информации в локальных вычислительных сетях.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной

литературы по программе, ознакомления с материалами лекций, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд электронной библиотеки, интернет-ресурсы и профессиональные информационные сервисы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и пособий, разработанные конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения. Индивидуальные консультации проводятся посредством возможностей электронного учебного курса (форум с преподавателем).

№ темы	Наименование (содержание) темы, по которой предусмотрена самостоятельная работа	Формы и методы проведения
2.1	Выявление угроз безопасности информации на объектах информатизации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
2.2	Основные организационные меры защиты информации от несанкционированного доступа	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
2.3	Основные технические и программные средства защиты информации от несанкционированного доступа	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к промежуточной аттестации

Задания для самостоятельной работы:

Слушателю предлагается изучить основополагающие законодательные акты в области организации работ в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации:

— Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
— Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»;
— Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
— Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
— Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
— Постановление Правительства РФ от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации»;
— Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»;
— Постановление Правительства РФ от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства,

строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения и о внесении изменения в Положение о сертификации средств защиты информации»;

— Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
— Постановление Правительства РФ от 21.03.2012 № 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»;
— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;
— Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);

— Приказ Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
— Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
— Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
— Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
— Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
— Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.).

Перечень основной и дополнительной учебной литературы, необходимой для освоения модуля 2

Основная литература

— Аверченков, В. И. Служба защиты информации: организация и управление: учебное пособие: / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 186 с.: ил., схем. –URL: https://biblioclub.ru/index.php?page=book&id=93356. – Библиогр. в кн. – ISBN 978-5-9765-1271-9.
— Защита интеллектуальной собственности: учебник / И. К. Ларионов, М. А. Гуреева, В. В. Овчинников [и др.] ; под ред. И. К. Ларионова, М. А.

Гуреевой, В. В. Овчинникова. – 5-е изд., стер. – Москва: Дашков и К°, 2023. – 256 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=710103 – Библиогр. в кн. – ISBN 978-5-394-05367-2.

— Прохорова, О. В. Информационная безопасность и защита информации: учебник: / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.: табл., схем., ил. – URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн. – ISBN 978-5-9585-0603-3.

Дополнительная литература

— Мансуров, Г. З. Право цифровой безопасности: учебник: / Г. З. Мансуров. – Москва: Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – DOI 10.23681/687364.

— Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6.

— Корнилова, А. А. Защита персональных данных: учебное пособие: / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2020. – 119 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн.

Электронные ресурсы:

1. Электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/.
2. Российская государственная библиотека https://www.rsl.ru/.

2.4.3. РАБОЧАЯ ПРОГРАММА МОДУЛЯ 3 «Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных»

Целью освоения модуля является совершенствование компетенций, обеспечивающих формирование у слушателей целостного представления, расширение теоретико-методологических знаний и закрепление профессиональных навыков в выявлении угроз безопасности персональных данных при их обработке в информационных системах персональных данных, определении организационных и технических мер защиты информации в информационных системах персональных данных.

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения модуля 3:

- способность идентифицировать и предупреждать угрозы безопасности персональных данных;
- способность определить и внедрить оптимальные организационные и технические меры защиты информации в информационных системах персональных данных.

Планируемые результаты обучения по модулю 3

По итогам освоения модуля слушатели должны

знать:

- основные виды угроз безопасности персональных данных;
- меры по предотвращению угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее;
- способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;
- методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее;
- организационно-распорядительную документацию по защите информации на объекте информатизации;

— методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее.

уметь:

— определять возможные угрозы безопасности персональных данных;
— разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации;
— определять и внедрять оптимальные организационные и технические меры защиты информации в информационных системах персональных данных;
— разрабатывать техническое задание на создание системы защиты информации в организации.

Учебно-тематический план модуля 3

№ п/п	Наименование разделов, модулей, тем	Всего часов	В том числе:		Формы контроля
			лекции	практические занятия	
Модуль 3.	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	**9**	**8,5**	**0,5**	
Тема 3.1.	Угрозы безопасности информации	2	2	-	Тестирование
Тема 3.2.	Утечка информации	2	2	-	
Тема 3.3.	Защита информации от утечки	4,5	4,5	-	
Промежуточная аттестация	Тестирование по модулю «Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных»	0,5	-	0,5	

Содержание модуля 3

Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

Тема 3.1. Угрозы безопасности информации

Угрозы безопасности информации. Случайные и преднамеренные угрозы. Традиционный шпионаж и диверсии. Системы подслушивания. Видео

разведка. Закладные устройства. Несанкционированный доступ к информации. Электромагнитные излучения и наводки. Несанкционированная модификация структур. Вредительские программы. Классификация злоумышленников.

Тема 3.2. Утечка информации

Утечка информации по техническим каналам. Физическая природа передачи информации. Каналы утечки информации. Особенности каналов утечки информации. Побочные электромагнитные излучения и наводки (ПЭМИН).

Тема 3.3. Защита информации от утечки

Защита информации от утечки по техническим каналам в общем плане. Защита информации от утечки по визуально-оптическим каналам. Средства и способы защиты информации от утечки по визуально-оптическому каналу. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным каналам. Защита от утечки за счёт электромагнитного излучения. Программно-аппаратный комплекс «Зарница». Защита от утечки за счет паразитной генерации. Защита от утечки по цепям питания. Защита от утечки за счет взаимного влияния проводов и линий связи. Взаимные влияния в линиях связи. Защита информации от утечки по материально-вещественным каналам.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, ознакомления с материалами лекций, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд электронной библиотеки, интернет-ресурсы и профессиональные информационные сервисы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и пособий, разработанные конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения. Индивидуальные консультации проводятся посредством возможностей электронного учебного курса (форум с преподавателем).

№ темы	Наименование (содержание) темы, по которой предусмотрена самостоятельная работа	Формы и методы проведения
3.1	Угрозы безопасности информации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
3.2	Утечка информации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
3.3	Защита информации от утечки	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к промежуточной аттестации

Задания для самостоятельной работы:

Слушателю предлагается изучить основополагающие законодательные акты в области организации работ в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации:

— Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
— Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»;
— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
— Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем

персональных данных»;

- Постановление Правительства РФ от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации»;
- Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»;
- Постановление Правительства РФ от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения и о внесении изменения в Положение о сертификации средств защиты информации»;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 21.03.2012 № 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»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств

криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;
— Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
— Приказ Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
— Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
— Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
— Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не

составляющей государственную тайну»;

— Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);

— Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.).

Перечень основной и дополнительной учебной литературы, необходимой для освоения модуля 3

Основная литература

— Аверченков, В. И. Служба защиты информации: организация и управление: учебное пособие: / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 186 с.: ил., схем. –URL: https://biblioclub.ru/index.php?page=book&id=93356. – Библиогр. в кн. – ISBN 978-5-9765-1271-9.

— Управление кадровой безопасностью организации: учебник для бакалавриата и магистратуры: / Ю. В. Долженкова, Е. В. Камнева, А. Л. Сафонов [и др.]; под ред. Ю. В. Долженковой; Финансовый университет при Правительстве Российской Федерации. – Москва: Прометей, 2022. – 286 с.: ил., табл., схем. –– URL: https://biblioclub.ru/index.php?page=book&id=700997. – Библиогр.: с. 245-256. – ISBN 978-5-00172-241-0.

— Защита интеллектуальной собственности: учебник / И. К. Ларионов, М. А. Гуреева, В. В. Овчинников [и др.] ; под ред. И. К. Ларионова, М. А. Гуреевой, В. В. Овчинникова. – 5-е изд., стер. – Москва: Дашков и К°, 2023. – 256 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=710103 – Библиогр. в кн. – ISBN 978-5-394-05367-2.

— Прохорова, О. В. Информационная безопасность и защита информации: учебник: / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.: табл., схем., ил. – URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн.

– ISBN 978-5-9585-0603-3.

Дополнительная литература

— Мансуров, Г. З. Право цифровой безопасности: учебник: / Г. З. Мансуров. – Москва: Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – DOI 10.23681/687364.

— Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6.

— Корнилова, А. А. Защита персональных данных: учебное пособие: / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2020. – 119 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн.

Электронные ресурсы:

1. Электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/.
2. Российская государственная библиотека https://www.rsl.ru/.

2.4.4. РАБОЧАЯ ПРОГРАММА МОДУЛЯ 4 «Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Целью освоения модуля является совершенствование компетенций, обеспечивающих формирование у слушателей целостного представления, расширение теоретико-методологических знаний и закрепление профессиональных навыков при организации и ведении работ по обеспечению безопасности персональных данных.

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения модуля 4:

— способность организовать и проводить работы по обеспечению безопасности персональных данных.

Планируемые результаты обучения по модулю 4

По итогам освоения модуля слушатели должны

знать:

- основные требования, предъявляемые к организации и ведению работ по обеспечению безопасности персональных данных;
- права и обязанности оператора персональных данных;
- меры по предотвращению угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

уметь:

- организовывать работы по обеспечению безопасности персональных данных;
- разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации;
- применять нормативные правовые акты и нормативно-техническую документацию в части выделения в них требований, процедур, регламентов, рекомендаций для адаптации и внедрения в локальную нормативную документацию;
- определять и внедрять оптимальные организационные и технические меры защиты информации в информационных системах персональных данных.

Учебно-тематический план модуля 4

№ п/п	Наименование разделов, модулей, тем	Всего часов	В том числе:		Формы контроля
			лекции	практические занятия	
Модуль 4.	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	**16**	**9,5**	**6,5**	
Тема 4.1.	Основные понятия обработки персональных данных	1	1	-	Выполнение практического задания, тестирование
Практическая работа по теме 4.1. «Основные понятия обработки персональных данных»		2	-	2	
Тема 4.2.	Субъект персональных данных	1	1	-	
Тема 4.3.	Оператор персональных данных	1	1	-	
Тема 4.4.	Меры по обеспечению безопасности персональных данных	2	2	-	
Тема 4.5.	Обработка персональных данных	3	3	-	
Практическая работа по теме 4.5. «Обработка персональных данных»		4	-	4	
Тема 4.6.	Нарушения законодательства РФ в области персональных данных	1,5	1,5	-	

Промежуточная аттестация	Тестирование по модулю «Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	0,5	-	0,5	

Содержание модуля 4

Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Тема 4.1. Основные понятия обработки персональных данных

Основные понятия, используемые в ФЗ от 27.07.2006 № 152 «О персональных данных». Принципы и условия обработки персональных данных. Условия обработки персональных данных.

Тема 4.2. Субъект персональных данных

Права субъекта персональных данных. Согласие субъекта персональных данных на обработку его персональных данных.

Тема 4.3. Оператор персональных данных

Обязанности оператора при сборе персональных данных. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ от 27.07.2006 № 152 «О персональных данных».

Тема 4.4. Меры по обеспечению безопасности персональных данных

Меры по обеспечению безопасности персональных данных при их обработке. Состав и содержание мер по обеспечению безопасности персональных данных.

Тема 4.5. Обработка персональных данных

Уведомление об обработке персональных данных. Лица, ответственные за организацию обработки персональных данных в организациях. Обработка персональных данных без средств автоматизации. Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

Тема 4.6. Нарушения законодательства РФ в области персональных данных

Ответственность за нарушение законодательства Российской Федерации в области персональных данных при обработке персональных

данных работника. Ответственность за нарушение законодательства Российской Федерации в области персональных данных.

Содержание семинаров, практических занятий

№ темы	Наименование темы, по которой предусмотрено занятие семинарского типа	Формы и методы проведения
4.1.	Основные понятия обработки персональных данных	выполнение практического задания
4.5	Обработка персональных данных	выполнение практического задания

Пример практического задания

Практическая работа по теме 4.1. «Основные понятия обработки персональных данных»

Задание 1. Составьте классификации персональных данных по разным признакам согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных». Результат представить для проверки в виде иерархической схемы или таблицы.

Задание 2. Определите, какие группы/категории персональных данных обрабатываются в вашей организации и каков их набор (при выполнении задания укажите, пожалуйста направление деятельности организации, в которой вы работаете).

Практическая работа по теме 4.5. «Обработка персональных данных»

Задание 1. Определите в вашей организации:

- категории персональных данных;
- производственные процессы, задействованные в обработке персональных данных;
- информационные системы, используемые в обработке персональных данных;
- лица/подразделения, участвующие в обработке персональных данных.

Примечание. Для выполнения задания используйте следующие нормативно-правовые акты, регламентирующие обработку персональных данных:

- ФЗ РФ от 27.07.2006 № 152;
- Постановление Правительства РФ от 01.11.2012 № 1119;
- Постановление Правительства РФ от 15 сентября 2008 г. № 687

Задание 2. Опишите:

- критерии сбора персональных данных в вашей организации (ФЗ РФ от 27.07.2006 № 152);
- основные меры, которые необходимо выполнить вашей организации в рамках использования персональных данных (ФЗ РФ от 27.07.2006 № 152);
- условия достижения цели обработки персональных данных в вашей организации (ФЗ РФ от 27.07.2006 № 152).

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, ознакомления с материалами лекций, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд электронной библиотеки, интернет-ресурсы и профессиональные информационные сервисы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и пособий, разработанные конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения. Индивидуальные консультации проводятся посредством возможностей электронного учебного курса (форум с преподавателем).

№ темы	Наименование (содержание) темы, по которой предусмотрена самостоятельная работа	Формы и методы проведения
4.1	Основные понятия обработки персональных данных	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Выполнение практического задания

№ темы	Наименование (содержание) темы, по которой предусмотрена самостоятельная работа	Формы и методы проведения
4.2	Субъект персональных данных	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
4.3	Оператор персональных данных	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
4.4	Меры по обеспечению безопасности персональных данных	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
4.5	Обработка персональных данных	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Выполнение практического задания
4.6	Нарушения законодательства РФ в области персональных данных	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к промежуточной аттестации

Задания для самостоятельной работы:

Слушателю предлагается изучить основополагающие законодательные акты в области организации работ в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации:

— Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
— Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»;
— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
— Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
— Постановление Правительства РФ от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к

информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации»;

- Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»;
- Постановление Правительства РФ от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения и о внесении изменения в Положение о сертификации средств защиты информации»;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 21.03.2012 № 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»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;
— Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
— Приказ Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
— Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
— Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
— Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
— Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной

технической комиссии при Президенте РФ от 30.03.1992 г.);

— Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.).

Перечень основной и дополнительной учебной литературы, необходимой для освоения модуля 4

Основная литература

— Аверченков, В. И. Служба защиты информации: организация и управление: учебное пособие: / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 186 с.: ил., схем. –URL: https://biblioclub.ru/index.php?page=book&id=93356. – Библиогр. в кн. – ISBN 978-5-9765-1271-9.

— Управление кадровой безопасностью организации: учебник для бакалавриата и магистратуры: / Ю. В. Должженкова, Е. В. Камнева, А. Л. Сафонов [и др.]; под ред. Ю. В. Должженковой; Финансовый университет при Правительстве Российской Федерации. – Москва: Прометей, 2022. – 286 с.: ил., табл., схем. –– URL: https://biblioclub.ru/index.php?page=book&id=700997. – Библиогр.: с. 245-256. – ISBN 978-5-00172-241-0.

— Защита интеллектуальной собственности: учебник / И. К. Ларионов, М. А. Гуреева, В. В. Овчинников [и др.] ; под ред. И. К. Ларионова, М. А. Гуреевой, В. В. Овчинникова. – 5-е изд., стер. – Москва: Дашков и К°, 2023. – 256 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=710103 – Библиогр. в кн. – ISBN 978-5-394-05367-2.

— Прохорова, О. В. Информационная безопасность и защита информации: учебник: / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.: табл., схем., ил. – URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн. – ISBN 978-5-9585-0603-3.

Дополнительная литература

- Мансуров, Г. З. Право цифровой безопасности: учебник: / Г. З. Мансуров. – Москва: Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – DOI 10.23681/687364.
- Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6.
- Корнилова, А. А. Защита персональных данных: учебное пособие: / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2020. – 119 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн.

Электронные ресурсы:

1. Электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/.
2. Российская государственная библиотека https://www.rsl.ru/.

2.4.5. РАБОЧАЯ ПРОГРАММА МОДУЛЯ 5 «Меры безопасности, применяемые при обработке персональных данных в информационных системах»

Целью освоения модуля является совершенствование компетенций, обеспечивающих формирование у слушателей целостного представления, расширение теоретико-методологических знаний и закрепление профессиональных навыков по подбору и внедрению мер безопасности, применяемых при обработке персональных данных.

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения модуля 5:

- способность классифицировать и определять меры безопасности, применяемые при обработке персональных данных;
- организовать подбор и внедрение систем защиты информации в организации.

Планируемые результаты обучения по модулю 5

По итогам освоения модуля слушатели должны

знать:

— методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее;

— технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах;

— технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акусто-электромагнитные);

— технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных специальных электронных устройств перехвата информации в технические средства и (или) предметы интерьера помещения;

— способы и средства защиты информатизации от утечки за счет побочных электромагнитных излучений и наводок;

— способы и средства защиты акустической речевой информации от утечки по техническим каналам;

— эксплуатационную документацию на систему защиты информации;

— порядок создания автоматизированных систем в защищенном исполнении.

уметь:

— разрабатывать техническое задание на создание системы защиты информации в организации;

— разрабатывать разрешительную систему доступа к информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации;

— разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации;

— анализировать данные о назначении, функциях, условиях функционирования основных технических средств и систем, установленных на объектах информатизации, и характере обрабатываемой на них информации;
— организовывать ввод системы защиты информации в эксплуатацию.

Учебно-тематический план модуля 5

№ п/п	Наименование разделов, модулей, тем	Всего часов	В том числе:		Формы контроля
			лекции	практические занятия	
Модуль 5.	Меры безопасности, применяемые при обработке персональных данных в информационных системах	**9**	**8,5**	**0,5**	
Тема 5.1.	Типовые программно-технические средства защиты информации	2	2	-	Тестирование
Тема 5.2.	Организация защиты персональных данных в организации	3	3	-	
Тема 5.3.	Требования к защите, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	3,5	3,5	-	
Промежуточная аттестация	Тестирование по модулю «Меры безопасности, применяемые при обработке персональных данных в информационных системах»	0,5	-	0,5	

Содержание модуля 5

Меры безопасности, применяемые при обработке персональных данных в информационных системах

Тема 5.1. Типовые программно-технические средства защиты информации

Правовая база. Межсетевой экран. Брандмауэр. Криптография. Цифровая подпись.

Тема 5.2. Организация защиты персональных данных в организации

Защита персональных данных работника (общие положения). Требования к обработке персональных данных. Защита персональных данных. Организация доступа работников к персональным данным других работников.

Тема 5.3. Требования к защите, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, ознакомления с материалами лекций, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд электронной библиотеки, интернет-ресурсы и профессиональные информационные сервисы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и пособий, разработанные конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения. Индивидуальные консультации проводятся посредством возможностей электронного учебного курса (форум с преподавателем).

№ темы	Наименование (содержание) темы, по которой предусмотрена самостоятельная работа	Формы и методы проведения
5.1	Типовые программно-технические средства защиты информации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
5.2	Организация защиты персональных данных в организации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем
5.3	Требования к защите, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к промежуточной аттестации

Задания для самостоятельной работы:

Слушателю предлагается изучить основополагающие законодательные акты в области организации работ в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации:

- Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства РФ от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации»;
- Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;
- Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
- Приказ Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
- Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие

требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

- Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
- Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
- Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
- Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997 г.);
- Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997 г.);
- Руководящий документ «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин автоматизированных кассовых систем и требования по защите информации»;
- Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты

информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. решением Государственной технической комиссии при Президенте РФ от 04.06.1999 № 114);

— Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (введен в действие приказом Государственной технической комиссии при Президенте РФ от 19.06.2002 № 187);
— Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;
— Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.);
— ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний».
— Межгосударственный стандарт ГОСТ 30373-95/ГОСТ Р 50414-92 «Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний» (введен в действие постановлением Госстандарта РФ от 15.05.1996 № 308);
— ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники».

Перечень основной и дополнительной учебной литературы, необходимой для освоения модуля 5

Основная литература

— Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва: Директ-Медиа, 2022. – 128 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – Библиогр.: с. 117-118. – ISBN 978-5-4499-3327-0. – DOI 10.23681/694670.

— Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / А. Г. Фабричнов, А. С. Дёмушкин, Т. В. Кондрашова, Н. Н. Куняев. – Москва: Логос, 2011. – 452 с. – (Новая университетская библиотека). – URL: https://biblioclub.ru/index.php?page=book&id=84996. – ISBN 978-5-98704-541-1.
— Безопасность электронного документооборота: учебное пособие: / П. А. Тищенко, Ю. М. Казаков, Р. А. Филиппов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 54 с. – URL: https://biblioclub.ru/index.php?page=book&id=602225. – Библиогр. в кн. – ISBN 978-5-4499-1928-1.
— Защита интеллектуальной собственности: учебник / И. К. Ларионов, М. А. Гуреева, В. В. Овчинников [и др.] ; под ред. И. К. Ларионова, М. А. Гуреевой, В. В. Овчинникова. – 5-е изд., стер. – Москва: Дашков и К°, 2023. – 256 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=710103 – Библиогр. в кн. – ISBN 978-5-394-05367-2.
— Прохорова, О. В. Информационная безопасность и защита информации: учебник: / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.: табл., схем., ил. – URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн. – ISBN 978-5-9585-0603-3.

Дополнительная литература

— Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6.
— Корнилова, А. А. Защита персональных данных: учебное пособие: / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2020. – 119 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн.

Электронные ресурсы:

1. Электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/.
2. Российская государственная библиотека https://www.rsl.ru/.

2.4.6. РАБОЧАЯ ПРОГРАММА МОДУЛЯ 6 «Создание модели системы защиты персональных данных в организации»

Целью освоения модуля является совершенствование компетенций, обеспечивающих закрепление профессиональных навыков по созданию модели системы защиты персональных данных в организации.

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения модуля 6:

— способность создать функционирующую модель системы защиты персональных данных в организации.

Планируемые результаты обучения по модулю 6

По итогам освоения модуля слушатели должны

знать:

— методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее;

— порядок создания автоматизированных систем в защищенном исполнении.

уметь:

— разрабатывать техническое задание на создание системы защиты информации в организации;

— разрабатывать разрешительную систему доступа к информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации;

— анализировать данные о назначении, функциях, условиях функционирования основных технических средств и систем, установленных на объектах информатизации, и характере обрабатываемой на них информации.

Учебно-тематический план модуля 6

№ п/п	Наименование разделов, модулей, тем	Всего часов	В том числе:		Формы контроля
			лекции	практические занятия	
Модуль 6.	Создание модели системы защиты персональных данных в организации	15	-	15	

Практическая работа № 1. Определение условий функционирования системы обработки персональных данных в организации	2	-	2	Проверка практической работы
Практическая работа № 2. Определение актуальных угроз безопасности персональных данных в организации при их обработке в информационной системе	2	-	2	
Практическая работа № 3. Определение необходимого уровня защищенности персональных данных в организации	2	-	2	
Практическая работа № 4. Определение перечня нормативно-правовых актов при определении/описании создаваемой с учетом уже существующих средств защиты персональных данных в организации	3	-	3	
Практическая работа № 5. Определение перечня организационно-распорядительных документов, необходимых для регламентации защиты персональных данных в организации	3	-	3	
Практическая работа № 6. Определение на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующих актуальных угроз безопасности в организации	3	-	3	

Содержание модуля 6

Создание модели системы защиты персональных данных в организации

Практическая работа № 1. Определение условий функционирования системы обработки персональных данных в организации.

Практическая работа № 2. Определение актуальных угроз безопасности персональных данных в организации при их обработке в информационной системе.

Практическая работа № 3. Определение необходимого уровня защищенности персональных данных в организации.

Практическая работа № 4. Определение перечня нормативно-правовых актов при определении/описании создаваемой с учетом уже существующих средств защиты персональных данных в организации.

Практическая работа № 5. Определение перечня организационно-распорядительных документов, необходимых для регламентации защиты персональных данных в организации.

Практическая работа № 6. Определение на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующих актуальных угроз безопасности в организации.

Содержание семинаров, практических занятий

№ темы	Наименование темы, по которой предусмотрено занятие семинарского типа	Формы и методы проведения
6.1.	Практическая работа № 1. Определение условий функционирования системы обработки персональных данных в организации	выполнение практического задания
6.2.	Практическая работа № 2. Определение актуальных угроз безопасности персональных данных в организации при их обработке в информационной системе	выполнение практического задания
6.3.	Практическая работа № 3. Определение необходимого уровня защищенности персональных данных в организации	выполнение практического задания
6.4.	Практическая работа № 4. Определение перечня нормативно-правовых актов при определении/описании создаваемой с учетом уже существующих средств защиты персональных данных в организации	выполнение практического задания
6.5.	Практическая работа № 5. Определение перечня организационно-распорядительных документов, необходимых для регламентации защиты персональных данных в организации	выполнение практического задания
6.6.	Практическая работа № 6. Определение на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующих актуальных угроз безопасности в организации	выполнение практического задания

Пример практического задания

Практическая работа № 1. Определение условий функционирования системы обработки персональных данных в организации

Задние 1. Определите условия функционирования системы обработки персональных данных в вашей организации, как объекта защиты.

Для этого необходимо описать:

- назначение системы и ее функции/задачи, которые она решает;
- правовое поле, в рамках которого система существуют и какие нормативные/контрактные требования на нее распространяются;
- какие компоненты/модули/подсистемы ее составляют и целевое назначения каждого модуля/подсистемы;
- состав прикладного и системного программного обеспечения, а также аппаратные компоненты, используемые в системе;
- территориальная распределенность /размещение системы и используемые каналы связи с указанием подключения к сетям общего пользования (включая сеть Интернет);

- взаимодействие с другими (включая сторонние, собственниками которых являются другие юридические лица) информационными системами (включая ИСПДн);
- пользователи системы, их уровни доступа и функции;
- сторонние компании, участвующие в эксплуатации и использовании системы, а также компании, которые имеют и/или могут в теории получать доступ к различным компонентам системы;
- условия администрирования системы;
- пользователи системы, их уровни доступа и функции;
- размещение физических компонент (площадки, границы контролируемых вашей компанией зон (далее – КЗ) на площадках, порядок доступа в КЗ, порядок обслуживания, обязательства контрагентов);
- перечень защищаемых информационных ресурсов системы и степень/уровень их конфиденциальности (включая отнесение к информации ограниченного доступа в соответствии (ФЗ РФ от 27.07.2006 № 149-ФЗ).

Практическая работа № 2. Определение актуальных угроз безопасности персональных данных в организации при их обработке в информационной системе

Задание 1. Определите актуальные угрозы безопасности персональных данных в вашей организации при их обработке в информационной системе.

Для этого необходимо учесть:

- оценка актуальности угроз проводится без учета применяемых технических средств защиты информации, (даже если они уже сейчас существуют/внедрены в систему, не должны учитываться - указанной позиции придерживается ФСТЭК России);
- любая сторонняя организация, даже если это дочернее лицо, рассматривается как потенциальный нарушитель (сведения об этом должны найти отражение в оценке потенциальных нарушителей, праве собственности/владении различными компонентами системы, порядке доступа к компонентам системы и т.д.);
- если компанией принимается решение об обеспечении

безопасности персональных данных с использованием средств криптографической защиты информации или механизмов, использующих/реализующих криптографические преобразования, то в рамках моделирования угроз необходимо будет кроме нормативно-методических документов ФСТЭК России использовать еще документы ФСБ России и определить необходимый класс криптозащиты;

- при моделировании угроз необходимо провести оценку актуального типа угроз, как установлено в п. 6 и 7 Постановление Правительства РФ от 1 ноября 2012 г. № 1119 (т.к. иначе вы не сможете определить необходимый уровень защищенности персональных данных).

Практическая работа № 3. Определение необходимого уровня защищенности персональных данных в организации

Задание 1. Определите необходимый уровень защищенности персональных данных в вашей организации.

Практическая работа № 4. Определение перечня нормативно-правовых актов при определении/описании создаваемой с учетом уже существующих средств защиты персональных данных в организации

Задание 1. Определите перечень нормативно правовых актов при определении /описании создаваемой с учетом уже существующих средств защиты системы защиты персональных данных в вашей организации.

Практическая работа № 5. Определение перечня организационно-распорядительных документов необходимых для регламентации защиты персональных данных в организации

Задание 1. Определите перечень организационно-распорядительных документов необходимых для регламентации защиты персональных данных в вашей организации.

При этом необходимо учесть:

- при разработке должны учитываться положения Постановление Правительства РФ от 1 ноября 2012 г. № 1119 и Постановление Правительства РФ от 15 сентября 2008 г. N 687;
- если компанией принято решение использовать для защиты персональных данных средства криптографической защиты информации, то необходимо учитывать Приказ ФАПСИ от 13 июня

2001 г. № 152.

Определить лиц, участвующих в обработке персональных данных и ответственных за обеспечение системы защиты персональных данных:

- ответственного за обеспечение безопасности персональных данных;
- администраторов средств защиты персональных данных
- пользователей криптосредств;
- пользователей системы;
- лиц, допущенных к электронному журналу сообщений и безопасности системы;
- лиц, допущенных в места размещения компонентов системы;
- лиц, допущенных к носителям персональных данных.

Для выполнения этой задачи используйте документ ФСТЭК России - Методический документ «Меры защиты информации в государственных информационных системах».

Практическая работа № 6. Определение на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующих актуальных угроз безопасности в организации

Задание 1. Определите на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующие актуальные угрозы безопасности в вашей организации.

Для этого необходимо учесть:

- если компанией принято решение использовать для защиты персональных данных средства криптографической защиты информации, то необходимо учитывать Приказ ФАПСИ от 13 июня 2001 г. № 152;
- если компанией принято решение использовать сертифицированные средства защиты информации в системе сертификации ФСТЭК России, то ей необходимо учитывать ограничения по эксплуатации и использованию, которые указаны в эксплуатационной документации (формуляры, паспорта и т.д.) на средства защиты;
- если компанией принято решение использовать сертифицированные ФСБ России средства криптографической защиты информации, то ей необходимо учитывать ограничения по

эксплуатации и использованию, которые указаны в правилах использования и эксплуатационной документации (формуляры, паспорта и т.д.) на средства защиты;

- если компанией принято решение использовать арендуемые у другой компании средства защиты или услуги по защите информации, то соответствующие положения в части оценки угроз, нарушителей и описание данных условий и механизмов должны найти отражение в разрабатываемых документах на систему защиты персональных данных, а компания, оказывающая услуги по защите информации, должна иметь лицензию ФСТЭК России на техническую защиту конфиденциальной информации (с соответствующим разрешенным видом деятельности), а для средств криптографической информации соответствующую лицензию ФСБ России.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, выполнения практических заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд электронной библиотеки, интернет-ресурсы и профессиональные информационные сервисы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и пособий, разработанные конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения. Индивидуальные консультации проводятся посредством возможностей электронного учебного курса (форум с преподавателем).

№ темы	Наименование (содержание) темы, по которой предусмотрена самостоятельная работа	Формы и методы проведения
6.1	Практическая работа № 1. Определение условий функционирования системы обработки персональных данных в организации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к выполнению практического задания
6.2	Практическая работа № 2. Определение актуальных угроз безопасности персональных данных в организации при их обработке в информационной системе	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к выполнению практического задания
6.3	Практическая работа № 3. Определение необходимого уровня защищенности персональных данных в организации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к выполнению практического задания
6.4	Практическая работа № 4. Определение перечня нормативно-правовых актов при определении/описании создаваемой с учетом уже существующих средств защиты персональных данных в организации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к выполнению практического задания
6.5	Практическая работа № 5. Определение перечня организационно-распорядительных документов, необходимых для регламентации защиты персональных данных в организации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к выполнению практического задания
6.6	Практическая работа № 6. Определение на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующих актуальных угроз безопасности в организации	Изучение основной и дополнительной литературы по программе; работа с интернет-сервисами правовых систем. Подготовка к выполнению практического задания. Подготовка к итоговой аттестации

Задания для самостоятельной работы:

Слушателю предлагается изучить основополагающие законодательные акты в области организации работ в области защиты информации

ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации:

— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
— Постановление Правительства РФ от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации»;
— Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»;
— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;

— Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
— Приказ Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
— Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
— Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
— Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
— Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
— Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
— Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
— Руководящий документ «Средства вычислительной техники. Защита от

несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);

— Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997 г.);
— Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997 г.);
— Руководящий документ «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин автоматизированных кассовых систем и требования по защите информации»;
— Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. решением Государственной технической комиссии при Президенте РФ от 04.06.1999 № 114);
— Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (введен в действие приказом Государственной технической комиссии при Президенте РФ от 19.06.2002 № 187);
— Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;
— Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.);
— ГОСТ Р 50752-95 «Информационная технология. Защита информации от

утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний».

— Межгосударственный стандарт ГОСТ 30373-95/ГОСТ Р 50414-92 «Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний» (введен в действие постановлением Госстандарта РФ от 15.05.1996 № 308);
— ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники».

Перечень основной и дополнительной учебной литературы, необходимой для освоения модуля 6

Основная литература

— Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва: Директ-Медиа, 2022. – 128 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – Библиогр.: с. 117-118. – ISBN 978-5-4499-3327-0. – DOI 10.23681/694670.
— Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / А. Г. Фабричнов, А. С. Дёмушкин, Т. В. Кондрашова, Н. Н. Куняев. – Москва: Логос, 2011. – 452 с. – (Новая университетская библиотека). – URL: https://biblioclub.ru/index.php?page=book&id=84996. – ISBN 978-5-98704-541-1.
— Безопасность электронного документооборота: учебное пособие: / П. А. Тищенко, Ю. М. Казаков, Р. А. Филиппов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 54 с. – URL: https://biblioclub.ru/index.php?page=book&id=602225. – Библиогр. в кн. – ISBN 978-5-4499-1928-1.
— Защита интеллектуальной собственности: учебник / И. К. Ларионов, М. А. Гуреева, В. В. Овчинников [и др.] ; под ред. И. К. Ларионова, М. А. Гуреевой, В. В. Овчинникова. – 5-е изд., стер. – Москва: Дашков и К°, 2023. – 256 с. – (Учебные издания для бакалавров). – URL:

https://biblioclub.ru/index.php?page=book&id=710103 – Библиогр. в кн. – ISBN 978-5-394-05367-2.

— Прохорова, О. В. Информационная безопасность и защита информации: учебник: / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.: табл., схем., ил. – URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн. – ISBN 978-5-9585-0603-3.

Дополнительная литература

— Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6.

— Корнилова, А. А. Защита персональных данных: учебное пособие: / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2020. – 119 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн.

Электронные ресурсы:

1. Электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/.
2. Российская государственная библиотека https://www.rsl.ru/.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-техническое оснащение Программы

Реализация Программы должна обеспечить приобретение слушателями профессиональных знаний и умений для выполнения их трудовых функций.

Выбор методов обучения для каждого занятия определяется преподавателем в соответствии с составом и уровнем подготовленности обучающихся, степенью сложности излагаемого материала, наличием и состоянием учебного оборудования, технических средств обучения, местом и продолжительностью проведения занятий.

Обучение производится с использованием дистанционных технологий, предусматривающих обеспечение обучающихся нормативными документами, учебно-методическими материалами и материалами для проведения проверки знания требований, обмен информацией между обучающимися, проходящими обучение, и лицами, проводящими обучение, посредством системы электронного обучения, участие обучающихся в интернет-конференциях, вебинарах, а также администрирование процесса обучения на основе использования компьютеров и информационно-телекоммуникационной сети «Интернет».

У слушателя должен быть персональный компьютер, оснащенный аудиоколонками, с доступом в сеть интернет и установленным видеоплеером, способным воспроизводить видеофайлы.

3.2. Кадровое обеспечение реализации программы

Педагогические работники, реализующие программу, должны удовлетворять квалификационным требованиям, указанным в квалификационных справочниках по соответствующим должностям и (или) профессиональных стандартах.

Информационно-методические условия реализации программы включают: учебный план, календарный учебный график, программы учебных предметов, методические материалы и разработки.

3.3. Информационное обеспечение программы

Нормативные документы:

- Конституция РФ;
- Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (КоАП РФ);
- Федеральный закон от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации»;

— Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;
— Федеральный закон от 03.04.1995 № 40-ФЗ «О федеральной службе безопасности»;
— Федеральный закон от 27.05.1996 № 57-ФЗ «О государственной охране»;
— Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
— Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;
— Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
— Федеральный закон от 27.12.2002 №184-ФЗ «О техническом регулировании»;
— Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
— Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
— Закон РФ от 21.07.1993 № 5485-I «О государственной тайне»;
— Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»;
— Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
— Указ Президента РФ от 07.08.2004 № 1013 «Вопросы Федеральной службы охраны Российской Федерации»;
— Указ Президента РФ от 16.08.2004 № 1082 «Вопросы Министерства обороны Российской Федерации»;
— Указ Президента РФ от 01.03.2011 № 248 «Вопросы Министерства внутренних дел Российской Федерации»;
— Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;
— Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
— Указ Президента РФ от 11.03.2003 № 308 «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации»;

— Постановление Правительства РФ от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации»;
— Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»;
— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
— Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
— Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
— Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;
— Постановление Правительства РФ от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации»;
— Постановление Правительства РФ от 18.05.2009 № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»;
— Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»;
— Постановление Правительства РФ от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к

охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения и о внесении изменения в Положение о сертификации средств защиты информации»;

— Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
— Постановление Правительства РФ от 21.03.2012 № 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»;
— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
— Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;

— Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
— Приказ Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
— Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
— Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
— Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
— Приказ Министерства труда и социальной защиты РФ от 09.08.2022 № 474н «Об утверждении профессионального стандарта «Специалист по технической защите информации»;
— Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
— Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
— Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к

информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);

— Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
— Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997 г.);
— Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997 г.);
— Руководящий документ «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин автоматизированных кассовых систем и требования по защите информации»;
— Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. решением Государственной технической комиссии при Президенте РФ от 04.06.1999 № 114);
— Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (введен в действие приказом Государственной технической комиссии при Президенте РФ от 19.06.2002 № 187);
— Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;
— Положение по аттестации объектов информатизации по требованиям

безопасности информации (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.);
— ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний».
— Межгосударственный стандарт ГОСТ 30373-95/ГОСТ Р 50414-92 «Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний» (введен в действие постановлением Госстандарта РФ от 15.05.1996 № 308);
— ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники».

Учебники и учебные пособия

— Защита интеллектуальной собственности: учебник / И. К. Ларионов, М. А. Гуреева, В. В. Овчинников [и др.] ; под ред. И. К. Ларионова, М. А. Гуреевой, В. В. Овчинникова. – 5-е изд., стер. – Москва: Дашков и К°, 2023. – 256 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=710103 – Библиогр. в кн. – ISBN 978-5-394-05367-2.
— Управление кадровой безопасностью организации: учебник для бакалавриата и магистратуры: / Ю. В. Долженкова, Е. В. Камнева, А. Л. Сафонов [и др.]; под ред. Ю. В. Долженковой; Финансовый университет при Правительстве Российской Федерации. – Москва: Прометей, 2022. – 286 с.: ил., табл., схем. –– URL: https://biblioclub.ru/index.php?page=book&id=700997. – Библиогр.: с. 245-256. – ISBN 978-5-00172-241-0.
— Мансуров, Г. З. Право цифровой безопасности: учебник: / Г. З. Мансуров. – Москва: Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – DOI 10.23681/687364.
— Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право,

2018. – 287 с.: ил. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6.

— Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / А. Г. Фабричнов, А. С. Дёмушкин, Т. В. Кондрашова, Н. Н. Куняев. – Москва: Логос, 2011. – 452 с. – (Новая университетская библиотека). – URL: https://biblioclub.ru/index.php?page=book&id=84996. – ISBN 978-5-98704-541-1.

— Прохорова, О. В. Информационная безопасность и защита информации: учебник: / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.: табл., схем., ил. – URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн. – ISBN 978-5-9585-0603-3.

— Андруник, А. П. Кадровая безопасность: инновационные технологии управления персоналом: учебное пособие / А. П. Андруник, М. Н. Руденко, А. Е. Суглобов. – 4-е изд. – Москва: Дашков и К°, 2024. – 508 с.: табл., схем. – (Учебные издания для вузов). – URL: https://biblioclub.ru/index.php?page=book&id=709776. – Библиогр. в кн. – ISBN 978-5-394-05699-4.

— Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва: Директ-Медиа, 2022. – 128 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – Библиогр.: с. 117-118. – ISBN 978-5-4499-3327-0. – DOI 10.23681/694670.

— Великанова, С. С. Информационные ресурсы кадровой службы : учебное пособие : / С. С. Великанова. – Москва: Директ-Медиа, 2022. – 144 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=683128. – Библиогр. в кн. – ISBN 978-5-4499-2892-4.

— Аверченков, В. И. Служба защиты информации: организация и управление: учебное пособие: / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 186 с.: ил., схем. –URL:

https://biblioclub.ru/index.php?page=book&id=93356. – Библиогр. в кн. – ISBN 978-5-9765-1271-9.

— Корнилова, А. А. Защита персональных данных: учебное пособие: / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2020. – 119 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн.

— Правовое регулирование информационных отношений в области государственной и коммерческой тайны, персональных данных: учебное пособие: / О. В. Ахрамеева, И. Ф. Дедюхина, О. В. Жданова [и др.]; Ставропольский государственный аграрный университет, Кафедра государственного и муниципального управления и права. – Ставрополь: Ставропольский государственный аграрный университет (СтГАУ), 2015. – 59 с. –URL: https://biblioclub.ru/index.php?page=book&id=438603.

— Информационные технологии в юридической деятельности: учебное пособие / С. Я. Казанцев, Н. М. Дубинина, А. И. Уринцов [и др.] под ред. А. И. Уринцова. – 2-е изд., перераб. и доп. – Москва: Юнити-Дана, 2020. – 353 с.: схем., табл, ил. – URL: https://biblioclub.ru/index.php?page=book&id=683023. – Библиогр.: с. 341. – ISBN 978-5-238-03242-9.

— Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / А. Г. Фабричнов, А. С. Дёмушкин, Т. В. Кондрашова, Н. Н. Куняев. – Москва: Логос, 2011. – 452 с. – (Новая университетская библиотека). – URL: https://biblioclub.ru/index.php?page=book&id=84996. – ISBN 978-5-98704-541-1.

— Безопасность электронного документооборота: учебное пособие: / П. А. Тищенко, Ю. М. Казаков, Р. А. Филиппов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 54 с. – URL: https://biblioclub.ru/index.php?page=book&id=602225. – Библиогр. в кн. – ISBN 978-5-4499-1928-1.

Доступ слушателя к электронной библиотеке осуществляется путем перехода по ссылке из кабинета пользователя системы дистанционного обучения. Логин и пароль для доступа в систему направляется слушателю на электронную почту работником учебного центра.

Электронные ресурсы:

1. Электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/.
2. Российская государственная библиотека https://www.rsl.ru/.

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Освоение Программы завершается итоговой аттестацией слушателей в форме - квалификационного экзамена.

Лицам, успешно освоившим Программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Результаты итоговой аттестации оформляются протоколом.

4.1. Контрольно-оценочные материалы (типовые задания) для оценки знаний

По окончании Программы осуществляется контроль уровня освоения заявленных компетенций в форме итоговой аттестации - квалификационного экзамена. Квалификационный экзамен проводится дистанционно.

В качестве экзаменационного задания слушателям необходимо выполнить тест, включающий 30 тестовых заданий. Тестовые задания подбираются случайно из всех вопросов, закрепленных за лекционными материалами в модулях обучения.

Предъявляемые слушателям тестовые задания – это задания закрытой формы с выбором одного или нескольких правильных ответов.

Итоги квалификационного экзамена оформляются локальным актом образовательной организации (протоколом).

При несогласии экзаменуемого с результатами квалификационного экзамена составляется акт, подписываемый членами экзаменационной комиссии и обучаемым, в котором отражается предмет спора. В этом случае в целях соблюдения гарантий объективности и независимости оценки качества подготовки, обучающемуся предоставляется возможность обратиться к руководству образовательной организации, а также к представителям работодателей и их объединений.

Типовые задания для проведения квалификационного экзамена

Правильный вариант ответа в тексте выделен жирным шрифтом

Модуль 1. Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных

Тема 1.1. Правовые основы технической защиты информации ограниченного доступа:

Вопрос 1. Целью информационной безопасности является обеспечение:

1. Понятности, полезности, доступности данных
2. **Доступности, целостности, конфиденциальности данных**
3. Сохранности данных

Вопрос 2. Система безопасности это:

1. Нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации
2. Нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия
3. **Организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающая защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз**

Вопрос 3. Что из перечисленного не входит в перечень задач, решаемых службой информационной безопасности:

1. Определение информационных и технических ресурсов, подлежащих защите
2. Выявление полного множества потенциально возможных угроз и каналов утечки информации
3. Определение требований к системе защиты информации
4. **Все пункты входят в перечень задач**

Вопрос 4. Государственная система лицензирования деятельности в области технической защиты информации включает в себя две составляющие:

1. **Допуск предприятий и организаций к оказанию услуг по защите информации**
2. Создание единой системы норм и регламентов деятельности служб, органов, реализующих защиту информации
3. **Контроль качества и эффективности оказываемых услуг в процессе их деятельности**

Вопрос 5. Обязательное подтверждение соответствия средств защиты информации требованиям по защите сведений соответствующей степени секретности осуществляется в формах:

1. Экспертизы соответствия
2. **Декларирования соответствия**
3. **Обязательной сертификации**

Вопрос 6. Субъект персональных данных имеет право:

1. **На получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных**
2. На доступ к персональным данных своих близких родственников
3. На доступ к персональным данных своих близких родственников при условии подачи запроса, содержащего номер основного документа, удостоверяющего личность субъекта

Вопрос 7. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. То есть целостность предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации - это:

1. Доступность
2. **Целостность**
3. Конфиденциальность

Вопрос 8. Защита от несанкционированного доступа к информации – это:

1. Доступность
2. Целостность
3. **Конфиденциальность**

Вопрос 9. Целью информационной безопасности является обеспечение:

1. Понятности, полезности, доступности данных

2. **Доступности, целостности, конфиденциальности данных**
3. Сохранности данных

Вопрос 10. Согласно терминологии Доктрины информационной безопасности РФ осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления – это:

1. **Обеспечение информационной безопасности**
2. Средства обеспечения информационной безопасности
3. Система обеспечения информационной безопасности

Вопрос 11. **Укажите, верно ли утверждение:** Реализация Доктрины осуществляется на основе отраслевых документов стратегического планирования РФ:

1. **Да**
2. Нет

Вопрос 12. Согласно Стратегии национальной безопасности РФ реализация органами публичной власти во взаимодействии с институтами гражданского общества и организациями политических, правовых, военных, социально-экономических, информационных, организационных и иных мер, направленных на противодействие угрозам национальной безопасности – это:

1. Национальная безопасность Российской Федерации
2. **Обеспечение национальной безопасности**
3. Угроза национальной безопасности
4. Система обеспечения национальной безопасности

Вопрос 13. Система безопасности это:

1. Нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия
2. **Организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающая защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз**
3. Нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода

методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации

Вопрос 14. Положения концепции предусматривают существование в рамках проблемы обеспечения безопасности информации в ИС:

1. **направление - защита информации от утечки по техническим каналам**
2. **направление - защита информации в ИС от несанкционированного доступа**
3. направление — защита информации в ИС от сбоев, ведущих к потере информации
4. направление - зашита от неавторизованного создания или уничтожения данных

Тема 1.2. Организационные основы технической защиты информации ограниченного доступа

Вопрос 1. Какие направления по обеспечению информационной безопасности Правительство РФ реализует в рамках своих полномочий:

1. разрабатывает и принимает на основе Конституции РФ законодательную базу в области обеспечения информационной безопасности
2. проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации
3. **разрабатывает федеральные целевые программы и выделяет необходимые финансовые средства для их реализации**
4. **осуществляет меры по предотвращению угроз информационной безопасности и организационному обеспечению этой деятельности**
5. **издает постановления и распоряжения в области обеспечения информационной безопасности и контролирует их обязательное исполнение**

Вопрос 2. Задачи и функции ФСБ России определены:

1. ФЗ «О Федеральной службе безопасности»
2. Стратегией национальной безопасности РФ
3. ФЗ «О безопасности»
4. **Положением о Федеральной службе безопасности Российской Федерации**

Вопрос 3. **Укажите, верно ли утверждение:** ФСО России в соответствии с законодательством РФ обеспечивает безопасность при подключении к сети Интернет федеральных органов государственной власти и органов государственной власти субъектов РФ:

1. **Да**
2. Нет

Вопрос 4. МВД России в рамках законодательства и в пределах своих полномочий обеспечивает:

1. организует деятельность по обеспечению информационной безопасности, защите государственной тайны в Вооруженных Силах
2. осуществляет разведывательную деятельность в интересах обороны и в пределах своей компетенции — в интересах безопасности Российской Федерации
3. **организацию предупреждения, выявления, пресечения, раскрытия и расследования преступлений, а также предупреждения и пресечения административных правонарушений, совершаемых в информационной сфере**

Вопрос 5. Укажите федеральный орган исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере обработки персональных данных, а также использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним:

1. **Минкомсвязи России**
2. Роскомнадзор России
3. ФСТЭК России

Вопрос 6. Укажите федеральный орган исполнительной власти, осуществляющим функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных, а также по защите прав субъектов персональных данных:

1. Минкомсвязи России
2. **Роскомнадзор России**
3. ФСТЭК России

Вопрос 7. Укажите федеральный орган исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности:

1. Минкомсвязи России
2. Роскомнадзор России
3. **ФСТЭК России**

Вопрос 8. Органы власти субъектов РФ в пределах предметов ведения:

1. **разрабатывают и принимают нормативные правовые акты в области обеспечения информационной безопасности**
2. обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности Российской Федерации
3. рассматривают проекты официальных документов по вопросам обеспечения информационной безопасности

Тема 1.3. Организационные основы технической защиты информации ограниченного доступа в организации

Вопрос 1. Что из перечисленного не входит в перечень задач, решаемых службой информационной безопасности:

1. Определение информационных и технических ресурсов, подлежащих защите
2. Выявление полного множества потенциально возможных угроз и каналов утечки информации
3. Определение требований к системе защиты информации
4. **Все пункты входят в перечень задач**

Вопрос 2. Что из перечисленного входит в компетенцию службы информационной безопасности организации:

1. **выявление нелояльных сотрудников**
2. мониторинг психологического климата в коллективе
3. адаптирование сотрудника к новому коллективу
4. контроль за исполнением сотрудником возложенных на него функций

Вопрос 3. Укажите, к каким средствам обеспечения информационной безопасности относятся криптографические средства защиты информации:

1. **методическим**

2. финансовым
3. нормативно-правовым
4. техническим

Вопрос 4. Укажите, в состав каких средств обеспечения информационной безопасности входит методическое обеспечение.

1. финансовое и материального
2. нормативно-правового
3. **технологического**

Вопрос 5. Государственная система лицензирования деятельности в области технической защиты информации включает в себя:

1. **Допуск предприятий и организаций к оказанию услуг по защите информации**
2. Создание единой системы норм и регламентов деятельности служб, органов, реализующих защиту информации
3. **Контроль качества и эффективности оказываемых услуг в процессе их деятельности**

Вопрос 6. Лицензирование деятельности по технической защите конфиденциальной информации осуществляет

1. **ФСТЭК России**
2. Минкомсвязи России
3. Роскомнадзор России

Тема 1.4. Сертификация средств защиты и аттестация объектов информатизации

Вопрос 1. Укажите срок, который должны обеспечить операторы федеральных государственных информационных систем при восстановлении информации, измененной или уничтоженной вследствие несанкционированного доступа к ней:

1. **не более 8 часов**
2. не более 12 часов
3. не более 24 часов
4. не более 3 дней

Вопрос 2. Согласно требованию какого документа допускается использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия:

1. **Положение о лицензировании деятельности по технической защите конфиденциальной информации**
2. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных
3. ФЗ «О техническом регулировании»

Вопрос 3. Согласно Постановлению правительства РФ 18 мая 2009 г. N 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» операторы федеральных государственных ИС обязаны обеспечить:

1. **защиту информации, содержащейся в информационных системах общего пользования, от уничтожения, изменения и блокирования доступа к ней**
2. **постоянный контроль возможности доступа неограниченного круга лиц к информационным системам общего пользования**
3. информационную безопасность при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям

Вопрос 4. Формой осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров называется:

1. **сертификация**
2. схема подтверждения соответствия
3. оценка соответствия
4. декларирование соответствия

Вопрос 5. Форма подтверждения соответствия продукции требованиям технических регламентов — это:

1. сертификация
2. схема подтверждения соответствия
3. оценка соответствия
4. **декларирование соответствия**

Вопрос 6. Обязательное подтверждение соответствия средств защиты информации требованиям по защите сведений соответствующей степени секретности осуществляется в формах:

1. Экспертизы соответствия

2. **Декларирования соответствия**
3. **Обязательной сертификации**

Вопрос 7. Форма и схемы обязательного подтверждения соответствия могут устанавливаться:

1. **техническим регламентом**
2. правительством РФ
3. государственными (контрактными) договорами

Вопрос 8. Что должен содержать технический регламент подтверждения соответствия?

1. **описание объектов технического регулирования**
2. **требования к объектам технического регулирования**
3. **правила их идентификации в целях применения технического регламента**
4. особенности оценки соответствия указанных объектов
5. все перечисленное

Вопрос 9. Срок действия декларации о соответствии определяется:

1. **техническим регламентом**
2. Федеральным органом исполнительной власти по техническому урегулированию
3. уполномоченным Правительством РФ Федеральным органом исполнительной власти

Вопрос 10. Форма сертификата соответствия:

1. определяется соответствующим техническим регламентом
2. **утверждается федеральным органом исполнительной власти по техническому регулированию**
3. утверждается уполномоченным Правительством РФ Федеральным органом исполнительной власти

Вопрос 11. Какой вид ЭП позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания:

1. простая электронная подпись
2. **усиленная неквалифицированная электронная подпись**
3. усиленная квалифицированная электронная подпись

Вопрос 12. У какого вида ЭП ключ проверки электронной подписи указан в квалифицированном сертификате:

1. простая электронная подпись
2. усиленная неквалифицированная электронная подпись

3. усиленная квалифицированная электронная подпись

Вопрос 13. Укажите, верно ли утверждение: к объектам информатизации, аттестуемыми по требованиям безопасности информации, помещения в которых установлены системы связи, предназначенные для обработки и передачи информации, подлежащей защите НЕ ОТНОСЯТСЯ:

1. Да
2. Нет

Вопрос 14. Что дает право обработки информации с определённым уровнем конфиденциальности на объекте информатизации:

1. наличие действующего «Аттестата соответствия»
2. наличие договора с уполномоченными федеральными органами по аттестации объектов информатизации по требованиям безопасности информации
3. перечень организационно-технических мероприятий, в результате которых подтверждается, что объект соответствует требованиям стандартов, утверждённых уполномоченными федеральными органами исполнительной власти

Вопрос 15. Укажите, кто несёт юридическую и финансовую ответственность за качество проведённых работ по аттестации объектов информатизации:

1. руководитель органа по аттестации объектов информатизации
2. сотрудники органа по аттестации объектов информатизации, проводившие работы
3. руководитель органа по аттестации объектов информатизации и сотрудники, проводившие работы

Вопрос 16. Укажите группу классов защищенности АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности:

1. 1 группа
2. 2 группа
3. 3группа

Модуль 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

Тема 2.1. Выявление угроз безопасности информации на объектах информатизации

Вопрос 1. К антропогенным источникам угроз информационной безопасности относятся:

1. Магнитные бури
2. **Представители надзорных организаций и аварийных служб**
3. Сети инженерных коммуникации

Вопрос 2. К антропогенным источникам угроз информационной безопасности относятся:

1. **Угроза безопасности объекта**
2. Источник угрозы
3. Уязвимость объекта
4. Атака

Вопрос 3. Возможное воздействие на объект, которое прямо или косвенно может нанести ущерб его безопасности – это:

1. **Угроза безопасности объекта**
2. Источник угрозы
3. Уязвимость объекта
4. Атака

Вопрос 4. Присущие объекту причины, приводящие к нарушению безопасности информации на объекте – это:

1. Угроза безопасности объекта
2. Источник угрозы
3. **Уязвимость объекта**
4. Атака

Вопрос 5. Укажите свойство информации быть известной только аутентифицированным законным ее владельцам или пользователям:

1. **Конфиденциальность информации**
2. Доступность информации
3. Целостность информации

Вопрос 6. Укажите нарушения при обеспечении конфиденциальности:

1. **утрата (неумышленная потеря, утечка) информации и средств ее обработки**
2. блокирование информации
3. отрицание подлинности информации

Вопрос 7. Укажите нарушения при обеспечении целостности:

1. хищение (копирование) информации и средств ее обработки
2. уничтожение информации и средств ее обработки
3. **модификация (искажение) информации**

Вопрос 8. Укажите критериев сравнения степень опасности, который определяет степень влияния уязвимости на неустранимость последствий реализации угрозы:

1. **Фатальность**
2. Доступность
3. Количество

Вопрос 9. К объективным уязвимостям информационной безопасности относятся:

1. **Сопутствующие техническим средствам излучения: электромагнитные, электрические, звуковые**
2. Ошибки (халатность) при подготовке и использовании программного обеспечения, эксплуатации технических средств; старение и размагничивание носителей информации
3. Отказы и неисправности технических средств, сбои программного обеспечения

Тема 2.2. Основные организационные меры защиты информации от несанкционированного доступа:

Вопрос 1. Аттестация НЕ является обязательной в случае:

1. Государственной тайны
2. Управлении экологически опасными объектами
3. **Деятельности медицинских учреждений**

Вопрос 2. В качестве заявителей аттестации могут выступать:

1. **заказчики, владельцы**
2. **разработчики аттестуемых объектов информатизации**
3. отраслевые и региональные учреждения
4. предприятия и организации по защите информации
5. специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию

Вопрос 3. В качестве органов по аттестации могут выступать:

1. заказчики, владельцы
2. разработчики аттестуемых объектов информатизации

3. отраслевые и региональные учреждения
4. предприятия и организации по защите информации
5. специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию

Вопрос 4. Укажите функции, осуществляемые в рамках аттестации органами по аттестации:

1. осуществление контроля за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией
2. формирование фонда нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке
3. рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации
4. организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации
5. проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации
6. предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию

Вопрос 5. Заключение договора между заявителем и органом по аттестации выполняется после:

1. подача и рассмотрение заявки на аттестацию
2. предварительного ознакомления с аттестуемым объектом
3. испытания в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте
4. разработки программы и методики аттестационных испытаний
5. проведение аттестационных испытаний объекта информатизации

Вопрос 6. **Укажите, верно ли утверждение:** Заключение по результатам аттестации подписывается членами аттестационной комиссии и представляется заявителю:

1. Да
2. **Нет**

Вопрос 7. Аттестат соответствия выдается:

1. **не более чем на 3 года**
2. не более чем на год
3. не более чем на 2 года

Вопрос 8. Утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77 определяет порядок организации и проведения работ по аттестации объектов информатизации:

1. **на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну**
2. на соответствие требованиям о защите информации ограниченного доступа, составляющей государственную тайну
3. на соответствие требованиям о защите информации ограниченного доступа

Вопрос 9. Назначение экспертов органов по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну из числа работников, участвующих в разработке и (или) внедрении системы защиты информации объекта информатизации:

1. **не допускается**
2.
3. допускается

Вопрос 10. Срок проведения работ по аттестации объекта информатизации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну:

1. **устанавливается владельцем объекта информатизации по согласованию с органом по аттестации**
2. устанавливается владельцем объекта информатизации без согласования с органом по аттестации
3. устанавливается органом по аттестации
4. **не может превышать четырех месяцев**

5. не может превышать одного месяца
6. не может превышать трех месяцев

Вопрос 11. В ходе аттестационных испытаний объекта информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну владельцем объекта информатизации:

1. **могут вноситься изменения в объект информатизации, с том числе в архитектуру его системы защиты информации**
2. не могут вноситься изменения в объект информатизации

Вопрос 12. Укажите пропущенное словосочетание: Заключение и протоколы в течение _____ после утверждения органом по аттестации объекта информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, направляются владельцу объекта информатизации:

1. **5 рабочих дней**
2. 5 дней
3. 3 рабочих дней
4. 3 дней
5. 10 дней

Вопрос 13. Укажите срок, в который протоколы контроля защиты информации ограниченного доступа, не составляющей государственную тайну, предоставляются на аттестованном объекте информатизации предоставляются в ФСТЭК России (территориальный орган ФСТЭК России):

1. **не реже одного раза в два года**
2. не реже одного раза в три года
3. не реже одного раза в год
4. не предоставляются

Вопрос 14. Укажите, что является основанием для приостановления действия аттестата соответствия:

1. **непредставление протоколов контроля защиты информации в ФСТЭК России (территориальный орган ФСТЭК России)**
2. любые изменения архитектуры системы защиты информации аттестованного объекта информатизации
3. **не устранение недостатков, выявленных ФСТЭК России (территориальным органом ФСТЭК России)**

Тема 2.3. Основные технические и программные средства защиты информации от несанкционированного доступа

Вопрос 1. Программная закладка «троянский конь» это:

1. **Программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба**
2. Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения
3. Тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей

Вопрос 2. Для обнаружения вирусов антивирусные программы используют следующие методы:

1. **Сигнатурный**
2. Дедуктивный
3. Эвристический

Вопрос 3. Укажите троянскую программу, которая способна выполнять удаленное управление зараженным компьютером:

1. **Backdoor**
2. Rootkit
3. Trojan-Dropper

Вопрос 4. Укажите троянскую программу, которая способна выполнять удаленное управление зараженным компьютером:

1. **Trojan-Notifier**
2. Trojan-PSW
3. Trojan-DDoS

Вопрос 5. Стадии жизненного цикла классического трояна:

1. **активация**
2. **выполнение вредоносных действий**
3. **проникновение на чужой компьютер**
4. поиск объектов для заражения
5. внедрение копий
6. подготовка копий

Вопрос 6. Подозрительная сетевая активность может быть вызвана ...

1. логической бомбой
2. **сетевым червем**
3. трояном
4. **P2P-червем**

Вопрос 7. Антивирусные базы можно обновить на компьютере, не подключенном к Интернет:

1. нет
2. **да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы**
3. да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором

Вопрос 8. Преимущества эвристического метода антивирусной проверки над сигнатурным:

1. **более надежный**
2. не требует регулярного обновления антивирусных баз
3. **существенно менее требователен к ресурсам**
4. позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

Модуль 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

Тема 3.1. Угрозы безопасности информации

Вопрос 1. Какие угрозы безопасности информации являются преднамеренными:

1. ошибки персонала
2. открытие электронного письма, содержащего вирус
3. **не авторизованный доступ**

Вопрос 2. Целью создания любой компьютерной сети является:

1. **удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (при необходимости)**
2. сохранение конфиденциальности и достоверности информации
3. своевременное получение информации

Вопрос **3.** Конфиденциальностью называется:

1. защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
2. описание процедур
3. **защита от несанкционированного доступа к информации**

Вопрос **4.** Естественные угрозы безопасности информации вызваны:

1. деятельностью человека
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3. **воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека**
4. корыстными устремлениями злоумышленников
5. ошибками при действиях персонала

Вопрос **5.** Искусственные угрозы безопасности информации вызваны:

1. **деятельностью человека**
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
4. корыстными устремлениями злоумышленников
5. ошибками при действиях персонала

Вопрос **6.** Укажите принцип действия устройства, позволяющего на расстоянии фиксировать разговор в помещении с закрытыми окнами:

1. **анализ отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн**
2. преобразование механических колебаний стекол в электрический сигнал с последующей передачей по радиоканалу
3. преобразование акустических колебания в электрические

Вопрос **7.** Укажите принцип действия стетоскопного микрофона:

1. анализ отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн
2. преобразование механических колебаний стекол в электрический сигнал с последующей передачей по радиоканалу
3. **преобразование акустических колебания в электрические**

Вопрос 8. Электромагнитные излучения используются злоумышленниками для:

1. получения информации
2. уничтожения информации
3. **получения и уничтожения информации**

Вопрос 9. Закладка – это:

1. **несанкционированное изменение структуры компьютерной сети**
2. обход средств защиты информации
3. использование привилегированных режимов работы

Вопрос 10. Программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах и выполняемые только при соблюдении определенных условий называются:

1. **Логические бомбы**
2. Черви
3. Троянские кони
4. Компьютерные вирусы

Вопрос 11. Программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии называются:

1. Логические бомбы
2. **Черви**
3. Троянские кони
4. Компьютерные вирусы

Тема 3.2. Утечка информации

Вопрос 1. Какой из пунктов не относится к видам каналов утечки информации с точки зрения физической природы:

1. Визуально-оптические, акустические
2. **Фотонные, динамические**
3. Электромагнитные, материально-вещественные

Вопрос 2. **Укажите, верно ли утверждение:** Большая часть причин и условий, создающих предпосылки и возможность утечки конфиденциальной информации, возникает из-за недоработок руководителей предприятий и их сотрудников:

1. **Да**
2. Нет

Вопрос 3. **Укажите, верно ли утверждение:** С позиции передачи информации человек рассматривается как носитель информации:

1. Да
2. **Нет**

Вопрос 4. Под структурным звуком понимают:

1. **механические колебания в твердых средах**
2. распространение звука в воздушном пространстве
3. распространение звука в воде

Вопрос 5. Утечка информации – это …

1. процесс раскрытия секретной информации
2. **несанкционированный процесс переноса информации от источника к злоумышленнику**
3. процесс уничтожения информации
4. непреднамеренная утрата носителя информации

Тема 3.3. Защита информации от утечки

Вопрос 1. Защита информации от утечки, это деятельность по предотвращению:

1. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации
2. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений
3. **неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа**
4. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации

Вопрос 2. Защита информации это:

1. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа
2. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
3. **деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё**

Вопрос 3. К посторонним лицам нарушителям информационной безопасности относится:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации
2. пользователи
3. сотрудники службы безопасности
4. **представители конкурирующих организаций**
5. лица, нарушившие пропускной режим

Вопрос 4. Аэрозольные завесы и дымообразующие вещества используются в качестве защиты информации от утечки по:

1. **визуально-оптическому каналу**
2. техническим каналам
3. акустическим каналам
4. электромагнитным каналам

Вопрос 5. Для общих целей используется шумомер:

1. нулевого класса
2. первого класса
3. **второго класса**
4. третьего класса

Вопрос 6. Укажите класс шумомеров, которые чаще всего используются на практике для оценки степени защищенности акустических каналов:

1. нулевого класса
2. первого класса
3. **второго класса**
4. третьего класса

Вопрос 7. Электростатическое экранирование:

1. **заключается в замыкании силовых линий электростатического поля источника на поверхность экрана и отводе наведенных зарядов на массу и на землю**
2. основано на замыкании силовых линий магнитного поля источника в толще экрана, обладающего малым магнитным сопротивлением для постоянного тока и в области низких частот

Вопрос 8. Укажите особенно опасные нежелательные излучения:

1. **побочные электромагнитные излучения (ПЭМИ)**
2. внеполосные
3. шумовые

Вопрос 9. Установка экранирующих устройств может производиться:

1. в непосредственной близости от источника излучения
2. на самом источнике
3. **оба варианта верны**

Вопрос 10. Паразитные емкостные связи обусловлены:

1. **электрической емкостью между элементами, деталями и проводниками устройств, несущих потенциал сигнала**
2. наличием взаимоиндукции между проводниками и деталями аппаратуры, главным образом между его трансформаторами
3. возникновением между выводными проводниками усилительных элементов, образующими колебательную систему с распределенными параметрами и резонансной частотой определенного порядка

Вопрос 11. **Укажите, верно ли утверждение:** Применение коаксиальных кабелей и волоконно-оптических линий практически полностью решает проблему защиты цепей и трактов линий связи от взаимного влияния.

1. **Да**
2. Нет

Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Тема 4.1. Основные понятия обработки персональных данных

Вопрос 1. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц – это:

1. **Распространение персональных данных**

2. Уничтожение персональных данных
3. Обезличивание персональных данных
4. Предоставление персональных данных

Вопрос 2. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц:

1. Распространение персональных данных
2. Уничтожение персональных данных
3. Обезличивание персональных данных
4. **Предоставление персональных данных**

Вопрос 3. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию:

1. **по достижении целей обработки**
2. **в случае утраты необходимости в достижении этих целей**
3. в случае обнаружения ошибки ввода данных
4. в случае использования персональных данных в другой информационной системе

Вопрос 4. **Укажите, верно ли утверждение:** Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных:

1. **Да**
2. Нет

Вопрос 5. **Укажите, верно ли утверждение:** Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано получать согласие субъекта персональных данных на обработку его персональных данных:

1. Да
2. **Нет**

Вопрос 6. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет:

1. **оператор**
2. лицо, осуществляющее обработку персональных данных по поручению оператора
3. ответственность не определена

Тема 4.2. Субъект персональных данных

Вопрос 1. Укажите, верно ли утверждение: Субъект персональных данных не вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки:

1. Да
2. **Нет**

Вопрос 2. Сведения предоставляются субъекту персональных данных или его представителю оператором в течение:

1. **десяти рабочих дней с момента обращения**
2. пяти рабочих дней с момента обращения
3. трех рабочих дней с момента обращения

Вопрос 3. Срок предоставления сведений субъекту персональных данных или его представителю оператором может быть продлен в случае:

1. **направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации**
2. направления оператором в адрес субъекта персональных данных мотивированного уведомления без указания причин продления срока предоставления запрашиваемой информации
3. не может быть продлен

Вопрос 4. Уведомление с указанием причин продления срока предоставления запрашиваемой информации:

1. **может быть направлен в форме электронного документа и подписан электронной подписью**
2. может быть направлен в форме электронного документа, подпись электронной подписью необязательна
3. не может быть направлен в форме электронного документа

Вопрос 5. Укажите, верно ли утверждение: Согласие на обработку персональных данных не может быть отозвано субъектом персональных данных.

1. Да
2. **Нет**

Вопрос 6. Укажите, верно ли утверждение: Обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

1. **Да**
2. Нет

Тема 4.3. Оператор персональных данных

Вопрос **1. Укажите, верно ли утверждение:** Оператор может быть освобожден от обязанности предоставить субъекту персональных данных сведения.

1. **Да**
2. Нет

Вопрос **2.** Перед кем оператор персональных данных несет ответственность?

1. **Перед субъектом персональных данных**
2. Перед Роскомнадзором
3. Вышестоящей организацией

Вопрос **3.** Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных:

1. В течение 3 рабочих дней после начала обработки
2. В течение 10 рабочих дней после начала обработки
3. **До начала обработки**
4. В течение 7 рабочих дней после начала обработки

Вопрос **4. Укажите, верно ли утверждение:** Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей по обработке персональных данных.

1. **Да**
2. Нет

Тема 4.4. Меры по обеспечению безопасности персональных данных

Вопрос **1.** Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться:

1. **на материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения**
2. на любых материальных носителях информации
3. на материальных носителях информации и с обеспечением защиты этих данных от неправомерного или случайного доступа к ним

Вопрос 2. Управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа обеспечивают:

1. **Меры по управлению доступом**
2. Меры по идентификации и аутентификации
3. Меры по ограничению программной среды

Вопрос 3. Обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации обеспечивают

1. **Меры по антивирусной защите**
2. Меры по ограничению программной среды
3. Меры по обнаружению (предотвращению) вторжений

Вопрос 4. Защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных обеспечивают

1. **Меры по защите информационной системы, ее средств, систем связи и передачи данных**
2. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных
3. Меры по ограничению программной среды

Вопрос 5. В информационных системах 1 уровня защищенности персональных данных применяются:

1. **средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса**
2. средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса
3. средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 6 класса

Вопрос 6. В информационных системах 4 уровня защищенности персональных данных применяются:

1. средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса
2. средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса
3. **средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 6 класса**

Вопрос 7. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать:

1. Управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа
2. **Присвоение субъектам и объектам доступа уникального признака, сравнение предъявляемого субъектом (объектом) доступа уникального признака с перечнем присвоенных уникальных признаков**

Вопрос 8. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1. **Уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных**
2. **Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных**
3. Правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также процедуру регистрации и учета всех действий

Тема 4.5. Обработка персональных данных

Вопрос 1. В случае изменений сведений в оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных обо всех произошедших за указанный период изменениях:

1. **не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения**
2. не позднее 30-го числа месяца, следующего за месяцем, в котором возникли такие изменения
3. не позднее 3-го числа месяца, следующего за месяцем, в котором возникли такие изменения

Вопрос 2. В случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение:

1. **10 рабочих дней с даты прекращения обработки персональных данных**
2. 30 рабочих дней с даты прекращения обработки персональных данных
3. 5 рабочих дней с даты прекращения обработки персональных данных

Вопрос 3. Уполномоченный орган по защите прав субъектов персональных данных вносит сведения реестр операторов в течение:

1. **30 дней с даты поступления уведомления об обработке персональных данных**
2. 10 дней с даты поступления уведомления об обработке персональных данных
3. 90 дней с даты поступления уведомления об обработке персональных данных

Вопрос 4. Лицо, ответственное за организацию обработки персональных данных, получает указания:

1. **от исполнительного органа организации, являющейся оператором**
2. от уполномоченного органа по защите прав субъектов персональных данных

Вопрос 5. Лицо, ответственное за организацию обработки персональных данных НЕ обязано:

1. осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных
2. доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных,

локальных актов по вопросам обработки персональных данных, требований к защите персональных данных

3. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов
4. **осуществлять сбор сведений, относящейся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных)**

Вопрос 6. Обработка персональных данных считается неавтоматизированной, если такие действия с персональными данными осуществляются:

1. **при непосредственном участии человека**
2. без использования информационной системы
3. без использования персонального компьютера

Вопрос 7. Свойство обезличенных данных, обеспечивающее сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания называется:

1. **Полнота**
2. Структурированность
3. Релевантность

Вопрос 8. Свойство обезличенных данных, обеспечивающее невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации называется:

1. **Анонимность**
2. Структурированность
3. Релевантность

Вопрос 9. Свойство обезличенных данных, обеспечивающее сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания, называется:

1. Анонимность
2. **Структурированность**
3. Релевантность

Вопрос 10. Метод обезличивания, заключающийся в разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств, называется:

1. метод введения идентификаторов
2. метод изменения состава или семантики
3. **метод декомпозиции**
4. метод перемешивания

Вопрос 11. Укажите метод обезличивания, НЕ обеспечивающий полноту обезличенных данных:

1. **Метод изменения состава или семантики**
2. Метод введения идентификаторов
3. Метод декомпозиции

Вопрос 12. Укажите метод, который может использоваться совместно с методами введения идентификаторов и декомпозиции:

1. **Метод перемешивания**
2. Метод изменения состава или семантики

Тема 4.6. Нарушения законодательства РФ в области персональных данных

Вопрос 1. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, влечет наложение административного штрафа на должностных лиц в размере:

1. от одной тысячи до трех тысяч рублей
2. **от пяти тысяч до десяти тысяч рублей**
3. от десяти тысяч до двадцати тысяч рублей
4. от тридцати тысяч до пятидесяти тысяч рублей

Вопрос 2. Какой размер штрафа установлен для организации за не опубликование политики по обработке и защите персональных данных?

1. от семисот до одной тысячи пятисот рублей
2. от трех тысяч до шести тысяч рублей
3. от пяти тысяч до десяти тысяч рублей
4. **от пятнадцати тысяч до тридцати тысяч рублей**
5. от двадцати пяти тысяч до сорока пяти тысяч рублей

Вопрос 3. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных влечет предупреждение или наложение административного штрафа:

1. **на должностных лиц**
2. на юридических лиц
3. на индивидуальных предпринимателей
4. на граждан

Вопрос **4.** Нарушение законодательства Российской Федерации в области персональных данных регламентировано:

1. **КоАП РФ**
2. УК РФ
3. ТК РФ
4. НК РФ

Вопрос **5. Укажите, верно ли утверждение:** Увольнение работника (при наличии всех признаков дисциплинарного проступка) за разглашение персональных данных невозможно в случае, если он не проконтролировал исполнение требования о хранении персональных данных:

1. Да
2. **Нет**

Вопрос **6.** Укажите нормативно-правовой акт, который устанавливает ответственность в случаях превышения должностными лицами работодателя своих полномочий по доступу к информации о частной жизни работника:

1. **УК РФ**
2. ТК РФ
3. КоАП РФ

Вопрос **7.** Укажите нормативно-правовой акт, который устанавливает ответственность за нарушение права работников на свободный бесплатный доступ к своим персональным данным:

1. **КоАП РФ**
2. УК РФ
3. ТК РФ

Модуль 5. Меры безопасности, применяемые при обработке персональных данных в информационных системах

Тема 5.1. Типовые программно-технические средства защиты информации

Вопрос **1.** Некоторая последовательность символов, сохраняемая в секрете и предъявляемая пользователем при обращении к компьютерной системе:

1. аутентификатор

2. **пароль**
3. идентификатор

Вопрос 2. Устройство, программа, которые осуществляют фильтрацию данных на основе заранее заданной базы правил:

1. авторизация
2. мониторинг
3. **межсетевой экран**

Вопрос 3. Основная задача брандмауэра:

1. защита сети от удаленных атак
2. **выполняет функцию внешнего маршрутизатора**
3. защита от вирусов
4. запрещает доступ к любым другим компьютерам

Вопрос 4. Укажите брандмауэр, позволяющий контролировать тип и объем трафика, поступающего на узел:

1. Брандмауэр сетевого уровня
2. **Брандмауэры уровня приложения**
3. Брандмауэр уровня соединения

Вопрос 5. Сколько ключей используется в системах с открытым ключом?

1. 1
2. **2**
3. 3

Вопрос 6. Электронной подписью называется:

1. **присоединяемое к тексту его криптографическое преобразование**
2. текст
3. зашифрованный текст

Вопрос 7. Укажите, верно ли утверждение: В системах электронных платежей применяется «слепая подпись»:

1. **Да**
2. Нет

Тема 5.2. Организация защиты персональных данных в организации

Вопрос 1. Укажите наиболее часто встречающуюся формулировку жалобы в области персональных данных на действия работодателя:

1. **«распространение информации о работнике третьим лицам»**
2. «нарушение права работников на свободный бесплатный доступ к своим персональным данным»

3. «несвоевременное предоставление запрошенной информации»

Вопрос 2. Какой нормативно-правовой акт закрепляет права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя:

1. ТК РФ
2. УК РФ
3. КоАП РФ

Вопрос 3. В каком случае работодатель вправе разглашать персональные данные работника третьей стороне или в коммерческих целях:

1. если работник дал устное согласие
2. если работник дал письменное согласие
3. если работник дал письменное согласие, заверенное нотариусом

Вопрос 4. Работодатель не нарушит права работника в сфере персональных данных если передал персональные данные работника:

1. в пределах одной организации
2. по мотивированному запросу только специально уполномоченным лицам
3. новому работодателю
4. в пределах организаций партнеров

Вопрос 5. Являются ли следующие сведения о сотрудниках: фамилии, имена и отчества, занимаемые ими должности, с указанием структурных подразделений, сведения о номерах корпоративных и внутренних телефонов, адреса их электронной почты персональными данными?

1. Да
2. Нет