



Автономная некоммерческая организация дополнительного профессионального образования  
Учебный центр  
«Гефест»

УТВЕРЖДАЮ

Директор  
Емельянова Н.Н.

«01» сентября 2024



**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА  
(программа повышения квалификации)  
«Работа со служебной документацией, содержащей информацию ограниченного  
распространения»**

Тверь

2024

## 1. Пояснительная записка

1.1. Программа повышения квалификации «Работа со служебной документацией, содержащей информацию ограниченного распространения» (далее - 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 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»;

1.2. Целью повышения квалификации по Программе 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.

1.3. Программа разработана, принята и реализована АНО ДПО УЦ «Гефест» руководствуется положениями Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

1.4. В результате освоения Программы слушатель 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.

По результатам освоения Программы слушатель должен уметь:

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.

1.5. Образовательная организация, проводящая обучение по Программе, имеет лицензию на осуществление образовательной деятельности и аккредитована Минтрудом России на оказание услуг обучения работодателей и работников вопросам охраны труда.

1.6. По окончании обучения по Программе проводится проверка знаний, и слушателям, успешно прошедшим итоговую аттестацию, выдаются удостоверения о повышении квалификации установленного образца.

## **2. Базовые требования к содержанию Программы**

2.1. Настоящая программа отвечает следующим требованиям:

не противоречит федеральным государственным образовательным стандартам высшего и среднего профессионального образования и ориентирована на современные образовательные технологии и средства обучения. Ориентация на современные образовательные технологии реализована в формах и методах обучения, в методах контроля и управления образовательным процессом и средствах обучения;

соответствует принятым правилам оформления программ.

2.2. В Программе реализован механизм варьирования между теоретической подготовкой и решением практическим задач.

2.3. Содержание Программы определено учебным планом, календарным учебным графиком (Приложение № 1) и рабочими программами учебных модулей (Приложение № 2).

2.4. Условия реализации программы и оценка качества освоения программы представлены в приложениях № 3 и 4 соответственно.

**УЧЕБНЫЙ ПЛАН И КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК**  
**дополнительной профессиональной программы повышения квалификации**  
**«Работа со служебной документацией, содержащей информацию ограниченного распространения»**

Требования к уровню подготовки слушателей, необходимому для освоения программы:

- лица, желающие освоить дополнительную профессиональную программу, должны иметь среднее профессиональное или высшее образование.

- обладать навыками работы на персональном компьютере

Категория слушателей: руководители и специалисты организаций, а также для все заинтересованные лица, уже осуществляющих или планирующих профессиональную деятельность в сфере работы со служебной информацией ограниченного распространения.

Срок обучения: 16 часов.

Формы обучения: очно-заочная с применением дистанционных образовательных технологий, заочная с применением дистанционных образовательных технологий.

**УЧЕБНЫЙ ПЛАН**

№ п/п	Наименование модулей/тем	Кол-во часов	Форма контроля		
			Лекции	Практические и семинарные работы	Тестирование
1	Законодательство в области защиты служебной информации ограниченного распространения	1	1	-	-
2	Общие положения по порядку обращения с документами и прочими материальными носителями, содержащими служебную информацию ограниченного распространения	1,5	1,5	-	-
3	Порядок приема и учета документов и изданий	1,5	1,5	-	-
4	Размножение и рассылка (отправка) документов и изданий	1,5	1,5	-	-
5	Группировка исполненных документов в дела	1,5	1,5	-	-
6	Использование документов, дел и изданий. Снятие с дел грифа «Для служебного пользования»	1	1	-	-
7	Отбор документов, дел и изданий для хранения и к уничтожению	1	1	-	-
8	Обеспечение сохранности документов, дел и изданий. Проверка их наличия	1	1	-	-
9	Формы и образцы применяемых документов	1	1		

10	Организация работы с документами, содержащими служебную информацию ограниченного распространения, на объектах (территориях)	2	2		
11	Практические, самостоятельные работы	2		2	
12	Проверка знаний	1	-	-	Тестирование
Итого:		16	13	2	1

### КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

№ п/п	Наименование модулей/тем	Итого часов, ч.		
		Д1	Д2	
1.	Законодательство в области защиты служебной информации ограниченного распространения	1		
2.	Общие положения по порядку обращения с документами и прочими материальными носителями, содержащими служебную информацию ограниченного распространения	1,5		
3.	Порядок приема и учета документов и изданий	1,5		
4.	Размножение и рассылка (отправка) документов и изданий	1,5		
5.	Группировка исполненных документов в дела	1,5		
6.	Использование документов, дел и изданий. Снятие с дел грифа «Для служебного пользования»	1		
7.	Отбор документов, дел и изданий для хранения и к уничтожению		1	
8.	Обеспечение сохранности документов, дел и изданий. Проверка их наличия		1	
9.	Формы и образцы применяемых документов		1	
10.	Организация работы с документами, содержащими служебную информацию ограниченного распространения, на объектах (территориях)		2	
11.	Практические, самостоятельные работы		2	
12.	Проверка знаний		1	
<b>ИТОГО:</b>		<b>8</b>	<b>8</b>	<b>16</b>

**РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ МОДУЛЕЙ**  
**дополнительной профессиональной программы повышения квалификации**  
**«Работа со служебной документацией, содержащей информацию ограниченного**  
**распространения»**

Рабочая программа учебных предметов, курсов, дисциплин (модулей) содержит перечень тем, а также рассматриваемых в них вопросов с учетом их трудоемкости.

Рабочая программа учебных предметов, курсов, дисциплин (модулей) является неотъемлемой частью ДПП с учетом законодательства Российской Федерации в области антитеррористической защищенности объектов (территорий).

В настоящем разделе закрепляются рабочие программы дисциплин (модулей), а также содержательный минимум, которые обучающиеся осваивают в рамках ДПП.

**Тема: 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.

**Тема: 2 Общие положения по порядку обращения с документами и прочими материальными носителями, содержащими служебную информацию ограниченного распространения**

Основы понимания по порядку обращения с документами и прочими материальными носителями, содержащими служебную информацию ограниченного распространения

**Тема 3. Порядок приема и учета документов и изданий**

Общий порядок приема и учета документов и изданий, позволяющий принять методы порядка в практической деятельности при работе с документами «Для служебного пользования»

**Тема 4. Размножение и рассылка (отправка) документов и изданий**

Принципы копирования и учета документации

**Тема 5. Группировка исполненных документов в дела**

Делопроизводство при обращении со служебной информацией ограниченного распространения

**Тема 6. Использование документов, дел и изданий. Снятие с дел грифа «Для служебного пользования»**

Работа с документами с информацией ограниченного распространения. Принципы снятия грифа ДСП

**Тема 7. Отбор документов, дел и изданий для хранения и к уничтожению**

Процедуры обеспечения хранения и подготовка к уничтожению и уничтожение сведений, содержащих ограниченный распространение.

**Тема 8. Обеспечение сохранности документов, дел и изданий. Проверка их наличия**

Проведение анализа в части сведений ограниченного доступа.

**Тема 9. Формы и образцы применяемых документов**

Образцы документов, которые могут быть применимы при работе со сведениями, содержащими ограничение на распространение.

**Тема 10. Организация работы с документами, содержащими служебную информацию ограниченного распространения, на объектах (территориях)**

Рассмотрение Постановления Правительства РФ от 3 ноября 1994 г. N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности"

**УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ****Нормативно правовые документы, используемые при изучении дополнительной профессиональной программы (программы повышения квалификации «Работа со служебной документацией, содержащей информацию ограниченного распространения»****Нормативные документы**

Федеральный закон от 6 марта 2006 г. N 35-ФЗ О противодействии терроризму

Федеральный закон от 07.08.2001 N 115-ФЗ О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

Федеральный закон от 25.07.2002 N 114-ФЗ О противодействии экстремистской деятельности

Федеральный закон от 09.02.2007 №16 О транспортной безопасности

Федеральный закон от 21.07.2011 №256 О безопасности объектов топливно-энергетического комплекса

Федеральный закон от 2 ноября 2013 года № 302-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»

Федеральный закон от 3 июля 2016 года № 226-ФЗ «О войсках национальной гвардии»

Федеральный закон от 6 июля 2016 года № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»

Федеральный закон от 6 июля 2016 года № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»

Постановление Правительства РФ от 24.10.2005 N 638

Постановление Правительства РФ от 04.05.2008 N 333

Постановление Правительства РФ от 31.03.2009 N 289 Об утверждении Правил аккредитации юридических лиц для проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств

Постановление Правительства РФ от 22.12.2011 N 1107 О порядке формирования и ведения реестра объектов топливно-энергетического комплекса

Постановление Правительства РФ от 05.05.2012 N 460 Об утверждении Правил актуализации паспорта безопасности объекта топливно-энергетического комплекса

Постановление Правительства РФ от 05.05.2012 N 459 Об утверждении Положения об исходных данных для проведения категорирования объекта топливно-энергетического комплекса, порядке его проведения и критериях категорирования

Постановление Правительства РФ от 25.12.2013 N 1244 Об антитеррористической защищенности объектов (территорий)

Постановление Правительства РФ от 04.10.2013 N 880 Об утверждении Положения о федеральном государственном контроле (надзоре) в области транспортной безопасности

Постановление Правительства РФ от 02.10.2013 N 861 Об утверждении Правил информирования субъектами топливно-энергетического комплекса об угрозах совершения и о совершении актов незаконного вмешательства на объектах топливно-энергетического комплекса

Постановление Правительства РФ от 03.12.2014 N 1309 Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека и формы паспорта безопасности этих объектов (территорий)

Постановление Правительства РФ от 15.11.2014 N 1208 Об утверждении требований по

соблюдению транспортной безопасности для физических лиц, следующих либо находящихся на объектах транспортной инфраструктуры или транспортных средствах, по видам транспорта, а также в зонах безопасности, установленных вокруг отдельных судов и (или) иных плавучих средств с ядерным реактором либо судов и (или) иных плавучих средств, транспортирующих ядерные материалы, объектов транспортной инфраструктуры

Постановление Правительства РФ от 30.10.2014 N 1130 Об утверждении требований к антитеррористической защищенности объектов (территорий), находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федерального агентства связи, Федерального агентства по печати и массовым коммуникациям, а также подведомственных им организаций, и формы паспорта безопасности таких объект

Постановление Правительства РФ от 29.08.2014 N 875 Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по техническому и экспортному контролю, ее территориальных органов и подведомственных организаций и формы паспорта безопасности этих объектов (территорий)

Постановление Правительства РФ от 25.03.2015 N 272 Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)

Постановление Правительства РФ от 06.03.2015 N 202 Об утверждении требований к антитеррористической защищенности объектов спорта и формы паспорта безопасности объектов спорта

Постановление Правительства РФ от 23.12.2016 N 1467 Об утверждении требований к антитеррористической защищенности объектов водоснабжения и водоотведения, формы паспорта безопасности объекта водоснабжения и водоотведения и о внесении изменений в некоторые акты Правительства Российской Федерации

Постановление Правительства РФ от 13.05.2016 N 410 Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства труда и социальной защиты Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, и формы паспорта безопасности этих объектов (территорий)

Постановление Правительства РФ от 23.01.2016 N 29 Об утверждении требований по обеспечению транспортной безопасности объектов транспортной инфраструктуры по видам транспорта на этапе их проектирования и строительства и требований по обеспечению транспортной безопасности объектов (зданий, строений, сооружений), не являющихся объектами транспортной инфраструктуры и расположенных на земельных участках, прилегающих к объектам транспортной инфраструктуры и отнесенных в соответствии с земельным законодательством

Постановление Правительства РФ от 11.02.2017 N 176 Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий)

Постановление Правительства РФ от 13.01.2017 N 8 Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)

Постановление Правительства РФ от 27.05.2017 N 638

Постановление Правительства Российской Федерации от 12.01.2007 № 6 «Об утверждении Правил осуществления социальной реабилитации лиц, пострадавших в результате террористического акта, а также лиц, участвующих в борьбе с терроризмом»

Постановление Правительства Российской Федерации от 21.02.2008 № 105 «О возмещении вреда, причиненного жизни и здоровью лиц в связи с их участием в борьбе с терроризмом»

Постановление Правительства Российской Федерации от 13.03.2008 № 167 «О возмещении

лицу, принимавшему участие в осуществлении мероприятия по борьбе с терроризмом, стоимости утраченного или поврежденного имущества»

Постановление Правительства Российской Федерации от 16.04.2008 № 278 «О возмещении расходов, связанных с использованием при проведении контртеррористической операции транспортных средств, принадлежащих организациям или физическим лицам»

Постановление Правительства Российской Федерации от 01.02.2011 № 42 «Об утверждении Правил охраны аэропортов и объектов их инфраструктуры» (в части определения порядка охраны аэропортов и объектов их инфраструктуры в целях предотвращения несанкционированного прохода (проезда) лиц и транспортных средств, проноса оружия, взрывчатых веществ и других опасных устройств, предметов, веществ на территорию аэропортов)

Постановление Правительства Российской Федерации от 15.02.2011 № 73 «О некоторых мерах по совершенствованию подготовки проектной документации в части противодействия террористическим актам» (в части обязательности включения в состав проектной документации требований по антитеррористической защищенности объектов)

Постановление Правительства Российской Федерации от 15.02.2014 № 110 «О выделении бюджетных ассигнований из резервного фонда Правительства Российской Федерации по предупреждению и ликвидации чрезвычайных ситуаций и последствий стихийных бедствий»

Постановление Правительства Российской Федерации от 18.04.2014 № 353 «Об утверждении Правил обеспечения безопасности при проведении официальных спортивных соревнований»

Постановление Правительства Российской Федерации от 16.07.2016 № 678 «О требованиях по обеспечению транспортной безопасности, в том числе требованиях к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств морского и речного транспорта»

Постановление Правительства Российской Федерации от 19.10.2017 № 1273 «Об утверждении требований к антитеррористической защищенности торговых объектов (территорий) и формы паспорта безопасности торгового объекта (территории)»

Постановление Правительства РФ от 2 августа 2019 г. N 1006 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)"

Постановление Правительства РФ от 7 ноября 2019 г. N 1421 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования Российской Федерации и подведомственных ему организаций, объектов (территорий), относящихся к сфере деятельности Министерства науки и высшего образования Российской Федерации, формы паспорта безопасности этих объектов (территорий) и признании утратившими силу некоторых актов Правительства Российской Федерации" (с изменениями и дополнениями)

Указ Президента РФ от 02.09.2012 N 1258 Об утверждении состава Национального антитеррористического комитета по должностям

Указ Президента РФ от 11.08.2003 N 960 Вопросы Федеральной службы безопасности Российской Федерации

Указ Президента РФ от 15.02.2006 N 116 О мерах по противодействию терроризму вместе с Положением о Национальном антитеррористическом комитете

Указ Президента РФ от 15.05.2018 N 215 О структуре федеральных органов исполнительной власти

Указ Президента РФ от 17.06.2003 N 680 О центральных компетентных органах Российской Федерации, ответственных за выполнение Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом

Указ Президента РФ от 26.12.2015 N 664 О мерах по совершенствованию государственного управления в области противодействия терроризму вместе с Положением о Национальном антитеррористическом комитете

Указ Президента РФ от 31.12.2015 N 683 О Стратегии национальной безопасности Российской Федерации

Указ Президента РФ от 14.06.2012 N 851 О порядке установления уровней террористической опасности, предусматривающих принятие дополнительных мер по обеспечению безопасности личности, общества и государства

Указ Президента РФ от 28.10.2014 N 693 Об осуществлении контроля за обеспечением безопасности объектов топливно-энергетического комплекса

Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019 – 2023 годы

Концепция противодействия терроризму в Российской Федерации (утв. Президентом РФ 5 октября 2009 г.)

## ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

### 1. Формы аттестации

Итоговая аттестация проводится в форме тестирования. Тест состоит из 20 вопросов, ответить на которые необходимо в течение 40 минут. На прохождение теста отводится три попытки. Результаты теста контролирует преподаватель-тьютор, назначенный организатором обучения.

К итоговой аттестации допускаются слушатели, освоившие учебный план в полном объеме.

Результаты тестирования рассматриваются комиссией в составе 3 человек путем объективной и независимой оценки качества подготовки слушателей. По результатам рассмотрения комиссия принимает решение об успешном завершении слушателем обучения.

### 2. Оценочные материалы

#### 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 какому 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 вышеперечисленное
- 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

**15. 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

**16. 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

**17. 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

**18. 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

**19. 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

**20. 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

### **21. 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

### **22. 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, невозполнимый 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

### **23. 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

### **24. 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

### **25. Какой пометкой маркируют документы с ограниченным доступом?**

А) только для персонала

Б) конфиденциально

В) для служебного пользования

**26. 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

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

- А) можно
- Б) нельзя
- В) только по защищенным каналам связи

**28. 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

**29. 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

**30. 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

**31. 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

**32. 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

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

- А) приказ
- Б) рапорт
- В) акт

**34. Кем осуществляется проставление пометки «Для служебного пользования»?**

- А) руководителем организации

- Б) специалистом службы корпоративной защиты
- В) исполнителем документа или должностным лицом, подписывающим или утверждающим лот документ. исходя из его содержания

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

- А) исполнителем документа
- Б) сотрудником подразделения делопроизводства
- В) административно-хозяйственной службой

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

- А) перечень адресатов
- Б) указатель рассылки
- В) список получателей

**37. 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

**38. 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

**39. 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

**40. 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

**41. 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

**42. 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

**43. 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

**44. 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

**45. 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

**46. 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

**47. 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

**48. 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

**49. 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

**50. 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

**51. 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

**52. 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

**53. 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

**54. 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

55. Владелец 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 доступа 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

**55. 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

**56. 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

**57. 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

**58. 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

**59. 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.)

**60. 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.)

**61. 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.)

**62. Что из перечисленного относится к естественным угрозам информационной безопасности?**

- А) катаклизмы, независимые от человека: пожары, ураганы, наводнение, удары молнии
- Б) хакерские атаки, противоправные действия конкурентов, месть сотрудников
- В) компьютерные вирусы

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

- А) катаклизмы, независимые от человека: пожары, ураганы, наводнение, удары молнии
- Б) хакерские атаки, противоправные действия конкурентов, месть сотрудников
- В) ошибки, которые совершаются людьми по неосторожности или незнанию

**64. 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

**65. Какие виды угроз информационной безопасности наиболее опасны?**

- А) преднамеренные угрозы

- Б) естественные угрозы
- В) искусственные угрозы

**66. 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

**67. 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

**68. 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

**69. 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

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

- А) организационно-правовые
- Б) программные
- В) нормативно-правовые

**71. 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

**72. 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

**73. 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