Общество с ограниченной ответственностью
«Информационно – консультационный учебный центр
дополнительного профессионального образования
«Профстандарт»
(ООО «ИКУЦ ДПО «Профстандарт»)

УТВЕРЖДАЮ:

Директор ООО «ИКУЦ ДПО «Профстандарт»
_____ А.Ю. Шульженко
"___" _____ 2021 г.

Приказ № _____ от _____

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПО ТЕМЕ

«Работа с документами, содержащими служебную информацию ограниченного распространения»

СОГЛАСОВАНО
Зам. директора по учебно-методической работе
_____Евстифеев Р.И.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0161CBC0001CAFCEAC4D9FE835607CA475
Владелец: ШУЛЬЖЕНКО АНЖЕЛИКА ЮРЬЕВНА
Действителен: с 26.09.2022 до 26.12.2023

Мурманск
2021

План дополнительной профессиональной программы

1. **Цель изучения программы, организационно-педагогические условия ее реализации**
2. **Планируемые результаты обучения**
3. **Учебный план**
4. **Рабочая программа**
5. **Глоссарий**
6. **Литература**
7. **Итоговые тесты по программе «Работа с документами, содержащими служебную информацию ограниченного распространения»**

1. Цель изучения программы, организационно-педагогические условия ее реализации

Цель изучения программы «Работа с документами, содержащими служебную информацию ограниченного распространения»**:**
- изучение систем документации; рассмотрение системы защиты служебной и конфиденциальной информации, обеспечения открытого доступа граждан к информации в соответствии с положениями законодательства в органах власти и организациях.

Организационно-педагогические условия

Категория слушателей: специалисты со средним профессиональным образованием или с высшим образованием.

Срок обучения: 72 часа

Форма обучения: определяется совместно с образовательной организацией и Заказчиком (без отрыва от производства, с частичным отрывом от производства, то есть – очно-заочная форма, с применением дистанционных образовательных технологий)

Режим занятий: определяется совместно с Заказчиком (не менее 4 часов в день)

Календарный учебный график: составляется по мере набора учебных групп

Контроль проверки знаний: итоговый тест

Условия реализации педагогического процесса:
Образовательный процесс осуществляется на основе учебного плана, разработанного в соответствии с действующим законодательством. Обучение проходит очно – заочно, с использованием дистанционных образовательных технологий.
Разделы программы изложены в учебном плане. Объем разделов программы и их расположение связаны не только с действующими нормами и правилами, но и с необходимостью системного охвата изучаемых вопросов.

2. Планируемые результаты обучения по дополнительной профессиональной программе

Процесс обучения проводится очно-заочно, с применением дистанционных образовательных технологий, организовывается работа с методическими и справочными материалами, с применением технических средств обучения.

В результате освоения данной дополнительной профессиональной программы слушатель **должен знать:**

- основы законодательства в области работы с документами, содержащими служебную информацию ограниченного распространения;
- общие понятия и определения, используемые в вышеуказанной сфере;
- пути предупреждения правонарушений в области работы с документами, содержащими служебную информацию ограниченного распространения;
- вопросы, связанные с неотвратимостью ответственности за совершение правонарушений в области работы с документами, содержащими служебную информацию ограниченного распространения;

Слушатель должен **иметь навыки:**

- применения и работы с документами, содержащими служебную информацию ограниченного распространения;
- контролировать выполнение требований законодательства в области работы с документами, содержащими служебную информацию ограниченного распространения.

По результатам обучения окончившему курсы специалисту выдается удостоверение установленного образца, со сроком действия 5 лет.

3. Учебный план

Модуль	Наименование разделов и дисциплин	Всего ак. час
1.	**Понятия, признаки. Нормативно-правовая база работы с документами ограниченного доступа и работа с ней**	**12**
2.	**Основы информационной безопасности и защиты информации**	**12**
3.	**Порядок обращения с документами, содержащими служебную информацию**	**12**
4.	**Регистрация документов. Контроль исполнения документов**	**12**
5.	**Формирование и хранение дел в делопроизводстве. Организация архивного хранения документов**	**12**
6.	**Служебная тайна и её охрана. Юридическая ответственность за разглашение коммерческой тайны**	**10**
7.	**Итоговая аттестация (зачет)**	**2**
	ИТОГО	**72**

4. Рабочая программа
курса повышения квалификации в объеме 72 академических часов по теме **«Работа с документами, содержащими служебную информацию ограниченного распространения)»**

Модуль 1. Понятия, признаки. Нормативно-правовая база работы с документами ограниченного доступа и работа с ней

Содержание: Словарь терминов. Нормативно-правовые акты. Понятия «конфиденциально» и «для служебного пользования».

Модуль 2. Основы информационной безопасности и защиты информации

Содержание: Система информационной безопасности. Объекты защиты в концепциях ИБ. Категории и носители информации. Средства защиты информации. Способы передачи конфиденциальной информации на расстоянии.

Модуль 3. Порядок обращения с документами, содержащими служебную информацию

Содержание: Гриф ограничения доступа. Правила работы с документами ограниченного доступа. Разработка Положения о порядке работы со служебной информацией ограниченного распространения**.** Шаблоны документов по защите служебной информации.

Модуль 4. Регистрация документов. Контроль исполнения документов

Содержание: Прием, учет (регистрация) документов, содержащих информацию ограниченного распространения. Пошаговая регистрация входящего документа: бумажный носитель, электронный документ. Обучение должностных лиц.

Модуль 5. Формирование и хранение дел в делопроизводстве. Организация архивного хранения документов

Содержание: Особенности работы, оформление, хранение. Уничтожение дел, документов, изданий, содержащих служебную информацию ограниченного распространения.

Модуль 6. Служебная тайна и её охрана. Юридическая ответственность за разглашение коммерческой тайны

Содержание: Служебная тайна как объект права. Защита служебной тайны. Разглашение коммерческой тайны. Акт о разглашении охраняемой законом тайны. Порядок действий при разглашении работником тайны. Ответственность за разглашение коммерческой тайны. Особенности проведения служебного расследования по фактам утраты конфиденциальных документов. Образцы документов.

Итоговая аттестация - экзамен (тестирование)

5. Глоссарий

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

База персональных данных – именуемая совокупность упорядоченных персональных данных в электронной форме и/или в форме картотек персональных данных.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Владелец баз персональных данных – государственный орган, орган местного самоуправления, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Гриф «для служебного пользования» — особая пометка на документах, а также папках в которых они могут храниться, проставляемая на всех листах и приложениях, которые относятся к отдельному документу. Наличие данного грифа строго ограничивает круг лиц, которые могут получить доступ к этой документации. В частности, на документы, имеющие определенный гриф секретности, не распространяются нормативы законодательства, касающиеся возможности беспрепятственного доступа к информации.

Доступ в операционную среду компьютера (информационную систему персональных данных) – получение возможности запуска на выполнение штатных

команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация (в области обработки информации) – любые данные, представленные в электронной форме, написанные на бумаге, высказанные на совещании или находящиеся на любом другом носителе, используемые финансовым учреждением для принятия решений, перемещения денежных средств, установления ставок, предоставления ссуд, обработки операций и т.п., включая компоненты программного обеспечения системы обработки.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная угроза – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не

допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – любое действие или совокупность действий, совершенных полностью или частично в информационной (автоматизированной) системе и/или в картотеках персональных данных, которые связаны со сбором, регистрацией, накоплением, сбериганием, адаптацией, изменением, обновлением, использованием и распространением (реализацией, передачей), обезличивание, уничтожением ведомостей о физическом лице.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в т.ч. его фамилия, имя, отчество; год, месяц, дата и место рождения; адрес, семейное, социальное, имущественное положение, образование, профессия, доходы; др. информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Служебная информация ограниченного распространения – это несекретная информация, затрагивающая деятельность организации, ограничение на распространение которой определено требованиями обеспечения антитеррористической защищенности объекта.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе

персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

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

6. Список литературы

1. Указ Президента РФ от 30.11.1995 N 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне".
2. Федеральный закон от 06.03.2006 N 35-ФЗ (ред. от 08.12.2020). "О противодействии терроризму".
3. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 09.03.2021) "О коммерческой тайне".
4. Федеральный закон от 22 октября 2004 г. N 125-ФЗ "Об архивном деле в Российской Федерации".
5. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) "О персональных данных".
7. ГОСТ Р 7.0.8-2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело».
8. Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне".
9. Постановление Правительства РФ от 2 августа 2019 г. № 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)".
10. Постановление 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" (с изменениями и дополнениями).
11. 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".
12. Постановление Правительства Российской Федерации от 25.03.2015 № 272 "Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)".
13. Приказ Федеральной службы государственной статистики от 31 января 2011 г. N 24 "Об утверждении Инструкции о порядке учёта, обращения и хранения документов и других материальных носителей информации, содержащих служебную информацию ограниченного распространения" (с изменениями и дополнениями).
14. Распоряжением Правительства Мурманской области от 20.12.2012 № 438-РП. Инструкция по делопроизводству в исполнительных органах государственной власти мурманской области. Мурманск 2012 г.

15. Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера».
16. М. В. Кирсанова, С. П. Кобук, Ю. М. Аксёнов «Делопроизводство в органах власти и местного самоуправления».
17. Л. А. Румынова «Документационное обеспечение управления».
18. Хитарова И. Ю. Методика включения музея в систему информационной безопасности социально-культурной сферы.
19. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. Пособие. – М.: ИНФРА-М, 2001. – 304с.
20. Глухов Н.И. Коммерческая тайна предприятия и технология ее защиты: Учебно-методическое пособие. – Иркутск: ГУ НЦ РВХ ВСНЦ СО РАМН, 2005. – 204 с.
21. Вострецова Е.Н. Основы информационной безопасности: Изд-во Уральского ун-та. – 2019. – 208с.
22. Алексенцев А. И. Конфиденциальное делопроизводство. М.: Управление персоналом, 2003.
23. Демушкин А. С. Документы и тайна. М.: Городец, 2003. - 400 с.

Документация в информационном обществе: законодательство и стандарты: доклады и сообщения на XII Международной научно-практической конференции 22-23 ноября 2005 г. Росархив. ВНИИДАД. - М., 2006.

7.Итоговый тест

Вопрос 1

Информация – это

а) Любые данные, представленные на материальном носителе;

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

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

Вопрос 2

Информационная система персональных данных – это

а) Пользователь, средства автоматизации, базы данных;

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

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

Вопрос 3

Безопасность персональных данных – это

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

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

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

Вопрос 4

Доступ к информации – это

а) Возможность получения информации и ее использования;

б) Возможность использования информации;

в) Возможность доступа к информации;

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

Вопрос 5

Целью Федерального закона от 27.07.2006 № 152-ФЗ является:

а) Контроль за обработкой персональных данных операторами персональных данных;

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

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

Вопрос 6

Защищаемая информация – это

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

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

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

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

Вопрос 7

Что понимается под понятием «Конфиденциальность персональных данных»?

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

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

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

Вопрос 8

Общедоступные персональные данные – это

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

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

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

Вопрос 9

Целостность информации – это

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

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

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

Вопрос 10

Должна ли предусматривать разрешительная система доступ к конфиденциальной информации должностных лиц из внешних организаций, выполняющих совместную работу с организацией где введен режим конфиденциальности?

а) нет, не должна

б) да, должна

в) зависит от индивидуального решения руководителя, даже если это ставит под угрозу срыва выполнение совместных работ

Вопрос 11

Почему на пакетах (конвертах) с конфиденциальными документами не проставляют гриф конфиденциальности?

а) гриф проставляют всегда

б) чтобы не привлекать внимания

в) т.к. это не имеет никакого значения, важно лишь содержание конверта

Вопрос 12

Что делать с ошибочно присланными конфиденциальными документами?

а) их нужно выбросить

б) их нужно отправить обратно

в) по согласованию с отправителем переслать в нужный адрес

Вопрос 13

Стоит ли принимать надорванный пакет (конверт) с конфиденциальными документами, если он адресован в вашу организацию?