ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «УДЦ ЗНАНИЯ ПЛЮС»

РАССМОТРЕНО
На заседании педагогического совета
Протокол № 1 от 13 января 2021 г.

УТВЕРЖДАЮ
Директор
Р.Ф.Галиакберов

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)»

144 академических часа

г. Стерлитамак

Содержание

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Дополнительная профессиональная программа повышения квалификации «Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)» (далее – Программа) – это комплекс учебно–методических документов, регламентирующий цели, содержание, формы организации, технологии обучения и оценивания для достижения слушателями установленных, в форме компетенций, требований к уровню подготовки лиц, освоивших Программу для совершенствования и получение новой компетенции, необходимой для профессиональной деятельности, и повышения профессионального уровня в рамках имеющейся квалификации. Программу реализует Частное учреждение дополнительного профессионального образования «Учебно- деловой центр «Знания плюс» (далее – УЦ) с использованием дистанционных образовательных технологий и электронного обучения.

1.2. Программа разработана с учетом квалификационных требований к результатам освоения образовательных программ и направлена на совершенствование и получение новой компетенции, необходимой для профессиональной деятельности, и повышение профессионального уровня в рамках имеющейся квалификации слушателей на основании следующих нормативно-правовых документов:

- Федеральный закон от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 28 декабря 2010 года № 390-ФЗ «О безопасности»
- Указ Президента РФ от 13 сентября 2004 года № 1167 «О неотложных мерах по повышению эффективности борьбы с терроризмом»;
- Указ Президента РФ от 15 февраля 2006 года № 116 «О мерах по противодействию терроризму»;
- Указ Президента РФ от 14 июня 2012 года № 851 «О порядке установления уровней террористической опасности, предусматривающих принятие дополнительных мер по обеспечению безопасности личности, общества и государства»;
- Концепция противодействия терроризму в Российской Федерации (утверждена Президентом РФ от 05.10.2009);
- Концепция общественной безопасности в Российской Федерации (утверждена Президентом РФ от 14.11.2013 № Пр-2685)
- Постановление Правительства от 15 февраля 2011 года № 73 «О некоторых мерах по совершенствованию подготовки проектной документации в части противодействия террористическим актам»;
- Положения ст.76 Федерального закона № 273-ФЗ «Об образовании в Российской Федерации» от 29 декабря 2012 г.;

- Приказ Министерства образования и науки РФ от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

- Приказ Министерства образования и науки РФ от 12 января 2016 г. N 7 "Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.02 Менеджмент (уровень бакалавриата)";

- Приказ Министерства труда и социальной защиты Российской Федерации от 15 июня 2020 года N 333н «Об утверждении профессионального стандарта «Специалист по организационному и документационному обеспечению управления организацией»;

- Квалификационный справочник должностей руководителей, специалистов и других служащих 4-е издание, дополненное (утв. постановлением Минтруда РФ от 21 августа 1998 г. N 37).

1.3. Обучение по программе осуществляется на основе договора об оказании услуг, заключаемого со слушателем и (или) с физическим или юридическим лицом, обязующимся оплатить обучение лица, зачисляемого на обучение.

1.4. Слушатели при овладении дополнительной профессиональной программой повышения квалификации «Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)» обеспечиваются доступом к системе электронного образовательного ресурса, представленного в электронно-цифровой форме и включающего в себя текстовые, аудиовизуальные и мультимедийные учебно-методические материалы для самостоятельного изучения обучаемыми дополнительной профессиональной программы повышения квалификации, к которой предоставляется доступ через информационно-телекоммуникационную сеть «Интернет».

1.5. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы:

- лица, желающие освоить дополнительную профессиональную программу, должны иметь среднее профессиональное или высшее образование. Наличие указанного образования должно подтверждаться документами государственного образца;

- обладать навыками работы на персональном компьютере.

1.6. Программа предназначена для повышения квалификации специалистов с высшим и средним профессиональным образованием, уже осуществляющих или планирующих профессиональную деятельность в сфере работы со служебной информацией ограниченного распространения. Программа позволяет в процессе обучения слушателя приобрести как фундаментальные знания, так и практические навыки в указанной сфере профессиональной деятельности.

1.7. Нормативная трудоемкость обучения по данной Программе составляет 144 часа, включая все виды учебной работы слушателя.

1.8. Форма обучения заочная (без отрыва от работы) с использованием дистанционных образовательных технологий.

1.9. Учебная нагрузка для всех видов учебной работы слушателя устанавливается для программы продолжительностью 144 академических часа не более 40 часов в неделю.

2. ЦЕЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ

2.1. Целью реализации Программы является:

- повышение профессионального уровня в рамках имеющейся квалификации в сфере ведения делопроизводства с использованием информационных технологий и требований, предъявляемых к специалистам по работе со служебной информацией ограниченного распространения, содержащейся в документах об антитеррористической защищенности;

- внедрение лучших технических разработок и новейших технологий в обеспечение подготовки и оформления необходимой документации;

- освоение новых компетенций для профессиональной деятельности специалиста в области работы со служебной информацией ограниченного распространения, содержащейся в документах об антитеррористической защищенности;

- подготовка слушателей к практической профессиональной деятельности по управлению служебной информацией ограниченного распространения в различных учреждениях.

2.2. В результате освоения дополнительной профессиональной программы повышения квалификации предусмотрено совершенствование компетенций и получение новых компетенций, необходимых для профессиональной деятельности слушателей и повышения их профессионального уровня в рамках имеющейся квалификации:

- осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

- определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

- осуществлять деловую коммуникацию в устной и письменной формах.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

3.1. Выпускник курса повышения квалификации «Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)» должен обладать профессиональными компетенциями, соответствующими виду деятельности. Планируемые результаты обучения включают в себя:

- овладение знаниями законодательных актов и нормативно-методических материалов, регламентирующих работу со служебной информацией ограниченного распространения, содержащейся в документах об антитеррористической защищенности;

- овладение знаниями характеристик основных видов документов предприятия (организации), требований к их оформлению, принципов работы с документами;

- овладение технологиями составления и оформления документов, регламентирующих работу в делопроизводстве организации;

- овладение умением использования современного оборудования для обработки документов;

- овладение знаниями и умениями в предотвращении и минимизации ущерба в случае возникновения угрозы террористических актов в учреждении.

3.2. Слушатели, успешно завершившие обучение по Программе, получают комплексные знания в сфере делопроизводства и документационном обеспечении формирования и хранения служебной информацией ограниченного распространения, содержащейся в документах об антитеррористической защищенности организации и могут решать профессиональные задачи в процессе трудовой деятельности:

- осуществлять работу по разработке и оформлению документов об антитеррористической защищенности организации;

- осуществлять работу по систематизации и хранению документов, содержащих служебную информацию ограниченного распространения, связанную с антитеррористической защищенности организации.

3.3. Настоящая Программа отвечает следующим требованиям:

• отражает квалификационные требования к специалисту по работе со служебной информацией ограниченного распространения в организации;

• не противоречит государственным образовательным стандартам высшего и среднего профессионального образования;

• ориентирована на современные образовательные технологии и средства обучения (обучение проводится с использованием дистанционных технологий);

• соответствует установленным правилам оформления программ.

4. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ

4.1. В результате обучения по дополнительной профессиональной программе повышения квалификации «Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)» слушатель должен приобрести следующие компетенции:

Код	Наименование компетенций
Универсальные компетенции (УК):	
УК–1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
Общепрофессиональные компетенции (ОК):	
ОК-1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК-2	Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК-3	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях
ОК-4	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития
ОК 5	Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности
ОК 6	Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями
ОК 7	Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9	Быть готовым к смене технологий в профессиональной деятельности
Профессиональные компетенции (ПК)	
ПК 3.1	Осуществлять работу по организации комплекса мероприятий по антитеррористической защите учреждения

ПК 3.2	Осуществляет разработку, оформление и хранение служебной информации ограниченного распространения, содержащейся в документах об антитеррористической защищенности организации

4.2. В результате освоения дополнительной профессиональной программы повышения квалификации «Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)» слушатель должен:

Выполнять трудовые функции	**Уметь**	**Знать**
Организация работы со служебной информацией ограниченного распространения и связанной с ней документацией		
Выполнение операций по предварительному рассмотрению и регистрации документов организации	Организовывать взаимодействие подразделений организации в процессе разработки и исполнения различных видов ее документов	Законодательные и нормативные правовые акты Российской Федерации в сфере документационного обеспечения управления
Ведение регистрационных и учетных форм документов организации	Создавать базы данных по организационно-распорядительным документам организации и осуществлять контроль их ведения	Методические документы и национальные стандарты в области работы с информацией ограниченного доступа в организации
Организация передачи документов между уровнями управления, руководством, исполнителями в организации	Создавать систему индексации документов организации и использовать ее в информационно-справочных целях	Состав локальных нормативных актов организации
Разработка и согласования документов в организации	Выделять документы организации, не требующие регистрации	Правила работы с документами организации, установленные ее

Выполнять трудовые функции	Уметь	Знать
		законодательными и локальными нормативными актами
Проведение анализа информационных и документационных потоков в организации	Регистрировать документы организации ограниченного доступа	Распределение функций и вопросов деятельности между руководством и структурными подразделениями организации
Разработка технологии работы с документами и информацией в организации	Создавать и использовать метаданные документов в процессе их движения и обработки в организации	Функциональные особенности системы электронного документооборота организации
Проверка подлинности документов, поступивших в организацию	Выполнять работу со служебной информацией ограниченного распространения в рамках процедур, установленных в организации	Правила оформления и движения служебной информации и ее документальное оформление
Разработка документов и организация их хранения в подразделениях организации	Разрабатывать документацию в соответствии с требованиями	Законодательные и нормативные правовые акты Российской Федерации в области работы со служебной информацией ограниченного доступа
Осуществление информационно-справочной работы со служебной информацией учреждения		
Формирование требований	Работать с источниками	Правила и порядок

Выполнять трудовые функции	Уметь	Знать
к информационно-поисковым системам документов организации, используемым в документационном обеспечении управления	информации, выявлять критерии ее оценки и отбора в соответствии с заданиями руководства организации	формирования баз данных организации
Формирование и ведение баз данных об организационно-распорядительных документах организации	Подбирать, систематизировать и классифицировать документы по определенным критериям	Особенности функционирования справочно-информационных и информационно-поисковых систем организации
Формирование требований к разграничению уровней доступа работников организации к документам и информации в соответствии с выполняемыми ими функциями	Структурировать информацию, выделять необходимую для работы службы документационного обеспечения управления организации	Порядок доступа к различным категориям информации в организации
Обеспечение доступа к документам и информации организации Разработка форм представления информации	Оформлять информацию в наглядном систематизированном виде в соответствии с предъявляемыми требованиями к форме представления информации	Способы получения информации из различных источников
Подготовка отчетов и	Работать с электронными	Формы составления,

Выполнять трудовые функции	Уметь	Знать
аналитических справок по вопросам служебной информации ограниченного распространения, имеющей отношение к антитеррористической защите	базами данных и системами электронного документооборота организации	представления и передачи информации и их особенности
Поиск и предоставление информации по антитеррористической защите учреждения		Технология работы с документами и информацией ограниченного доступа
Организация оперативного хранения информации ограниченного распространения в организации и передачи дел		
Формирование пакета документов в соответствии с требованиями	Разрабатывать нормативно-техническую документацию	Методические документы и национальные стандарты в области работы с информацией
Контроль создания и ведения справочно-поисковых средств по документам, хранящимся в подразделениях организации (номенклатура дел, описи)	Систематизировать документы и информацию, формировать в соответствии с требованиями	Правила работы с документами организации, установленные законодательными и локальными нормативными актами
Обеспечение сохранности созданных в организации организационно-распорядительных документов на различных носителях	Осуществлять методическое руководство организацией хранения документов в структурных подразделениях организации, оказывать им практическую помощь	Порядок и содержание процедур организации оперативного хранения документов и информации их подготовки к передаче

Выполнять трудовые функции	Уметь	Знать
Подготовка документов для передачи другому лицу при передаче полномочий	Обеспечивать защиту документов и информации организации от несанкционированного доступа	Особенности хранения бумажных и электронных документов, правила оформления передачи их другому уполномоченному лицу

5. СОДЕРЖАНИЕ ПРОГРАММЫ. УЧЕБНЫЙ ПЛАН. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

5.1. В учебном плане отражается логическая последовательность освоения разделов дополнительной профессиональной программы повышения квалификации, обеспечивающих формирование компетенций, указывается общая трудоемкость разделов программы продолжительностью 144 академических часа, а также указывается форма итоговой аттестации.

Учебный план дополнительной профессиональной программы повышения квалификации
«Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)».

№ п/п	Наименование дисциплин, тем	Всего час.	В том числе		Форма контроля знаний
			ЛК*	СРС*	
1.	**Модуль 1. ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ЗАЩИТЫ СЛУЖЕБНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ**	**56**	**36**	**20**	
1.1.	Федеральные законы Российской Федерации	18	12	6	
1.2.	Указы Президента Российской Федерации	16	12	4	
1.3.	Постановления Правительства Российской Федерации	22	12	10	
2.	**Модуль 2. ОБЕСПЕЧЕНИЕ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИЙ**	**24**	**16**	**8**	
2.1	Категорирование объектов и порядок его проведения	4	3	1	
2.2	Мероприятия по обеспечению антитеррористической защищенности объектов (территорий)	6	4	2	
2.3	Контроль за выполнением требований к антитеррористической защищенности объектов (территорий)	4	2	2	
2.4	Порядок информирования об угрозе совершения или о совершении террористического акта на объектах (территориях) и реагирования лиц, ответственных за обеспечение	6	4	2	

	антитеррористической защищенности объекта (территории), на полученную информацию				
2.5	Паспорт безопасности объекта (территории)	4	3	1	
3.	**Модуль 3. ПОРЯДОК ОБРАЩЕНИЯ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ**	**24**	**16**	**8**	
3.1.	Документы для служебного пользования: особенности работы	6	4	2	
3.2.	Организация работы с документами для служебного пользования	6	4	2	
3.3	Хранение документов для служебного пользования	6	4	2	
3.4	Ответственность за ДСП-документы	6	4	2	
4.	**Модуль 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**	**36**	**26**	**10**	
4.1	Понятие «информационная безопасность»	6	4	2	
4.2.	Обеспечение защиты информации	8	6	2	
4.3	Контроль информационной безопасности	6	4	2	
4.4	Угрозы информационной безопасности	8	6	2	
4.5	Средства защиты информационной безопасности	8	6	2	
5	**Итоговая аттестация (экзамен)**	**4**		**4**	**Итоговое тестирование**
	Итого:	**144**	**94**	**50**	

Условные обозначения:

ЛК – лекции; СРС*– самостоятельная работа слушателя.*

5.3. Календарный учебный график дополнительной профессиональной программы повышения квалификации «Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)»

Режим занятий: 4 недели, не более 40 академических часов в неделю. Продолжительность учебной недели составляет 5 дней.

№ п/п	Наименование дисциплин, тем	Общая трудоемкость, академ. час	Недели, ч			
			1	2	3	4
1.	Модуль 1. ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ЗАЩИТЫ СЛУЖЕБНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ	56	У 40	У 16		
2.	Модуль 2. ОБЕСПЕЧЕНИЕ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИЙ	24		У 24		
3.	Модуль 3. ПОРЯДОК ОБРАЩЕНИЯ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ	24			У 24	
4.	Модуль 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ	36			У 16	У 20
10.	Итоговая аттестация (экзамен)	4				Э 4
	Итого:	144	40	40	40	24

Условные обозначения:

У – учебный процесс (аудиторная и самостоятельная работа слушателей)

Э – итоговая аттестация (экзамен).

5.4. Аннотации рабочих программ учебных дисциплин, требования к результатам освоения дисциплин.

Модуль 1. ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ЗАЩИТЫ СЛУЖЕБНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

Цели освоения дисциплины:

получение профессиональных знаний о законодательных основах и нормативных базах по антитеррористической защите.

В результате изучения дисциплины слушатель должен:

знать:

законодательные и нормативные правовые акты Российской Федерации, регламентирующие вопросы антитеррористической защищенности объектов от возможных террористических посягательств,

требования антитеррористической безопасности учреждения,

содержание и правила оформления пакета документов по антитеррористической безопасности в организации

уметь:

работать с источниками информации о правоустанавливающих и нормативных актах

владеть:

навыками формирования пакета документов по антитеррористической безопасности в организации

Модуль 2. ОБЕСПЕЧЕНИЕ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИЙ

Цель освоения дисциплины:

получение профессиональных знаний и навыков касательно обеспечения антитеррористической защищенности организаций.

В результате изучения дисциплины слушатель должен:

знать:

правила категорирования объектов и порядок его проведения

мероприятия по обеспечению антитеррористической защищенности объектов (территорий)

правила контроля за выполнением требований к антитеррористической защищенности объектов (территорий)

порядок информирования об угрозе совершения или о совершении террористического акта на объектах (территориях) и реагирования лиц, ответственных за обеспечение антитеррористической защищенности объекта (территории), на полученную информацию

правила оформления паспорта безопасности объекта (территории)

уметь:

организовывать мероприятия по предотвращению теракта и уменьшению вероятности возникновения и ликвидации последствий в случае его возникновения.

владеть:

навыками организации антитеррористических мероприятий.

Модуль 3. ПОРЯДОК ОБРАЩЕНИЯ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

Цель освоения дисциплины:

получение профессиональных знаний и навыков обращения со служебной информацией ограниченного распространения

В результате изучения дисциплины слушатель должен:

знать:

особенности организации работы с документами для служебного пользования в различных организациях и учреждениях,

правила хранения документации для служебного пользования,

категории должностных лиц, имеющих право доступа к служебной информации ограниченного доступа,

правила приема, учета (регистрации) документов, содержащих информацию ограниченного распространения

порядок работы с документами со служебной информацией ограниченного распространения,

ответственность за нарушение обращения со служебной информацией ограниченного распространения.

уметь:

обращаться со служебной информацией ограниченного распространения.

владеть:

навыками обращения со служебной информацией ограниченного распространения.

Модуль 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Цель освоения дисциплины:

получение профессиональных знаний и навыков по основам информационной безопасности и защите информации.

В результате изучения дисциплины слушатель должен:

знать:

основы информационной безопасности,

правила обеспечения защиты информационной безопасности,

основные угрозы информационной безопасности,

способы предотвращения хищения электронной информации.

уметь:

организовать работу со служебной информацией ограниченного доступа на электронных носителях.

владеть:

навыками работы со служебной информацией ограниченного доступа и обеспечения ее сохранности.

6. ОРГАНИЗАЦИОННО–ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ОБУЧЕНИЯ

6.1. Материально–технические условия реализации дополнительной профессиональной программы повышения квалификации «Работа со служебной информацией ограниченного распространения (ДСП – для служебного пользования)». Программа реализуется с использованием дистанционных образовательных технологий и электронного обучения.

Вид деятельности	Программное обеспечение	Вид оборудования
Разработка учебных материалов	Обучающе–контролирующая система	Компьютер с выходом в Интернет
Разработка тестов оценки знаний	Обучающе–контролирующая система	Компьютер с выходом в Интернет
Информационная поддержка слушателей	Почтовая программа Gmail	Компьютер с выходом в Интернет

При проведении занятий используются нормативные правовые акты и документы, учебно–методическая литература.

6.2. Реализация программы с применением дистанционных образовательных технологий (ДОТ).

Программа реализуется с использованием дистанционных образовательных технологий и электронного обучения. Для организации и реализации внеаудиторной работы слушателей используется Электронный образовательный ресурс – методическое обеспечение, включающее текстовые, аудиовизуальные и мультимедийные учебно-методические материалы и электронные версии учебно–методических материалов. Видео– и аудио–конференции, чаты, пересылка изучаемых материалов, дискуссии и семинары, проводятся с использованием дистанционных образовательных технологий (ДОТ).

Учебный центр (УЦ) при реализации образовательных программ с использованием электронного обучения и ДОТ обеспечивает порядок и формы доступа слушателей и преподавателей к информационным образовательным ресурсам, посредством предоставления индивидуальных логина и пароля, и последующей их активации.

Образовательный процесс с использованием электронного обучения и ДОТ проводится в соответствии с утвержденными учебными планами, графиками занятий, а также действующими нормативными документами, регламентирующими образовательный процесс.

Основными видами деятельности с применением ДОТ являются:

– лекции, реализуемые во всех технологических средах: работа с электронными

учебными курсами, в системах on–line (вебинар, чат и т.д.) и off–line (видео–лекции, лекции–презентации и т.д.);

– практические и семинарские занятия во всех технологических средах (вебинар, собеседование в чате и т.д.);

– индивидуальные и групповые консультации, реализуемые во всех технологических средах (вебинар, чат и т.д.);

– самостоятельная работа слушателей, в том числе работа с электронными версиями учебно–методических материалов;

– текущий контроль с применением электронного обучения и/или ДОТ;

– промежуточные аттестации с применением электронного обучения и/или ДОТ;

– итоговая аттестация с применением электронного обучения и/или ДОТ.

6.3. Кадровое обеспечение.

Реализация дополнительной профессиональной программы повышения квалификации обеспечена педагогическими кадрами, как из числа преподавательского состава УЦ, так и приглашенных преподавателей, имеющими профильное высшее образование.

Состав итоговой аттестационной комиссии по данной программе формируется из числа педагогический работников, специалистов и руководителей УЦ, прошедших соответствующую подготовку и аттестацию по обеспечению антитеррористической безопасности учреждений и работе со служебной информацией ограниченного распространения, содержащейся в документах об антитеррористической защищенности организации.

6.4. Учебно–методическое и информационное обеспечение дисциплины (модуля)

Организационно-педагогические условия реализации дополнительной профессиональной программы повышения квалификации с применением дистанционных образовательных технологий и электронного обучения обеспечивают реализацию программы в полном объеме, в соответствии с необходимым качеством подготовки слушателей.

Применяемые средства, методы обучения соответствуют возрастным особенностям, способностям, интересам и потребностям слушателей: периодическая печать, учебные, методические, справочные пособия, компьютерные программы (обучающие и профессиональные).

Слушатели обеспечены консультационной поддержкой опытных организаторов и высокопрофессиональных преподавателей.

Каждый слушатель обеспечен доступом к информационным ресурсам (электронным библиотечным ресурсам, компьютерным базам данных и др.), соответствующим по содержанию темам дисциплин программы, наличием электронных учебников, учебно-методических пособий, разработок и рекомендаций по всем темам и по всем видам занятий, а

также наглядными пособиями в электронной форме. Источники учебной информации отвечают современным требованиям.

Слушатель обеспечивается полным комплектом учебно-методических материалов по теме курса повышения квалификации: учебно-методические материалы на электронном носителе, мультимедийные презентации, видео и другие дополнительные материалы.

Доступ к материалам курса осуществляется слушателями под индивидуальными логинами и паролями, через личный кабинет слушателя на сайте дистанционного обучения.

Материально-техническая база организации, предоставляющей образовательные услуги, обеспечивает нормальное и ритмичное проведение всех видов учебных занятий, предусмотренных учебным планом и реализацию установленных требований.

Образовательная деятельность в УЦ организована с применением информационного и коммуникационного оборудования, с использованием современных технологий обучения.

Материальная база УЦ соответствует нормативам.

7. СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

Нормативно-правовые документы

Законодательные акты Российской Федерации

1. Закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне» (с изменениями и дополнениями);
2. Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изменениями и дополнениями);
3. Федеральный закон от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму» (с изменениями и дополнениями);
4. Федеральный закон от 28 декабря 2010 года № 390-ФЗ «О безопасности» (с изменениями и дополнениями);

Указы Президента Российской Федерации

5. Указ Президента Российской Федерации от 13 сентября 2004 года № 1167 «О неотложных мерах по повышению эффективности борьбы с терроризмом»;
6. Указ Президента Российской Федерации от 15 февраля 2006 года № 116 «О мерах по противодействию терроризму» (с изменениями и дополнениями);
7. Указ Президента Российской Федерации от 14 июня 2012 года № 851 «О порядке установления уровней террористической опасности, предусматривающих принятие дополнительных мер по обеспечению безопасности личности, общества и государства»;

8. Указ Президента Российской Федерации от 26 декабря 2015 года № 664 «О мерах по совершенствованию государственного управления в области противодействия терроризму» (с изменениями и дополнениями);
9. Указ Президента Российской Федерации от 31 декабря 2015 года № 683 «О стратегии национальной безопасности Российской Федерации»;
10. Указ Президента Российской Федерации от 30 ноября 2016 года № 640 «Об утверждении концепции внешней политики Российской Федерации»;

Концепции

11. Концепция противодействия терроризму в Российской Федерации (утверждена Президентом РФ от 05.10.2009);
12. Концепция общественной безопасности в Российской Федерации (утверждена Президентом РФ от 14.11.2013 № Пр-2685);

Постановления Правительства Российской Федерации

13. Постановление Правительства Российской Федерации от 25 декабря 2013 года № 1244 «Об антитеррористической защищенности объектов (территорий)» (с изменениями и дополнениями).

Учебно-методическая литература

1. Антитеррористическая безопасность: Сборник материалов III Всероссийской научно-практической конференции / под общ. ред. В.Н. Нозикова, А.В. Печерского, А.Ю. Малыгина. - Пенза: Приволжский Дом знаний, 2019. - 244 с.
2. Афонин С.А., Вартанова Е.Л., Зинченко Е.П. и др. Современный терроризм и борьба с ним: социально-гуманитарные измерения. -- М.: МНЦМО, 2017. - 216 с.
3. Бельский В.Ю., Сацута А.И. Терроризм как социально – политическое явление. Противодействие в современных условиях: монография. – М.: ЮНИТИ – ДАНА, 2015. – 367 с.
4. Бутрин С.М. Политические технологии противодействия терроризму в Российской Федерации: дис… канд. полит. наук. -М., 2016.
5. Горбунов Ю.С. Терроризм и правовое регулирование противодействия ему: монография. - М.: Молодая гвардия, 2018. - 460 с.
6. Карпов А.В. Экстремизм и его спутник терроризм - реальные угрозы российской государственности / А.В.Карпов, В.В.Ломакин // Нац. интересы: приоритеты и безопасность. - 2010. - N 17. - С.112.
7. Метелев С.Е. Современный терроризм и методы антитеррористической деятельности: монография. - М.: ЮНИТИ-ДАНА. Закон и право, 2018. - 308с.
8. Моторный И.Д. Защита гражданских объектов от терроризма : науч.-практ. пособие / И.Д. Моторный. - М.: Изд. дом Шумиловой И.И., 2015. - 163 с.

9. Ольшанский Д.В. Психология терроризма. – СПб: «Питер», 2012. – 215 с.
10. Основы противодействия терроризму: учебное пособие / Я. Д. Вишняков [и др.] ; под ред. Я.Д. Вишнякова. - М.: Academia, 2016. - 235 с.
11. Петров С.В. Обеспечение безопасности организаций и производственных объектов. Практич. пособие: - М.: НЦ ЭНАС, 2017.
12. Репин Ю.В. «Безопасность и защита человека в чрезвычайных ситуациях». – М.: Дрофа, 2015. – С.98.

8. ФОРМЫ АТТЕСТАЦИИ

Итоговая аттестация (экзамен) – итоговое тестирование по всем модулям программы.

Контроль успеваемости слушателей включает в себя целенаправленный систематический мониторинг освоения слушателями дополнительной профессиональной программы повышения квалификации в целях:

- получения необходимой информации о выполнении слушателями дополнительной профессиональной программы повышения квалификации,
- оценки уровня знаний, умений и приобретенных (усовершенствованных) слушателями компетенций;
- стимулирования самостоятельной работы слушателей.

После изучения всех разделов качество освоения проверяется тестированием.

Итоговые вопросы тестирования для подготовки и проверки знаний лиц, прошедших обучение по Программе, представлены в электронной комплексной системе подготовки и итоговой аттестации (экзамена) – обучающе-контролирующей системе.

Итоговая аттестация для слушателей проводится в соответствии с требованиями, установленными Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказом Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

К итоговой аттестации допускаются лица, выполнившие требования, предусмотренные дополнительной профессиональной программой повышения квалификации и успешно изучившие все модули, и темы, предусмотренные учебным планом.

Итоговая аттестация проводится в сроки, предусмотренные учебным планом и календарным графиком учебного процесса.

Форма проведения итоговой аттестации (экзамена) – тестирование в обучающе-контролирующей системе.

Экзаменующийся на право получения удостоверения о повышении квалификации должен ответить на сформированные программой тестовые вопросы в ограниченный временной интервал.

Экзаменационные тесты включают темы изученных предметов, представляют собой тестовую часть в виде вопроса или утверждения и 3-5 вариантов ответов на каждый вопрос.

Результаты итогового экзамена оцениваются в режиме «зачет» и «не зачет».

Итоговый экзамен считается сданным, если соискатель правильно ответил не менее чем на 90% вопросов.

Лицам, успешно освоившим дополнительную профессиональную программу повышения квалификации, решением аттестационной комиссии учебного центра выдается документ об окончании обучения – удостоверение о повышении квалификации.

В состав аттестационной комиссии входят: председатель комиссии и члены комиссии.

Аттестационную комиссию возглавляет Председатель, который организует и контролирует ее деятельность, обеспечивает единство требований, предъявляемых к слушателям.

В случае, если слушатель не может пройти итоговую аттестацию по уважительным причинам (болезнь, производственная необходимость и др.), которые могут быть подтверждены соответствующими документами, то ему могут быть перенесены сроки прохождения итоговой аттестации на основе личного заявления.

Лицам, не прошедшим итоговое тестирование или получившим на итоговой аттестации оценку «неудовлетворительно», а также лицам, освоившим часть дополнительной профессиональной программы профессиональной переподготовки и (или) отчисленным в ходе освоения дополнительной профессиональной программы, выдается справка об обучении.

9. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Примерные тестовые вопросы для проведения промежуточной и итоговой аттестации

1. ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ЗАЩИТЫ СЛУЖЕБНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

1. Какая информация относится к служебной информации ограниченного распространения?

А) информация, не подлежащая огласке

Б) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуется служебной необходимостью

В) информация, не подлежащая разглашению, либо на распространение которой наложены ограничения вследствие возможного причинения вреда лицам, заинтересованным в ее нераспространении

2. На каком законе основывается регулирование информации, информационных технологий и защита информации?

А) Федеральный закон от 20.04.1995 № 45-ФЗ

Б) Федеральный закон от 22.10.2004 № 125-ФЗ

В) Федеральный закон от 27.07.2006 № 149-ФЗ

3. К каком типу информации относится информация о тайне голосования?

А) информация ограниченного распространения

Б) общедоступная информация

В) персональная информация

4. К какому типу информации относятся персональные данные?

А) информация ограниченного распространения

Б) общедоступная информация

В) государственная тайна

5. Какие виды информации существуют в зависимости от порядка ее предоставления или распространения?

А) информация, свободно распространяемая

Б) информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях

В) информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению

Г) все вышеперечисленная

Д) варианты Б и В

6. Кто может быть обладателем информации?

А) гражданин (физическое лицо), юридическое лицо

Б) субъект Российской Федерации

В) муниципальное образование

Г) все вышеперечисленное

Д) варианты А и Б

7. Какие права есть у обладателей информации?

А) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа

Б) использовать информацию, в том числе распространять ее, по своему усмотрению

В) передавать информацию другим лицам по договору или на ином установленном законом основании

Г) все вышеперечисленное

Д) варианты Б и В

8. Какая информация относится к общедоступной?

А) информация, касающаяся деятельности организаций

Б) общеизвестные сведения и иная информация, доступ к которой не ограничен

В) информация, составляющая профессиональную тайну

9. Информация, размещаемая ее обладателями в сети Интернет в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является…

А) общедоступной информацией, размещаемой в форме открытых данных

Б) закрытая информация ограниченного пользования

В) частично доступная информация

10. Доступ к какой информации не может быть ограничен?

А) о состоянии здоровья работников

Б) о трудовом стаже работников

В) о состоянии окружающей среды

11. Какая информация предоставляется бесплатно?

А) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях

Б) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица

В) оба варианта правильные

12. При каких условиях может быть ограничен срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну?

А) в соответствии с письменным распоряжением руководителя организации

Б) только с согласия гражданина (физического лица), предоставившего такую информацию о себе

В) для соблюдения требований здоровой конкуренции

13. Какой документ устанавливает требования к осуществлению взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти?

А) Федеральный закон от 06.04.2011 г. № 63-ФЗ

Б) Федеральный закон от 27.07.2006 г. № 149-ФЗ

В) Федеральный закон от 29.12.2012 г. № 273-ФЗ

14. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

А) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

Б) соблюдение конфиденциальности информации ограниченного доступа

В) реализацию права на доступ к информации

Г) все вышеперечисленное

Д) варианты Б и В

15. Чем должна ограничиваться обработка персональных данных?

А) достижением конкретных, заранее определенных и законных целей

Б) согласием объекта, предоставившего персональные данные

В) интересами работодателя

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

А) обязано

Б) не обязано

В) обязано, если оператор получил согласие субъекта персональных данных в электронном виде

17. На кого возлагается обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных?

А) на работодателя

Б) на оператора

В) на лицо, осуществляющее обработку персональных данных по поручению оператора

18. Допускается ли получение согласия субъекта персональных данных на обработку его персональных данных в форме электронного документа в целях предоставления государственных и муниципальных услуг?

А) допускается

Б) не допускается

В) допускается только при отсутствии возможности получить письменное согласие

19. Каким образом может быть предоставлено согласие оператору на обработку персональных данных, разрешенных субъектом персональных данных для распространения?

А) непосредственно

Б) с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных

В) оба варианта правильные

20. Необходимо ли согласие субъекта на обработку его биометрических данных?

А) согласие необходимо

Б) согласие не обязательно

В) согласие не нужно, если биометрические данные используются оператором для установления личности субъекта персональных данных

21. Что такое архивный документ?

А) материальный носитель с зафиксированной на нем информацией, который имеет реквизиты, позволяющие его идентифицировать, и подлежит хранению в силу значимости указанных носителя и информации для граждан, общества и государства

Б) архивный документ, отражающий трудовые отношения работника с работодателем

В) архивный документ, прошедший экспертизу ценности документов, поставленный на государственный учет и подлежащий постоянному хранению

22. Что такое особо ценный документ?

А) документ Архивного фонда Российской Федерации, который имеет непреходящую культурно-историческую и научную ценность, особую важность для общества и государства и в отношении которого установлен особый режим учета, хранения и использования

Б) архивный документ, отражающий трудовые отношения работника с работодателем

В) архивный документ, прошедший экспертизу ценности документов, поставленный на государственный учет и подлежащий постоянному хранению

23. Что такое уникальный документ?

А) документ, который имеет непреходящую культурно-историческую и научную ценность, особую важность для общества и государства и в отношении которого установлен особый режим учета, хранения и использования

Б) особо ценный документ, не имеющий себе подобных по содержащейся в нем информации и (или) его внешним признакам, невосполнимый при утрате с точки зрения его значения и (или) автографичности

В) архивный документ, прошедший экспертизу ценности документов, поставленный на государственный учет и подлежащий постоянному хранению

24. Что такое экспертиза ценности документов?

А) изучение документов на основании критериев их ценности в целях определения сроков хранения документов и отбора их для включения в состав Архивного фонда Российской Федерации

Б) комплекс работ по формированию архивных документов в единицы хранения (дела), описанию и оформлению таких единиц хранения

В) хранение архивных документов до их уничтожения в течение сроков, установленных нормативными правовыми актами

25. Что представляет собой временное хранение архивных документов?

А) изучение документов на основании критериев их ценности в целях определения сроков хранения документов и отбора их для включения в состав Архивного фонда

Б) комплекс работ по формированию архивных документов в единицы хранения (дела), описанию и оформлению таких единиц хранения

В) хранение архивных документов до их уничтожения в течение сроков, установленных нормативными правовыми актами

2. ОБЕСПЕЧЕНИЕ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИЙ

26. Какая деятельность должна быть организована в рамках работы со служебной информацией ограниченного распространения?

А) организовано и проведено категорирование объектов (территорий), подлежащих антитеррористической защите

Б) оформлен акт обследования и категорирования объекта (территории)

В) разработан паспорт безопасности объекта (территории)

Г) все вышеперечисленное

Д) варианты Б и В

27. Являются ли Перечни объектов (территорий), подлежащих антитеррористической защите, документами, содержащими служебную информацию ограниченного распространения?

А) являются

Б) не являются

В) являются, если численность работников на объекте более 100 человек

28. На основании чего определяется степень угрозы совершения террористического акта?

А) на основании Приказов МЧС

Б) на основании количественных показателей государственных статистических данных о совершенных и предотвращенных за последние 12 месяцев террористических актах

В) на основании сведений о возможных угрозах совершения террористического акта в районе расположения объекта

Г) варианты А и Б

Д) варианты Б и В

29. Прогнозный показатель количества пострадавших в результате возможных последствий совершения террористического акта на объекте (территории) принимается…

А) равным максимальному количеству единовременно пребывающих людей на объекте (территории) в рабочие дни

Б) равным минимальному количеству единовременно пребывающих людей на объекте (территории) в рабочие дни

В) равным максимальному количеству единовременно пребывающих людей на объекте (территории) в выходные дни

30. В течение какого срока создается комиссия по обследованию и категорированию объекта в отношении функционирующего объекта?

А) в течение 1 месяца со дня утверждения требований Постановления Правительства РФ от 02.08.2019 № 1006

Б) в течение 2 месяцев со дня утверждения требований Постановления Правительства РФ от 02.08.2019 № 1006

В) в течение 6 месяцев со дня утверждения требований Постановления Правительства РФ от 02.08.2019 № 1006

31. В течение какого срока создается комиссия по обследованию и категорированию объекта при вводе в эксплуатацию нового объекта?

А) в течение 14 дней со дня окончания мероприятий по вводу объекта в эксплуатацию

Б) в течение 2 месяцев со дня окончания мероприятий по вводу объекта в эксплуатацию

В) в течение 3 месяцев со дня окончания мероприятий по вводу объекта в эксплуатацию

32. В какой максимальный срок со дня создания комиссии по обследованию и категорированию объекта осуществляется ее работа?

А) 14 рабочих дней

Б) 30 рабочих дней

В) 60 рабочих дней

33. Что из перечисленного обычно рассматривается в качестве критических элементов объекта (территории)?

А) зоны, конструктивные и технологические элементы объекта (территории), в том числе зданий, инженерных сооружений и коммуникаций

Б) элементы систем, узлы оборудования или устройств потенциально опасных установок на объекте (территории)

В) места использования или хранения опасных веществ и материалов на объекте (территории)

Г) все вышеперечисленное

Д) варианты Б и В

34. Как оформляются результаты работы комиссии по обследованию и категорированию объекта?

А) приказом

Б) служебной запиской

В) актом

35. Сколько составляется экземпляров акта обследования и категорирования объекта (территории)?

А) 1 экземпляр

Б) 2 экземпляра

В) 3 экземпляра

36. Является ли служебная информация о состоянии антитеррористической защищенности объекта (территории), содержащаяся в акте обследования и категорирования объекта (территории), и принимаемых мерах по ее усилению служебной информацией ограниченного распространения?

А) является

Б) не является

В) является только на объектах 1 и 2 категории опасности

37. Антитеррористическая защищенность объектов (территорий) обеспечивается путем осуществления комплекса мер, направленных:

А) на воспрепятствование неправомерному проникновению на объекты (территории)

Б) на выявление нарушителей, установленных на объектах (территориях) пропускного и внутриобъектового режимов и (или) признаков подготовки или совершения террористического акта

В) на пресечение попыток совершения террористических актов на объектах (территориях)

Г) все вышеперечисленное

Д) варианты А и В

38. Какие мероприятия осуществляются в целях обеспечения антитеррористической защищенности объектов, отнесенных к 4 категории опасности?

А) разработка планов эвакуации работников; обеспечение пропускного и внутриобъектового режимов и осуществление контроля за их функционированием; оснащение

объектов (территорий) системами передачи тревожных сообщений в подразделения войск национальной гвардии РФ

Б) оснащение объектов (территорий) системами видеонаблюдения, охранной сигнализации; обеспечение охраны объектов (территорий) сотрудниками частных охранных организаций, подразделениями вневедомственной охраны войск национальной гвардии РФ

В) оборудование объектов (территорий) системой контроля и управления доступом; оснащение въездов на объект (территорию) воротами, обеспечивающими жесткую фиксацию их створок в закрытом положении

39. Какие мероприятия осуществляются в целях обеспечения антитеррористической защищенности объектов, отнесенных к 3 категории опасности?

А) разработка планов эвакуации работников; обеспечение пропускного и внутриобъектового режимов и осуществление контроля за их функционированием; оснащение объектов (территорий) системами передачи тревожных сообщений в подразделения войск национальной гвардии РФ

Б) оснащение объектов (территорий) системами видеонаблюдения, охранной сигнализации; обеспечение охраны объектов (территорий) сотрудниками частных охранных организаций, подразделениями вневедомственной охраны войск национальной гвардии РФ

В) оборудование объектов (территорий) системой контроля и управления доступом; оснащение въездов на объект (территорию) воротами, обеспечивающими жесткую фиксацию их створок в закрытом положении

Г) все вышеперечисленное

Д) варианты А и Б

40. Какие мероприятия осуществляются в целях обеспечения антитеррористической защищенности объектов, отнесенных к 2 категории опасности?

А) разработка планов эвакуации работников; обеспечение пропускного и внутриобъектового режимов и осуществление контроля за их функционированием; оснащение объектов (территорий) системами передачи тревожных сообщений в подразделения войск национальной гвардии РФ

Б) оснащение объектов (территорий) системами видеонаблюдения, охранной сигнализации; обеспечение охраны объектов (территорий) сотрудниками частных охранных организаций, подразделениями вневедомственной охраны войск национальной гвардии РФ

В) оборудование объектов (территорий) системой контроля и управления доступом; оснащение въездов на объект (территорию) воротами, обеспечивающими жесткую фиксацию их створок в закрытом положении

Г) все вышеперечисленное

Д) варианты Б и В

41. Какие мероприятия осуществляются в целях обеспечения антитеррористической защищенности объектов, отнесенных к 1 категории опасности?

А) оборудование контрольно-пропускных пунктов при входе (въезде) на прилегающую территорию объекта (территории); оснащение въездов на объект (территорию) средствами снижения скорости и (или) противотаранными устройствами

Б) оснащение объектов (территорий) системами видеонаблюдения, охранной сигнализации; обеспечение охраны объектов (территорий) сотрудниками частных охранных организаций, подразделениями вневедомственной охраны войск национальной гвардии РФ

В) оборудование объектов (территорий) системой контроля и управления доступом; оснащение въездов на объект (территорию) воротами, обеспечивающими жесткую фиксацию их створок в закрытом положении

Г) все вышеперечисленное

Д) варианты А и В

42. Что должна обеспечивать система видеонаблюдения на объекте?

А) непрерывное видеонаблюдение уязвимых мест и критических элементов объекта (территории), архивирование и хранение данных

Б) оперативное информирование лиц, находящихся на объекте (территории), о необходимости эвакуации и других действиях, обеспечивающих безопасность людей и предотвращение паники

В) разборчивость передаваемой речевой информации

43. Что должна обеспечивать система оповещения и управления эвакуацией людей на объекте?

А) непрерывное видеонаблюдение уязвимых мест и критических элементов объекта (территории), архивирование и хранение данных

Б) оперативное информирование лиц, находящихся на объекте (территории), о необходимости эвакуации и других действиях, обеспечивающих безопасность людей и предотвращение паники

В) разборчивость передаваемой речевой информации

Г) варианты А и Б

Д) варианты Б и В

44. В какой срок система видеонаблюдения должна обеспечивать архивирование и хранение данных?

А) в течение 1 суток

Б) в течение 1 недели

В) в течение 1 месяца

45. Какова периодичность проведения плановых проверок в форме документального контроля, выездного обследования антитеррористической защищенности объектов?

А) не реже 1 раза в год

Б) не реже 1 раза в 3 года

В) не реже 1 раза в 5 лет

46. На каком основании проводятся внеплановые проверки?

А) несоблюдения на объектах (территориях) требований к их антитеррористической защищенности, в том числе при поступлении от граждан жалоб на несоблюдение требований к антитеррористической защищенности объектов (территорий) и (или) бездействие должностных лиц органов (организаций), являющихся правообладателями объектов (территорий), в отношении обеспечения антитеррористической защищенности объектов (территорий)

Б) при необходимости актуализации паспорта безопасности объекта (территории)

В) в целях осуществления контроля за устранением недостатков, выявленных в ходе проведения плановых проверок антитеррористической защищенности объектов (территорий)

Г) все вышеперечисленное

Д) варианты Б и В

47. Каков максимальный срок проведения проверки антитеррористической защищенности объекта (территории)?

А) 1 сутки

Б) 5 рабочих дней

В) 14 суток

48. Какой документ составляется после проведения обследования и категорирования объекта (территории) комиссией?

А) паспорт безопасности объекта (территории)

Б) регламент обеспечения безопасности объекта

В) приказ об устранении недостатков

49. В какой срок после проведения обследования и категорирования объекта (территории) комиссией составляется паспорт безопасности объекта (территории)?

А) в течение 3 дней

Б) в течение 7 дней

В) в течение 30 дней

50. Каков максимальный срок, в течение которого осуществляется согласование паспорта безопасности объекта (территории) со дня его подписания?

А) 5 рабочих дней

Б) 10 рабочих дней

В) 45 рабочих дней

3. ПОРЯДОК ОБРАЩЕНИЯ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

51. Какой пометкой маркируют документы с ограниченным доступом?

А) только для персонала

Б) конфиденциально

В) для служебного пользования

52. На каком листе документа для служебного пользования указывают соответствующее количество отпечатанных экземпляров, вносят фамилию исполнителя, дату создания документа?

А) на обороте каждого последнего листа экземпляра документа

Б) на обороте каждого первого листа экземпляра документа

В) на первом листе экземпляра документа

53. Можно ли предавать документы с пометкой ДСП в электронном виде?

А) можно

Б) нельзя

В) только по защищенным каналам связи

54. Можно ли отнести к документам с пометкой ДСП сведения о возникших чрезвычайных ситуациях, об опасных природных явлениях?

А) можно

Б) нельзя

В) можно с разрешения руководителя организации

55. В соответствии с каким документом проводятся работы по защите служебной информации ограниченного распространения в органах системы МВД России?

А) Приказ МЧС России от 10.03.2006 г. № 144ДСП

Б) Приказ Судебного департамента при Верховном Суде РФ от 04.08.2015 г. № 228

В) Приказ МВД России от 9 ноября 2018 г. № 755

56. В системе МВД организация защиты служебной информации ограниченного распространения осуществляется в целях:

А) предотвращения утечки, хищения служебной информации ограниченного распространения по техническим каналам

Б) предотвращения несанкционированного уничтожения, искажения, подделки, копирования, распространения, блокирования служебной информации ограниченного распространения

В) предотвращения неправомерного или несанкционированного доступа к служебной информации ограниченного распространения

Г) все вышеперечисленное

Д) варианты Б и В

57. Кто в системе МВД организует своевременное проведение мероприятий по обеспечению сохранности служебной информации ограниченного распространения и ограничению доступа к ней при ее использовании, обработке, регистрации, пересылке, хранении и уничтожении?

А) руководители (начальники) органов, организаций, подразделений системы МВД

Б) служба корпоративной защиты

В) оперуполномоченные

58. Где осуществляется хранение документов, содержащих служебную информацию ограниченного распространения?

А) в рабочих столах сотрудников под замком

Б) в надежно запираемых шкафах, ящиках или хранилищах, оборудованных приспособлениями для опечатывания

В) в сейфах

59. Какой документ составляется на утраченные документы, дела и издания, содержащие служебную информацию ограниченного распространения?

А) приказ

Б) рапорт

В) акт

60. Кем осуществляется проставление пометки «Для служебного пользования»?

А) руководителем организации

Б) специалистом службы корпоративной защиты

В) исполнителем документа или должностным лицом, подписывающим или утверждающим этот документ, исходя из его содержания

61. Кем осуществляется уничтожение черновиков документа, содержащего служебную информацию ограниченного распространения?

А) исполнителем документа

Б) сотрудником подразделения делопроизводства

В) административно-хозяйственной службой

62. Что составляется при необходимости направления документов с пометкой «Для служебного пользования» на несколько адресов?

А) перечень адресатов

Б) указатель рассылки

В) список получателей

63. Какой документ составляется при смене сотрудника, ответственного за учет документов, содержащих служебную информацию ограниченного распространения?

А) акт приема-передачи этих документов, который подписывается сдающим и принимающим сотрудниками и утверждается руководителем (начальником) органа, организации, подразделения системы МВД России или лицом, им уполномоченным

Б) приказ о назначении ответственного

В) приказ о снятии полномочий

64. В каком случае разрешается открытое опубликование или распространение служебной информации ограниченного распространения?

А) в случае чрезвычайной ситуации

Б) после снятия в установленном порядке введенных ограничений

В) с письменного разрешения носителя информации

65. Что из перечисленного может являться основаниями для снятия пометки «Для служебного пользования» в системе МВД с документов?

А) необоснованное или осуществленное в нарушение законодательных и иных нормативных правовых актов Российской Федерации присвоение документу пометки «Для служебного пользования»

Б) наличие вступившего в законную силу решения суда, содержащего предписание о снятии ограничений на распространение содержащихся в документе сведений

В) изменение объективных обстоятельств, вследствие которых разглашение (распространение) конкретных сведений не нанесет ущерба интересам МВД России, и их защита становится нецелесообразной

Г) все вышеперечисленное

Д) варианты Б и В

66. Какой документ определяет порядок обращения со служебной информацией ограниченного распространения в федеральных судах?

А) Приказ МЧС России от 10.03.2006 г. № 144ДСП

Б) Приказ Судебного департамента при Верховном Суде РФ от 04.08.2015 г. № 228

В) Приказ МВД России от 9 ноября 2018 г. № 755

67. Кем принимается решение об отнесении служебного документа, подготовленного в суде, к разряду ограниченного распространения и о необходимости проставления пометки?

А) секретарем суда

Б) председателем (исполняющим обязанности председателя) соответствующего суда или иным уполномоченным им лицом по предложению исполнителя документа или иного лица, подписывающего или утверждающего документ

В) прокурором

68. Допускается ли выносить документы, передавать служебную информацию ограниченного распространения в судах по каналам факсимильной связи и электронной почте?

А) допускается

Б) запрещается

В) допускается с разрешения руководителя

69. Какой документ определяет порядок организации защиты служебной информации ограниченного распространения в налоговых органах?

А) Приказ МЧС России от 10.03.2006 г. № 144ДСП

Б) Приказ Федеральной налоговой службы от 21.04.2021 г. № ЕД-7-24/391@

В) Приказ МВД России от 9 ноября 2018 г. № 755

70. Что из перечисленного относится к целям защиты служебной информации ограниченного распространения в налоговой службе?

А) предотвращение утечки, хищения служебной информации ограниченного распространения по техническим каналам

Б) предотвращение несанкционированного уничтожения, искажения, подделки, копирования, распространения служебной информации ограниченного распространения

В) предотвращение неправомерного или случайного доступа неуполномоченных должностных лиц к служебной информации ограниченного распространения

Г) все вышеперечисленное

Д) варианты Б и В

71. Допускается ли печать электронных документов, а также электронных образов документов на бумажном носителе с пометкой ДСП?

А) допускается

Б) не допускается

В) допускается с использованием средств печати и копирования, подключенных к аттестованным информационным системам

72. Каким документом утвержден порядок обращения со служебной информацией ограниченного распространения в Министерстве здравоохранения?

А) Приказом Минздрава России от 10.03.2006 г. № 144ДСП

Б) Приказом Минздрава России от 9 ноября 2018 г. № 755

В) Приказом Министерства здравоохранения РФ от 14.07.2020 г. № 700н

73. Что из перечисленного относится к целям защиты служебной информации ограниченного распространения в налоговой службе?

А) предотвращение неправомерного (случайного) доступа неуполномоченных должностных лиц к служебной информации ограниченного распространения

Б) соблюдение конфиденциальности служебной информации ограниченного распространения

В) обеспечение полноты, целостности и достоверности служебной информации ограниченного распространения в системах подготовки, учета, хранения и обработки данных и документов

Г) все вышеперечисленное

Д) варианты Б и В

74. Какие информационные ресурсы подлежат защите в налоговой службе?

А) информационные ресурсы, содержащие сведения, отнесенные к служебной информации ограниченного распространения

Б) носители информации, содержащие служебную информацию ограниченного распространения, имеющиеся в распоряжении Министерства

В) программные средства, используемые для обработки служебной информации ограниченного распространения

Г) все вышеперечисленное

Д) варианты Б и В

75. Каким документом регламентирован порядок обращения со служебной информацией ограниченного распространения в организациях Министерства образования и науки Российской Федерации?

А) Приказом Министерства образования и науки РФ от 30 декабря 2010 г. № 2233

Б) Приказом Минздрава России от 9 ноября 2018 г. № 755

В) Приказом Министерства здравоохранения РФ от 14.07.2020 г. № 700н

4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

76. Какое из определений относится к понятию «Информационная безопасность»?

А) сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации

Б) защита компьютерных систем и сетей от раскрытия информации, кражи или повреждения их оборудования, программного обеспечения или электронных данных

В) совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных

77. Какова цель обеспечения информационной безопасности в организации?

А) обеспечение защиты компьютерных систем и сетей от кражи или повреждения их аппаратного обеспечения

Б) защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения

В) обеспечение защиты учетных данных пользователей

78. Какие существуют правовые, организационные и технические меры для защиты информации?

А) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

Б) соблюдение конфиденциальности информации ограниченного доступа

В) реализацию права на доступ к информации

Г) все вышеперечисленное

Д) варианты Б и В

79. Какие существуют организационно технические меры защиты информации при работе с электронным архивом?

А) экранирование помещений

Б) периодическая смена пароля пользователей

В) шифрование информации при передаче по компьютерным каналам связи

Г) все вышеперечисленное

Д) варианты Б и В

80. Как осуществляется государственное регулирование отношений в сфере защиты информации?

А) путем установления требований о защите информации

Б) путем установления ответственности за нарушение законодательства РФ об информации, информационных технологиях и о защите информации

В) оба варианта правильные

81. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

А) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации

Б) своевременное обнаружение фактов несанкционированного доступа к информации

В) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации

Г) все вышеперечисленное

Д) варианты А и В

82. Каковы три главных принципа успешного внедрения систем информационной безопасности на предприятии?

А) защищенность, открытость, системность

Б) конфиденциальность, целостность, доступность

В) взаимозаменяемость элементов, бесперебойный режим работы, индивидуальный подход к пользователям

83. Как можно охарактеризовать сущность конфиденциальности как принципа успешного внедрения систем информационной безопасности на предприятии?

А) введение в действие контроля, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия

Б) обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной; предотвращение искажения информации

В) сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо

84. Как можно охарактеризовать сущность целостности как принципа успешного внедрения систем информационной безопасности на предприятии?

А) введение в действие контроля, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия

Б) обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной; предотвращение искажения информации

В) сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо

85. Как можно охарактеризовать сущность доступности как принципа успешного внедрения систем информационной безопасности на предприятии?

А) введение в действие контроля, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия

Б) обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной; предотвращение искажения информации

В) сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо

86. Что представляет собой административный вид контроля информационной безопасности?

А) вид контроля, который состоит из утвержденных процедур, стандартов и принципов; он формирует рамки для ведения бизнеса и управления людьми

Б) средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации

В) среда рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.)

87. Что представляет собой логический вид контроля информационной безопасности?

А) вид контроля, который состоит из утвержденных процедур, стандартов и принципов; он формирует рамки для ведения бизнеса и управления людьми

Б) средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации

В) среда рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.)

88. Что представляет собой физический вид контроля информационной безопасности?

А) вид контроля, который состоит из утвержденных процедур, стандартов и принципов; он формирует рамки для ведения бизнеса и управления людьми

Б) средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации

В) среда рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.)

89. Что из перечисленного относится к естественным угрозам информационной безопасности?

А) катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии

Б) хакерские атаки, противоправные действия конкурентов, месть сотрудников

В) компьютерные вирусы

90. Что из перечисленного относится к искусственным непреднамеренным угрозам информационной безопасности?

А) катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии

Б) хакерские атаки, противоправные действия конкурентов, месть сотрудников

В) ошибки, которые совершаются людьми по неосторожности или незнанию

91. Что из перечисленного относится к искусственным преднамеренным угрозам информационной безопасности?

А) пожары, ураганы, наводнение, удары молнии

Б) хакерские атаки, противоправные действия конкурентов, месть сотрудников

В) ошибки, которые совершаются людьми по неосторожности или незнанию

92. Какие виды угроз информационной безопасности наиболее опасны?

А) преднамеренные угрозы

Б) естественные угрозы

В) искусственные угрозы

93. Что такое средства защиты информационной безопасности?

А) набор технических приспособлений, устройств, приборов различного характера, которые препятствуют утечке информации и выполняют функцию ее защиты

Б) системы видеонаблюдения

В) обучение сотрудников информационной грамотности

94. Какие средства защиты информации называют организационными?

А) совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и организационно-правовых (законодательная база, статут конкретной организации) средств

Б) программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней

В) технические виды устройств, которые защищают информацию от проникновения и утечки

95. Какие средства защиты информации называют программными?

А) совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и организационно-правовых (законодательная база, статут конкретной организации) средств

Б) программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней

В) технические виды устройств, которые защищают информацию от проникновения и утечки

96. Какие средства защиты информации называют техническими?

А) совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и организационно-правовых (законодательная база, статут конкретной организации) средств

Б) программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней

В) технические виды устройств, которые защищают информацию от проникновения и утечки

97. Какие средства защиты информации являются наиболее распространенными и востребованными на сегодняшний день?

А) организационно-правовые

Б) программные

В) нормативно-правовые

98. Что такое антивирусные программы?

А) программы, которые ограничивают доступ посторонним к информации

Б) программы, которые обеспечивают сохранность файлов с информацией

В) программы, которые борются с компьютерными вирусами и возобновляют зараженные файлы

99. Что такое облачный антивирус?

А) легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера

Б) предотвращение утечки данных с помощью технологий, направленных на предотвращение потери конфиденциальной информации, которая происходит на предприятиях по всему миру

В) преобразование информации таким образом, что ее расшифровка становится возможной только с помощью определенных кодов или шифров

100. Что такое криптографические системы?

А) легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера

Б) предотвращение утечки данных с помощью технологий, направленных на предотвращение потери конфиденциальной информации, которая происходит на предприятиях по всему миру

В) преобразование информации таким образом, что ее расшифровка становится возможной только с помощью определенных кодов или шифров