Автономная некоммерческая организация
дополнительного профессионального образования
«Международный университет профессиональных инноваций»

Утверждаю
Ректор
_____
В.В.Калашникова
Приказ № 30
«27» февраля 2023 г.

Образовательная программа
дополнительного профессионального образования

«Защита информации и защита персональных данных»

Тип программы: повышение квалификации

Количество часов: 72 часа

Документ по итогам обучения:
удостоверение о повышении квалификации

Москва
2023

Образовательная программа дополнительного профессионального образования повышения квалификации **«Защита информации и защита персональных данных»** – М.: МУПИ, 2023. – 29 с.
Программа подготовлена авторским коллективом АНО ДПО «Международный университет профессиональных инноваций».

Оглавление

Раздел 1. Общие положения
1.1. Пояснительная записка
1.2. Требования к результатам освоения программы
1.3. Характеристика обучения
2. Содержание программы
2.1. Учебный план
2.2. Календарный учебный график
2.3. Рабочие программы дисциплин (модулей)
2.4. Организация самостоятельной работы обучающихся
3. Условия реализации программы
3.1. Материально-технические условия реализации программы
3.2.Учебно-методическое обеспечение программы
4. Оценка качества освоения программы
5. Организационно-педагогические условия реализации программы

Раздел 1. Общие положения

1.1. Пояснительная записка

Дополнительная профессиональная программа **«Защита информации и защита персональных данных»** (далее - Программа), разработана в соответствии с:

1. Федерального закона «Об образовании в Российской Федерации» от 29.12.2012г. №273-ФЗ,

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

3. Приказа Минобрнауки РФ от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

4. Письмом Минобрнауки России от 22.04.2015 № ВК-1032/06 «О направлении методических рекомендаций» (вместе с «Методическими рекомендациями-разъяснениями по разработке дополнительных профессиональных программ на основе профессиональных стандартов),

5. Приказом Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. N 499 г. Москва "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам",

6. Единого квалификационного справочника с указанием конкретной должности/ профессии - ЕКС. Общеотраслевые квалификационные характеристики должностей работников, занятых на предприятиях, в учреждениях и организациях. Постановление Минтруда РФ от 21.08.1998 № 37,

7. Методических рекомендаций по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (Утверждено Министром образования и науки Российской Федерации 22 января 2015 г. № ДЛ-1/05вн),

8. Приказ Минобрнауки России от 17.11.2020 N 1427 "Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность" (Зарегистрировано в Минюсте России 18.02.2021 N 62548)

9. Профессиональным стандартом Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н «Специалист по защите информации в автоматизированных системах».

Дополнительные профессиональные программы — это программы повышения квалификации и программы профессиональной переподготовки (далее: ДПП).

Цель обучения: Повышение защищенности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости.

К освоению дополнительных профессиональных программ допускаются: лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование на основании Федерального Закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» ст. 76 п.3.

Продолжительность (трудоемкость) обучения: 72 академических часа, 2 недели. Для всех видов занятий академический час устанавливается продолжительностью 45 минут.

Форма обучения: очно-заочно с применением исключительно электронного обучения и дистанционных образовательных технологий.

Режим занятий: 8 академических часов в день, 40 часов в неделю.

1.2. Требования к результатам освоения программы

Цель программы: совершенствование профессиональных компетенций необходимых для слушателя в рамках имеющейся квалификации.

Планируемые результаты обучения направлены на совершенствование профессиональных компетенций, профессиональных знаний, умений, навыков. В планируемых результатах отражается преемственность с профессиональными стандартами и квалификационными характеристиками должностей.

В результате изучения программы слушатель должен знать:

- Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях
- Базовая конфигурация системы защиты информации автоматизированной системы
- Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах.
- Типовые средства, методы и протоколы идентификации, аутентификации и авторизации.
- Нормативные правовые акты в области защиты информации.
- Организационные меры по защите информации.

В результате изучения программы слушатель должен уметь:

- Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией.
- Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации.
- Производить монтаж и диагностику компьютерных сетей.
- Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи.

По окончании обучения должен владеть навыками:

- Проверка работоспособности системы защиты информации автоматизированной системы
- Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации
- Контроль стабильности характеристик системы защиты информации автоматизированной системы

Характеристика новой квалификации и связанных с ней видов профессиональной деятельности, трудовых функций и (или) уровней квалификации.

У обучающегося совершенствуются следующие компетенции:

- Способность администрировать средства защиты информации в компьютерных системах и сетях (ПК – 1)
- Способность обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям (ПК – 2)
- Способность обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям (ПК – 3)
- Способность проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников

информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба (ПК – 4)

- Способность разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности (ПК – 5)

- Способность проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам (ПК- 6)

Таблица соответствия компетенций дисциплинам (модулям) учебного плана

	Наименование дисциплин	ПК1	ПК2	ПК3	ПК4	ПК5	ПК 6
1	Основные вопросы технической защиты информации	+	+			+	+
2	Нормативно- правовое обеспечение защиты персональных данных		+		+		
3	Угроза и уязвимости безопасности персональных данных при их обработке в информационных системах			+			+
4	Организационные и технические мероприятия по защите персональных данных в информационных системах	+			+		+
5	Итоговая аттестация				+		+

1.3. Характеристика обучения

Нормативная трудоемкость обучения по данной программе – 72 часа, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

Форма обучения: Очная (с отрывом от работы), очно-заочная (с частичным отрывом от работы), заочная (без отрыва от работы). При реализации программы применяется форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебного плана, использовании различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения.

При любой форме обучения учебная нагрузка устанавливается не более 54 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

2. Содержание программы

Программа включает в себя: цель, планируемые результаты обучения, учебный план, календарный учебный график, рабочие программы учебных предметов, курсов, дисциплин (модулей), организационно-педагогические условия, формы аттестации, оценочные материалы и иные компоненты.

Допускается зачет модулей, освоенных в процессе предшествующего обучения по Программе, при условии совпадения тематики и времени освоения соответствующих дисциплин (модулей) с указанными в Программе.

2.1. Учебный план

Программа дополнительного профессионального образования повышения квалификации по курсу: «**Защита информации и защита персональных данных**».

Категория слушателей - лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование на основании Федерального Закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» ст. 76 п.3.

Срок обучения – 72 часа.

Форма обучения - очно-заочно с применением исключительно электронного обучения и дистанционных образовательных технологий.

№ п/п	Наименование дисциплин (модулей, курсов), разделов, тем	Общая трудоемкость, ч	В том числе:		СРС, ч	Формы контроля
			лекции	практические и семинарские занятия		
1	Основные вопросы технической защиты информации	16	2	7	7	Зачет
2	Нормативно- правовое обеспечение защиты персональных данных.	18	4	8	6	Зачет
3	Угроза и уязвимости безопасности персональных данных при их обработке в информационных системах	16	2	7	7	Зачет
4	Организационные и технические мероприятия по защите персональных данных в информационных системах	20	3	7	10	Зачет
5	**Итоговая аттестация**	2		2		Зачет
	Итого	72	11	31	30	Зачет

КП - курсовой проект, КР - курсовая работа, РК - контрольная работа, РГР - расчетно-графическая работа, Реф. –реферат.

Промежуточная аттестация: В соответствующей графе указывается количество и технология приема: «Т» - прием, осуществляемый по традиционной образовательной технологии; «Д» - прием, осуществляемый с использованием дистанционных образовательных технологий.

2.2. Календарный учебный график

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный месяц	**День освоения программы**	**Дисциплины (модули) программы (указываются номера дисциплин (модулей) согласно учебного плана программы)**	**Количество часов Учебной нагрузки**
1	2	3	4
День, в котором проводится обучение по программе **Режим занятий** **ПН - ПТ**	1 день	Основные вопросы технической защиты информации	8
	2 день	Основные вопросы технической защиты информации.	8
	3 день	Нормативно- правовое обеспечение защиты персональных данных.	8
	4 день	Нормативно- правовое обеспечение защиты персональных данных.	8
	5 день	Нормативно- правовое обеспечение защиты персональных данных. Угроза и уязвимости безопасности персональных данных при их обработке в информационных системах	2 6
	6 день	Угроза и уязвимости безопасности персональных данных при их обработке в информационных системах	8
	7 день	Угроза и уязвимости безопасности персональных данных при их обработке в информационных системах Организационные и технические мероприятия по защите персональных данных в информационных системах	2 6
	8 день	Организационные и технические мероприятия по защите персональных данных в информационных системах	8
	9 день	Организационные и технические мероприятия по защите персональных данных в информационных системах Итоговая аттестация	6 2
72 часа, 2 недели, 40 часов в неделю.			

2.3 Содержание модулей программы

Раздел 1. Общие вопросы технической защиты информации.

1.1. Основные понятия и определения.

Актуальность проблемы защиты персональных данных в информационных системах.

Основные понятия информационной безопасности.

Федеральный закон «Об информации, информационных технологиях и защите информации».

2. Нормативно- правовое обеспечение защиты персональных данных.

Международное и национальное право в области защиты персональных данных.

Конвенция «О защите физических лиц при автоматизированной обработке персональных данных». Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных. Директива в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи. Дополнительный протокол о защите частных лиц в отношении автоматизированной обработки данных личного характера, о наблюдательных органах и трансграничной передаче информации.

Федеральное законодательство Российской Федерации в области защиты персональных данных. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к материальным носителям биометрических персональных данных.

Содержание и основные положение Федерального Закона Российской Федерации «О персональных данных» № 152-ФЗ. Общие положения закона. Принципы и условия обработки персональных данных. Принципы обработки персональных данных. Категории персональных данных. Права субъекта персональных данных. Обязанности оператора персональных данных.

Специальные нормативные документы по технической защите сведений конфиденциального характера. Нормативно-методические документы ФСТЭК РФ. Нормативно-методические документы ФСБ РФ.

Раздел 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных.

3. Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах.

Основные принципы моделирования угроз с использованием методических документов ФСТЭК и ФСБ. Угрозы информационной безопасности. Общая характеристика уязвимостей информационной системы персональных данных.

Наиболее часто реализуемые угрозы. Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации в информационной системе персональных данных.

Методология формирования модели угроз с использованием Методических рекомендаций ФСБ. Общие принципы. Методология формирования модели угроз верхнего уровня. Методология формирования детализированной модели угроз. Методология формирования модели нарушителя.

4. Организационные и технические мероприятия по защите персональных данных в информационной системе.

Порядок организации защиты персональных данных. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Оценка обстановки и формирование замысла защиты персональных данных. Организационно-распорядительная документация по защите персональных данных.

Меры по обеспечению безопасности персональных данных. Состав и содержание мер по обеспечению безопасности персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных.

Построение системы защиты персональных данных. Основные этапы при построении системы защиты персональных данных. Комплекс организационных и технических мероприятий в рамках СЗПДн. Уведомление Роскомнадзора об обработке персональных данных.

Подсистемы в составе СЗПДн. Общая характеристика подсистем. Межсетевые экраны.

Аттестация, сертификация и лицензирование в области защиты персональных данных. Сертификация средств защиты персональных данных. Аттестации ИСПДн по требованиям безопасности информации. Лицензирование деятельности по защите персональных данных.

Контроль в области защиты персональных данных. Регуляторы в области защиты персональных данных. Проверки Роскомнадзора. Проверки ФСБ. Проверки ФСТЭК.

5. Итоговое тестирование. Итоговая аттестация.

2.4. Организация самостоятельной работы обучающихся

Целью самостоятельной работы является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности.

В учебном процессе выделяют такой вид самостоятельной работы как внеаудиторная (часы на нее отводятся согласно учебному плану, выполняется по заданию преподавателя, но без его непосредственного участия).

Объем времени, отведенный на самостоятельную работу, находит отражение:

- в учебном плане - в целом по теоретическому обучению (на внеаудиторную работу), по каждой дисциплине (модулю):

- в рабочих программах учебных дисциплин (модулей) и программах практик с ориентировочным распределением по разделам и (или) темам.

Методическое обеспечение самостоятельной работы студентов осуществляется посредством разработки перечня учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю), методических указаний для обучающихся по освоению дисциплины (модуля), которые разъясняют студентам особенности самостоятельной работы на различных видах занятий и во внеаудиторное время по каждой дисциплине (модулю).

Видами заданий для внеаудиторной самостоятельной работы могут быть: чтение текста (учебника, первоисточника, дополнительной литературы); составление плана текста; графическое изображение структуры текста; конспектирование текста; выписки из текста; работа со словарями и справочниками; ознакомление с нормативными документами; учебно-исследовательская работа; использование аудио- и видеозаписей, компьютерной техники и Интернета;

- для закрепления и систематизации знаний: работа с конспектом лекции (обработка текста); повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио- и видеозаписей); составление плана и тезисов ответа; составление таблиц для систематизации учебного материала; изучение карт и других материалов; ответы на контрольные вопросы; аналитическая обработка текста (аннотирование, рецензирование, реферирование, контент–анализ и др.).

Самостоятельная работа студентов в компьютерном классе включает следующие организационные формы учебной деятельности: работа с электронным учебником, просмотр видеолекций, работа с компьютерными тренажерами, компьютерное тестирование, изучение

дополнительных тем занятий, выполнение домашних заданий, выполнение курсовых работ по дисциплине.

Примерные формы выполнения самостоятельной работы: подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов; составление библиографии, тематических кроссвордов; тестирование и др.; решение задач и упражнений по образцу; решение вариативных задач и упражнений; выполнение чертежей, схем; выполнение расчетно-графических работ; решение ситуационных задач; подготовка к деловым играм; проектирование и моделирование разных видов и компонентов профессиональной деятельности; подготовка курсовых и дипломных работ (проектов); опытно-экспериментальная работа; упражнения на тренажере.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Аудитория (лекции, практикумы): компьютер, мультимедийный проектор, экран, доска, стулья и столы, учебные пособия (книги, раздаточный материал в электроном и бумажном виде), утвержденная программа обучения «Защита информации и защита персональных данных».

3.2. Учебно-методическое обеспечение программы

Система дистанционного обучения по адресу: https://ucheba.mupi.su

По каждой дисциплине в рабочих программах приведены сведения об используемых в учебном процессе:

- печатных раздаточных материалах для слушателей;
- учебных пособиях, изданных по отдельным разделам программы;
- профильной литературе;
- отраслевых и других нормативных документах;
- электронных ресурсах и т.д.

Литература:

Основная:

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. .

Дополнительная:

1. Шаблинский, И. Г. Правовое регулирование информационных отношений в сфере обработки персональных данных : учебное пособие для вузов / И. Г. Шаблинский ; под редакцией М. А. Федотова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 52 с.

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценка качества освоения программы включает текущую, промежуточную и итоговую аттестацию обучающихся.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю) или практике, входящий в состав соответствующей рабочей программы дисциплины (модуля) или программы практики, включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Для каждого результата обучения по дисциплине (модулю) или практике определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

Слушатели, успешно выполнившие все элементы учебного плана, допускаются к итоговой аттестации в форме итогового тестирования.

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

Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы и (или) отчисленным из организации, осуществляющей образовательную деятельность, выдается справка об обучении или о периоде обучения.

Формы контроля знаний

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить обучающихся, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

Семинарские (практические занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на практических занятиях оценивается по следующим критериям:

ответы на вопросы, предлагаемые преподавателем;

участие в дискуссиях;

выполнение проектных и иных заданий;

ассистирование преподавателю в проведении занятий.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание практических заданий входит в накопленную оценку.

Для успешного усвоения курса необходимо не только посещать аудиторные занятия, но и вести активную самостоятельную работу. При самостоятельной проработке курса обучающиеся должны:

просматривать основные определения и факты;

повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

изучить рекомендованную основную и дополнительную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;
самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;
использовать для самопроверки материалы фонда оценочных средств;
выполнять домашние задания по указанию преподавателя.
Домашнее задание оценивается по следующим критериям:
Степень и уровень выполнения задания;
Аккуратность в оформлении работы;
Использование специальной литературы;
Сдача домашнего задания в срок.
Оценивание домашних заданий входит в накопленную оценку.

Критерии оценки знаний, навыков

Максимальное значение балльной оценки рейтинга достижений слушателем по каждой дисциплине принимается равной 100 баллов, либо может быть заменено по решению на 100%, независимо от её трудоемкости.
Преподаватель оценивает работу практических занятиях. Оценки за работу на семинарских и практических занятиях преподаватель выставляет в рабочую ведомость. Оценка по 100 балльной шкале за работу на семинарских и практических занятиях определяется перед промежуточным или итоговым контролем.
Преподаватель оценивает самостоятельную работу обучающихся. Оценки за самостоятельную работу обучающегося преподаватель выставляет в рабочую ведомость. Оценка по 100 балльной шкале за самостоятельную работу определяется перед промежуточным или завершающим контролем.
В диплом выставляется результирующая оценка по учебной дисциплине.
Тест основан на проверке знаний по разделу. Промежуточное тестирование – это самотестирование.

%	Оценка
100 % -90 %	5
89 % -70 %	4
69 % -50 %	3
49 % и ниже	2

Дистанционная поддержка осуществляется на базе системы Moodle.

Оценивание выполнения практических заданий

4-балльная шкала (уровень освоения)	Показатели	Критерии
Отлично (повышенный уровень)	Полнота и правильность выполнения практического задания; Своевременность выполнения задания; Самостоятельность решения;	задание выполнено самостоятельно. При этом составлен правильный алгоритм выполнения задания, в логических рассуждениях и решении нет ошибок, получен верный ответ, задание выполнено рациональным способом.
Хорошо (базовый уровень)		задание выполнено с подсказкой преподавателя. При этом составлен правильный алгоритм выполнения задания, в логическом рассуждении и выполнении нет существенных ошибок; есть объяснение решения, допущено не более двух несущественных ошибок, получен верный ответ.
Удовлетворительно (пороговый уровень)		задание выполнено с подсказками преподавателя. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, задание выполнено не полностью или в общем виде.

Неудовлетвори-тельно (уровень не сформирован)		задание не выполнено.

Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы в информационной образовательной среде.

Изучение каждой темы следует начинать с изучения материалов лекции преподавателя и литературы по теме лекции. Далее следует изучить вопросы, оставленные для самостоятельной работы обучающегося. Ответы на контрольные вопросы к каждой теме позволят обучающимся систематизировать и закрепить изученный теоретический материал. Выполнение заданий даст возможность применить на практике теоретический материал, выявить степень усвоения материала, а также вопросы, на которые следует обратить особое внимание.

Оценочные средства для текущего контроля и аттестации

Формой заключительного контроля курса является зачет. Зачет имеет целью выявить и оценить полученные в ходе изучения курса теоретические знания, а также практические умения и навыки.

Самостоятельная работа является формой обучения без непосредственного контакта с преподавателем. В данном курсе предполагаются следующие виды самостоятельной работы слушателей: изучение учебно-методических материалов по каждому модулю в рамках программы, изучение основной и дополнительной литературы к каждому изучаемому модулю; участие слушателей в вебинаре; ответы на вопросы для самотестирования; подготовка к итоговой аттестации.

При подготовке к самотестированию/итоговому тестированию слушатель должен повторить пройденный материал с целью закрепления полученных в рамках изученного модуля (курса) знаний, умений и навыков. При подготовке к тестированию необходимо обращаться к рекомендованной преподавателем основной литературе и лекционному материалу.

Итоговая аттестация (далее–ИА) направлена на установление соответствия уровня повышения квалификации слушателей требованиям профессиональных компетенций, необходимых для выполнения профессиональной деятельности.

Итоговая аттестация слушателей, завершающих обучение по дополнительным профессиональным программам (далее –ДПП), является обязательной. Слушатели, успешно прошедшие итоговую аттестацию, получают соответствующие документы о квалификации.

Целью ИА является оценка сформированности компетенций повышения квалификации.

Итоговая аттестация включает:

- итоговый зачет.

Общая трудоемкость итогового зачета составляет 4 часа. Итоговая аттестация осуществляется с использованием дистанционных технологий.

К итоговому зачету допускаются обучающиеся, завершившие в полном объеме освоение образовательной программы.

При сдаче итогового зачета слушатели должны показать свою способность и умение, опираясь на полученные знания, сформированные умения, профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, аргументировать и

защищать свою точку зрения.
Планируемые результаты обучения направлены на совершенствование профессиональных компетенций, профессиональных знаний, умений, навыков. В планируемых результатах отражается преемственность с профессиональными стандартами и квалификационными характеристиками должностей.

Фонд оценочных средств

1. **Автоматизированная обработка персональных данных – это …**
   1. Обработка персональных данных с использованием средств автоматизации
   2. Обработка персональных данных с помощью средств вычислительной техники
   3. Обработка персональных данных пользователя с применением компьютера

2. **Информация – это …**
   1. Любые данные, представленные на материальном носителе
   2. Сведения, принадлежащие кому-либо и защищаемые законом
   3. Сведения (сообщения, данные), независимо от формы их представления
3. **Информационная система персональных данных – это …**
   1. Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств
   2. Пользователь, средства автоматизации, базы данных
   3. Контролируемое пространство, в котором происходит обработка персональных данных
   4. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
4. **Безопасность персональных данных – это …**
   1. Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных
   2. Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность персональных данных
   3. Состояние защищенности персональных данных, характеризуемое способностью технических средств обеспечить конфиденциальность персональных данных
5. **Блокирование персональных данных – это …**
   1. Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
   2. Временное прекращение обработки персональных данных
   3. Временное прекращение обработки персональных данных для уточнения персональных данных
6. **Доступ к информации – это …**
   1. Возможность получения информации и ее использования
   2. Возможность использования информации
   3. Возможность доступа к информации
   4. Возможность доступа к информации, но не ее использования
7. **Целью Федерального закона от 27.07.2006 № 152-ФЗ является:**
   1. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну
   2. Контроль за обработкой персональных данных операторами персональных данных

3. Соответствие законодательства РФ в сфере персональных данных Конвенции Совета Европы от 1981года

8. Защищаемая информация – это …

1. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
2. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации
3. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов
4. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями Федерального закона «О защищаемой информации в Российской Федерации»

9. Идентификация – это …

1. Присвоение субъектам и объектам доступа идентификатора и сравнение предъявляемого идентификатора с вводимым идентификатором
2. Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
3. Присвоение субъектам и объектам доступа идентификатора
4. Присвоение субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с вводимым идентификатором

10. Информационные технологии – это …

1. Средства поиска, сбора, хранения, обработки, предоставления, распространения информации
2. Методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких методов
3. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
4. Процессы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов

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

1. Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных
2. Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом
3. Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания

12. Материальный носитель (носитель информации) – это…

1. Любой материальный объект, используемый для хранения или передачи информации
2. Любой материальный объект, используемый для хранения информации
3. Любой материальный субъект, используемый для хранения или передачи информации

13. Межсетевой экран – это …

1. Функционально-распределенное программно-аппаратное средство, реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы
2. Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы
3. Локальное программное средство, реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы

14. Нарушитель безопасности персональных данных – это …

1. Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных
2. Физическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных
3. Физическое или юридическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных

15. Недекларированные возможности – это …

1. Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации
2. Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых появляются новые возможности для работы
3. Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

16. Общедоступные персональные данные – это …

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

17. Правила разграничения доступа – это …

1. Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
2. Совокупность правил для обеспечения информационной безопасности в организации
3. Совокупность правил, для объектов доступа

18. Специальные категории персональных данных – это …

1. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости
2. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни жизни
3. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни
4. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости

19. Трансграничная передача персональных данных – это …

1. Передача персональных данных на территорию иностранного государства
2. Передача персональных данных на территорию другого субъекта РФ органу власти данного субъекта, физическому лицу или юридическому лицу данного субъекта РФ
3. Передача персональных данных на территорию иностранного государства или органу власти иностранного государства
4. Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

20. Целостность информации – это ...

1. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения)
2. Состояние информации, при котором отсутствует любое ее изменение
3. Состояние информации, при котором изменение осуществляется только преднамеренно субъектами, имеющими на него право
4. Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

21. Что такое персональные данные?

1. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
2. Информация о частной жизни физического лица, доступ к которой он решил ограничить
3. Сведения о религиозных убеждениях, политических взглядов, расовой и национальной принадлежности субъекта персональных данных
4. Любые сведения независимо от формы их представления

22. Оператор персональных данных — это …

1. Государственный орган, осуществляющий автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке
2. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
3. Юридическое лицо, осуществляющее автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке
4. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, но не определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

23. Обработка персональных данных – это …

1. Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных)
2. Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, осуществляемые с помощью средств вычислительной техники
3. Чтение, запись, сортировка, модификация, передача персональных данных в информационной системе

24. Распространение персональных данных – это …

1. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц
2. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
3. Передача персональных данных оператору персональных данных

25. Предоставление персональных данных – это …

1. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
2. Действия, направленные на раскрытие персональных данных по мотивированному запросу

3. Нет правильного ответа

26. Уничтожение персональных данных – это …

1. Действия, в результате которых становится невозможно определить субъекта персональных данных в информационной системе персональных данных
2. Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных
3. Удаление персональных данных из информационной системы персональных данных
4. Действия, направленные на уничтожение носителей персональных данных

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

1. Невозможно распространять персональные данные
2. Невозможно выполнять сбор персональных данных
3. Выполняется уничтожение персональных данных в информационной системе
4. Становится невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

28. Что понимается под понятием «Контролируемая зона»?

1. Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств
2. Пространство, в котором не исключается неконтролируемое пребывание сотрудников и посетителей оператора, но исключается неконтролируемое пребывание посторонних транспортных, технических и иных материальных средств
3. Пространство, в котором не исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств

29. Что такое биометрические персональные данные?

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных
2. Сведения, которые характеризуют физиологические особенности человека, на основании которых можно установить его личность
3. Сведения, которые характеризуют биологические особенности человека, на основании которых можно установить его личность

30. Как расшифровывается аббревиатура «НСД» применительно к защите информации?

1. Национальные скоростные дороги
2. Несанкционированный доступ
3. Национальный союз дзюдо
4. Национально-социалистическое движение

31. Как расшифровывается аббревиатура «НДВ» применительно к защите информации?

1. Норматив допустимого воздействия
2. Недекларированная возможность
3. Небо для всех
4. Национальный директор по вооружению

32. Какое из свойств защищаемой информации не является основным?

1. Целостность
2. Регистрируемость
3. Доступность
4. Конфиденциальность

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

1. Федерального закона «О Государственной тайне»
2. Федерального закона «Об электронной цифровой подписи»
3. Федерального закона «О персональных данных»

4. Федеральных законов, Постановлений Правительства и нормативно-правовых актов уполномоченных органов государственной власти РФ в сфере информации и персональных данных

34. Дата официального опубликования Федерального закона «О персональных данных»:

1. 26 июня 2006 года
2. 26 июля 2007 года
3. 27 июля 2006 года
4. 27 июня 2007 года

35. Целью Федерального закона «О персональных данных» является:

1. Обеспечение защиты информации в Российской Федерации
2. Осуществление права на поиск, получение, передачу, производство и распространение информации
3. Обеспечение защиты персональных данных
4. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных

36. На какие отношения не распространяется действие Федерального закона "О персональных данных"?

1. На отношения, возникающие при обработке персональных данных физическими лицами, исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных
2. На отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну
3. Не распространяется на оба перечисленных варианта

37. Оператор персональных данных – это .. (Несколько вариантов ответа):

1. Физическое лицо
2. Юридическое лицо
3. Муниципальный орган
4. Государственный орган
5. Гражданин
6. Государственный служащий

38. Перед кем оператор персональных данных несет ответственность?

1. Перед субъектом персональных данных
2. Перед Роскомнадзором
3. Не перед кем не несет ответственности

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

1. На отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных
2. На отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну
3. На отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами
4. Распространяется на все перечисленные варианты

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

1. Администрация города или района
2. Департамент информационных технологий
3. Управление Роскомнадзора

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

1. Форму согласия на обработку персональных данных

2. Положение о защите персональных данных
3. Документы, определяющие политику в отношении обработки персональных данных

42. Управление Роскомнадзора уведомляет оператора персональных данных о проведении внеплановой проверки:

1. Не менее чем за 24 часа до начала ее проведения любым доступным способом
2. Не менее чем за 3 дня до начала ее проведения любым доступным способом
3. Не менее чем за 24 часа до начала ее проведения только в письменном виде

43. Срок проведения плановой проверки не может превышать:

1. 35 рабочих дней
2. 28 рабочих дней
3. 20 рабочих дней
4. Срок проведения проверок не ограничен

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

1. В течение 30 дней
2. В течение двух рабочих дней
3. В течение 5 рабочих дней
4. Срок предоставления документов не ограничен

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

1. 30 рабочих дней
2. 30 календарных дней
3. 20 календарных дней
4. 10 рабочих дней

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

1. 5 рабочих дней
2. 7 рабочих дней
3. 10 рабочих дней
4. 30 календарных дней

47. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных и уничтожить соответствующие персональных данных в срок, не превышающий с даты достижения цели обработки персональных данных:

1. 10 дней
2. 30 дней
3. 7 дней

48. 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 персональных данных
2. В течение 4 рабочих дней после начала обработки персональных данных
3. До начала обработки персональных данных
4. В течение 7 рабочих дней после начала обработки персональных данных

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

1. 7 рабочих дней
2. 10 рабочих дней
3. 15 календарных дней
4. 30 рабочих дней

50. Управление Роскомнадзора уведомляет о проведении плановой проверки:

1. Не позднее, чем в течение 3-х рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Управления Роскомнадзора с уведомлением о вручении или иным доступным способом
2. Не позднее, чем в течение 7-ми рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Управления Роскомнадзора с уведомлением о вручении или иным доступным способом
3. Не менее чем за 24 часа до начала ее проведения любым доступным способом
4. Предварительное уведомление Оператора о начале проведения плановой проверки не требуется

51. Контроль за выполнением требований Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» проводится не реже 1 раза в:

1. 5 лет
2. 3 года
3. 1 год

52. Основная статья, по которой предусмотрена ответственность для Оператора по результатам проверки:

1. УК РФ. Статья 137. Нарушение неприкосновенности частной жизни
2. КоАП. Статья 19.5. Невыполнение в срок законного предписания
3. КоАП. Статья 19.7. Непредставление сведений (информации)
4. КоАП. Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

53. Кто должен осуществлять внутренний контроль за соблюдением оператором законодательства Российской Федерации о персональных данных?

1. Администратор безопасности использования персональных данных
2. Ответственный за организацию обработки персональных данных
3. Ответственный за обеспечение безопасности персональных данных
4. Руководитель организации

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

1. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации
2. Использование средств контроля и управлении доступом
3. Использование запираемых шкафов, сейфов и решеток на окнах
4. Должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, устанавливаются оператором.

55.Какая ответственность предусмотрена за нарушение законодательства РФ о персональных данных?

1. Дисциплинарная
2. Административная
3. Уголовная
4. Все перечисленные

56. Рекомендуемые Роскомнадзором методы обезличивания персональных данных:

1. Метод введения идентификаторов; метод маскирования; метод перемешивания; метод замены состава или семантики
2. Метод введения идентификаторов; метод абстрагирования; метод перемешивания; метод разделения состава или семантики
3. Метод введения идентификаторов; метод декомпозиции; метод перемешивания; метод изменения состава или семантики

57. В соответствии с каким законодательным актом технические задания на создание информационных систем для ГИС и МИС обязательно выполнять в соответствии с ГОСТ 34.602-89, ГОСТ 5183-2000, ГОСТ Р 51624-2000, ГОСТ 34.601-90, ГОСТ 34.201-89?

1. Приказ ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
2. Приказ ФСТЭК 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»
3. Приказ ФСТЭК России от 20.07.2012 N 89 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации»
4. Федеральный закон от 27.12. 2002 N 184-ФЗ «О техническом регулировании»

58. Сколько дней максимум может длиться проверка ФСБ?

1. 20 рабочих дней
2. 20 календарных дней
3. 30 рабочих дней
4. 30 календарных дней

59. Какой документ составляется по результатам проверки ФСБ?

1. Отчет по результатам проверки
2. Акт проверки
3. Заключение о проверке
4. Протокол

60. Как называется документ, который составляется по результатам проверки и в нем указываются нарушения, которые необходимо устранить?

1. Предписание
2. Заключение
3. Акт о выявленных нарушениях
4. акт проверки

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

1. 7 календарных дней
2. 3 рабочих дня
3. 14 рабочих дней

62. Какие виды проверок бывают?

1. Документарные и выездные
2. Только документарные
3. Только выездные

63. Кто может взаимодействовать с сотрудниками Роскомнадзора при проведении выездной проверки?

1. Руководитель организации и уполномоченный сотрудник
2. Любой сотрудник
3. Только ответственный за организацию обработки персональных данных

64. Что мы получаем по итогу разработки модели угроз?

1. Перечень наиболее опасных угроз
2. Перечень наиболее вероятных угроз
3. Перечень актуальных угроз
4. Перечень неактуальных угроз

65. Какое из свойств защищаемой информации не является основным?

1. Целостность
2. Регистрируемость
3. Доступность
4. Конфиденциальность

66. Требования по защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах устанавливает:

1. Приказ ФСТЭК №21
2. Приказ ФСТЭК №17

3. Приказ ФСТЭК №58

67. Что из перечисленного не подлежит обязательному учёту?

1. Средства криптографической защиты информации
2. Материальные носители персональных данных
3. Блоки питания ПК, обрабатывающих персональные данные
4. Сотрудники, доступ которых к персональным данным обусловлен их должностными обязанностями

68. Обеспечение информационной безопасности есть обеспечение…

1. Независимости информации
2. Изменения информации
3. Копирования информации
4. Сохранности информации
5. Преобразования информации

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

1. Постановлением Правительства РФ от 13 февраля 2019 г. № 146
2. Приказом Минкомсвязи РФ от 21 января 2019 г. № 10
3. Приказом Роскомнадзора от 30 октября 2018 г. № 159

70. Перед передачей персональных данных субъекта на территорию другого государства оператор ….

1. Получает согласие на передачу персональных данных от субъекта
2. Принимает самостоятельно решение о передаче персональных данных субъекта
3. Выясняет, относится ли данная страна к государствам, обеспечивающим адекватную защиту персональных данных

71. Государственный контроль и надзор в сфере персональных данных, в соответствии с постановлением Правительства № 146 от 13.02.2019 года проводится посредством:

1. Плановых и внеплановых проверок +
2. Принятия мер по пресечению и устранению выявленных нарушений +
3. Проведения мероприятий по контролю без взаимодействия с операторами +
4. Проведения мероприятий по профилактике нарушений +
5. Проведением мероприятий по контролю за распространением персональных данных

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

1. 149-ФЗ с 1 декабря 2016 г.
2. 242-ФЗ с 1 сентября 2015 г.
3. Нет правильного ответа

73. В каком случае фотографию можно отнести к биометрическим персональным данным?

1. В случае, если копия паспорта с фотографией находится в личном деле сотрудника
2. В случае если фотография зарегистрирована в СКУД (система контроля и управления доступом, т.е. проходная завода) +
3. В случае если эта фотография сделана в публичном месте
4. В случае, если гражданин проходит паспортный контроль в зелёной зоне аэропорта

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

1. Порядок организации и проведения проверок операторов персональных данных +
2. Порядок контроля и надзора за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии со ст.19.ФЗ-152
3. Оба ответа верны

75. Управление Роскомнадзора региона, в соответствии с постановлением

Правительства РФ от 12.02.2019 г. № 146 согласует с органами прокуратуры внеплановые проверки:

1. По результатам обращения граждан, поступивших в Роскомнадзор +
2. В случае неисполнения оператором предписания Роскомнадзора +
3. По результатам проведения мероприятий по контролю без взаимодействия с оператором

76. При проведении проверки в отношении оператора, который осуществляет свою деятельность на территориях нескольких субъектов Российской Федерации, срок проведения проверки устанавливается отдельно по каждому филиалу, представительству оператора, при этом общий срок проведения такой проверки не может превышать...

1. 60 рабочих дней
2. 20 рабочих дней
3. 30 календарных дней

77. Основанием для продления срока проведения проверки является:

1. Получение в ходе проведения проверки от правоохранительных органов, в том числе органов прокуратуры, либо из иных источников документов, свидетельствующих о нарушении оператором требований
2. Возникновение обстоятельств непреодолимой силы (затопление, наводнение, пожар и тому подобное) на территории, где проводится проверка
3. Непредставление оператором в ходе проведения проверки необходимых документов
4. Выявление в ходе проведения проверки обстоятельств, связанных с большим объемом проверяемых и анализируемых документов, количеством осуществляемых видов деятельности по обработке персональных данных, разветвленностью организационно-хозяйственной структуры оператора, сложностью технологических процессов обработки персональных данных
5. Все ответы верны

78. Проводятся ли внеплановые документарные проверки в отношении оператора?

1. Проводятся
2. Не проводятся
3. Проводятся по согласованию с Прокуратурой

79. Проводится ли выездная проверка оператора - физического лица, не являющегося индивидуальным предпринимателем?

1. Проводится
2. Не проводится
3. Проводится по согласованию с Прокуратурой

80. К мероприятиям по контролю без взаимодействия проверяющего органа с операторами относится:

1. Наблюдение за соблюдением требований при размещении информации в сети "Интернет" и средствах массовой информации
2. Наблюдение за соблюдением требований посредством анализа информации о деятельности оператора, которая представляется оператором (в том числе посредством использования федеральных государственных информационных систем) в орган по контролю и надзору в соответствии с федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации или может быть получена (в том числе в рамках межведомственного информационного взаимодействия) органом по контролю и надзору
3. Оба ответа верны

81. В целях профилактики нарушения требований орган по контролю и надзору:

1. Размещает на своем официальном сайте в сети "Интернет" перечень нормативных правовых актов, содержащих требования
2. Осуществляет информирование операторов о положении дел в области защиты прав субъектов персональных данных
3. Обеспечивает ежегодное обобщение практики осуществления государственного контроля и надзора в области персональных данных посредством подготовки отчета о

деятельности по осуществлению государственного контроля и надзора в области персональных данных
4. Размещает на своем официальном сайте в сети "Интернет" информацию о наиболее часто выявляемых в ходе осуществления контроля и надзора нарушениях требований, в результате которых оператор был привлечен к административной ответственности либо оператору было выдано предписание об устранении выявленных нарушений
5. Размещает на своем официальном сайте в сети "Интернет" руководства по соблюдению требований, информацию о проведении семинаров и конференций
6. Осуществляет разъяснительную работу в средствах массовой информации и иными способами
7. Выдает предостережения о недопустимости нарушения требований
8. Все ответы верны

82. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются …

1. Роскомнадзором
2. Оператором
3. Правительством Российской Федерации

83. Допускается ли объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой?

1. Допускается
2. Не допускается
3. Допускается с письменного разрешения Роскомнадзора

84. Обязано ли лицо, осуществляющее обработку персональных данных по поручению оператора, получать согласие субъекта персональных данных на обработку его персональных данных?

1. Обязано
2. Не обязано
3. Обязано, если обрабатываются персональные данные иностранного гражданина

85. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед…

1. Субъектом персональных данных
2. Оператором
3. Роскомнадзором

86. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается…

1. Правительством Российской Федерации
2. Оператором
3. Органом муниципальной власти

87. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают ….., если такое согласие не было дано субъектом персональных данных при его жизни.

1. Наследники субъекта персональных данных
2. Лица, знакомые с субъектом персональных данных
3. Органы ЗАГС

88. Кем может осуществляться обработка персональных данных о судимости?

1. Государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации
2. Иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами

3. Оба ответа верны

89. Сколько существует уровней криптографической защиты персональных данных?

1. 6
2. 4
3. 8

90. Безопасность обработки персональных данных с использованием крипто-средств организуют и обеспечивают …

1. ФСТЭК и ФСБ
2. Операторы
3. Органы муниципальной власти

91. Какие нарушители с точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, называются внешними?

1. Нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена
2. Нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПД, реализующие угрозы непосредственно в ИСПДн
3. Нарушители, имеющие доступ к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена

92. Что такое среда распространения информативного сигнала?

1. Источник угрозы
2. Физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником
3. Утечка информации по техническим каналам

93. Что включают в себя угрозы несанкционированного доступа (НСД) в ИСПДн с применением программных и программно-аппаратных средств?

1. Угрозы доступа в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения)
2. Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т. п.
3. Угрозы внедрения вредоносных программ (программно-математического воздействия)
4. Все перечисленные угрозы

94. Какими могут быть угрозы безопасности персональных данных, реализуемые с использованием протоколов межсетевого взаимодействия по характеру угрозы?

1. С обратной связью и без обратной связи
2. Активные и пассивные
3. Внутрисегментные и межсегментные

95. В чем заключается сущность процесса реализации угрозы «Сканирование сети»?

1. Используется специальная программа-анализатор, которая перехватывает все пакеты, идущие по сети
2. В передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них +
3. Нет правильного ответа

96. Что такое доверенный объект?

1. Это элемент сети, легально подключенный к серверу
2. Это объект регистрации персональных данных, на который оформлена вся разрешительная документация
3. Это алгоритм идентификации и аутентификации хостов, пользователей и т. д.

97. Какую из перечисленных функций может выполнять вредоносная программа?

1. Скрывать признаки своего присутствия в программной среде компьютера
2. Разрушать (искажать произвольным образом) код программ в оперативной памяти
3. Сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных)

4. Все ответы верны

98. Какие угрозы необходимо учитывать при формировании модели угроз?

1. Прямые и косвенные
2. Верхнего и нижнего уровней
3. Криптографические и автоматические

99. Что является основной характеристикой безопасности?

1. Конфиденциальность
2. Целостность
3. Доступность
4. Все ответы верны

100. При оценке обстановки и формировании замысла защиты персональных данных проводится анализ информационных ресурсов. Что из перечисленного ниже в него включено?

1. Категорирование персональных данных
2. Выявление технических каналов утечки информации
3. Оценка непосредственного ущерба от реализации угроз
4. Нет правильного ответа

5. Организационно-педагогические условия реализации программы

5.1. Реализация дополнительной профессиональной программы обеспечивает приобретение обучающимися знаний и умений, требования к которым устанавливаются законодательством Российской Федерации, а также учитывать преемственность задач, средств, методов, организационных форм подготовки работников различных уровней ответственности и специфику.

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

5.3. Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала ведется в форме, доступной для понимания слушателей, соблюдается единство терминологии, определений и условных обозначений. В ходе занятий преподаватель увязывает новый материал с ранее изученным, дополняет основные положения примерами из практики, соблюдает логическую последовательность изложения.

5.4. Практические занятия проводятся с целью закрепления теоретических знаний и выработки у слушателей основных умений и навыков работы в ситуациях, максимально имитирующих реальные производственные процессы.

5.5. Реализация образовательной программы обеспечивается научно-педагогическими кадрами, квалификация которых должна соответствовать квалификационным характеристикам и (или) профессиональными стандартами (при наличии).

5.6. Требования к информационным и учебно-методическим условиям.

Внеаудиторная работа обучающихся сопровождается методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение. Во всех рабочих программах дисциплин (модулей) представлены специальные разделы, содержащие методические рекомендации по организации самостоятельной работы студентов, а также методические указания (рекомендации) по видам учебных занятий.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде университета. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа, обучающегося из любой точки, в которой имеется доступ к сети «Интернет», как на территории

университета, так и вне него.

Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и обновляется ежегодно.

Информация об электронно-библиотечных системах и базах данных, к которым у обучающихся имеется доступ на основе лицензионных соглашений университета, представлен на сайте университета.

Электронно-библиотечные системы (электронная библиотека) и электронная информационно-образовательная среда обеспечивают одновременный доступ не менее 25 % обучающихся по образовательной программе.

В случае недоступности используемого в учебном процессе библиографического источника (учебника, учебно-методического пособия, научного издания и т.д.) через электронно-библиотечную систему (электронную библиотеку) библиотечный фонд университета обеспечивает укомплектованность печатными изданиями из расчета не менее 50 экземпляров каждого из изданий основной литературы, перечисленной в рабочих программах дисциплин (модулей), практик, и не менее 25 экземпляров дополнительной литературы на 100 обучающихся.

Университет обеспечен необходимым комплектом лицензионного программного обеспечения (состав определяется в рабочих программах дисциплин (модулей) и ежегодно обновляется).

5.7. Общие требования к организации образовательного процесса.

МУПИ располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Для организации учебного процесса используются специальные помещения — учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для реализации программы задействован следующий кадровый потенциал:

- Преподаватели учебных дисциплин - Обеспечивается необходимый уровень компетенции преподавательского состава, включающий высшее образование в области соответствующей дисциплины программы или высшее образование в иной области и стаж преподавания по изучаемой тематике не менее трех лет; использование при изучении дисциплин программы эффективных методик преподавания, предполагающих вместе с традиционными лекционно-семинарскими занятиями решение слушателями вводных задач по предметам, занятия с распределением ролевых заданий между слушателями.
- Административный персонал - обеспечивает условия для эффективной работы педагогического коллектива, осуществляет контроль и текущую организационную работу.
- Информационно-технологический персонал - обеспечивает функционирование информационной структуры (включая ремонт техники, оборудования, макетов иного технического обеспечения образовательного процесса).