Автономная некоммерческая организация
Дополнительного профессионального образования
«СофтЛайн Эдюкейшн»

УТВЕРЖДАЮ:
Генеральный директор
АНО ДПО «СофтЛайн Эдюкейшн»
_____ И.В. Кривенкова
«__» _____ 20__г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАМА - ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Наименование программы: Современные требования законодательства к обработке и защите персональных данных

Категория слушателей: Инженеры по защите информации, специалисты I и II категорий по защите информации, специалисты других отделов компаний, желающие приобрести знания и навыки по обработке и обеспечению персональных данных.

Уровень квалификации: не ниже 6

Объем: 16 часов

Форма обучения: очная или очная с использованием дистанционных образовательных технологий

г. Москва, 2017 г.

Разработчик:

Мышерин Александр Владиславич – преподаватель, сертифицированный специалист: Код Безопасности (Secret Net, vGate)

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Нормативно-правовые основания разработки программы

Нормативную правовую основу разработки программы составляют:

Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

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

Приказ Министерством труда и социальной защиты Российской Федерации от 12 апреля 2013 г. № 148н «О утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов»;

Приказ Министерства образования и науки Российской Федерации от 09 января 2014 г. № 2 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

Постановление Правительства Российской Федерации от 6 мая 2008 года №362 «Об утверждении государственных требований к профессиональной подготовке и повышению квалификации государственных гражданских служащих Российской Федерации»

Программа разработана на основе профессионального стандарта:
«Специалист по защите информации в автоматизированных системах» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15.09.2016 г. № 522н, регистрационный номер 843).

1.2. Область применения программы

Настоящая программа предназначена для подготовки специалистов, желающих приобрести дополнительные навыки по обработке и обеспечению безопасности персональных данных.

1.3. Требования к слушателям (категории слушателей)

Для успешного прохождения программы слушатели должны:

- обладать знаниями основ информационных технологий;

- уметь работать с нормативно-правовыми актами.

1.4. Цель и планируемые результаты освоения программы

Программа направлена на освоение (совершенствование) следующих профессиональных компетенций:

ПК 1. Разработка организационно-распорядительных документов по защите персональных данных в автоматизированных системах
ПК 2. Внедрение организационных мер по защите персональных данных в автоматизированных системах
ПК 3. Обоснование необходимости защиты персональных данных в автоматизированной системе
ПК 4. Определение угроз безопасности персональных данных, обрабатываемых автоматизированной системой.

Обучающийся в результате освоения программы должен
иметь практический опыт:

- определения комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты персональных данных в автоматизированных систем;

- разработки модели угроз безопасности персональных данных автоматизированной системы;

- определения структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты персональных данных;

- анализа характера обрабатываемой информации и определение перечня информации, подлежащей защите;

- подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты персональных данных в информационной системе в ходе ее эксплуатации;

- определения правил и процедур выявления инцидентов и реагирования на них

уметь:

- классифицировать и оценивать угрозы информационной безопасности;

- контролировать эффективность принятых мер по защите персональных данных в автоматизированных системах;

- реализовывать правила разграничения доступа персонала к объектам доступа;

- анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами;

- организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем;

- использовать рисковую методологию управления защитой персональных данных в автоматизированной системе;

- формировать перечень мероприятий по предотвращению угроз безопасности персональных данных автоматизированной системы;

- анализировать и выявлять уязвимости информационных систем;

- разрабатывать проекты нормативных документов, регламентирующих работу по защите персональных данных в автоматизированных системах;

знать:

- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты персональных данных;

- основные угрозы безопасности персональных данных и модели нарушителя в автоматизированных системах;

- нормативные правовые акты в области защиты персональных данных;

- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите персональных данных;

- нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты персональных данных;

- методы защиты персональных данных от утечки по техническим каналам;

- принципы формирования политики информационной безопасности в автоматизированных системах;

- основные информационные технологии, используемые в автоматизированных системах.

1.5. Форма обучения – очная или очная с использованием дистанционных образовательных технологий.
Режим занятий: 8 ч. в день, 2 дня.
1.6. Форма документа, выдаваемого по результатам освоения программы - удостоверение о повышении квалификации установленного образца.

2. УЧЕБНЫЙ ПЛАН

Наименование раздела, модулей	Общая трудоемкость, час.	Аудиторные занятия с использованием или без использования дистанционных образовательных технологий, час.				СРС, час.	Текущий контроль (при наличии)		Промежуточный контроль*		
		Всего, час.	из них, час				ПР	Лаб. Р	Экз.	Зачет	Тест
			лекции	лаб. работы	семинары						
1	2	3	4	5	6	7	8	9	10	11	12
Модуль 1 Информация и информационная безопасность.	2	2	1		1		1				
Модуль 2. Основные положения закона о персональных данных.	4	4	1		3		3				
Модуль 3. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.	5	5	1		4		4				
Модуль 4. Реализация требований ФЗ "О персональных данных" в рамках предприятия.	4	4	1		3		3				
Итоговая аттестация	1										1 (Э)
Итого	16	15	4		11						1

Примечание –
В столбцах 2 – 7 указывается количество часов, в столбцах 8 – 12 указывается количество работ, тестов и т.п.
При отсутствии СРС, текущего контроля, промежуточной аттестации графы 7 - 9 исключить.
* В соответствующей графе указывается количество и технология приема:
«Т» - прием, осуществляемый по традиционной образовательной технологии;
«Э» - прием, осуществляемый с использованием технологий электронного обучения;
«Д» - прием, осуществляемый с использованием дистанционных образовательных технологий.

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Наименование раздела, модуля	*1 день*	*2 день*
Модуль 1 «Информация и информационная безопасность»	*Лекция №1 – 1 час;* *семинар №1 – 1 час*	
Модуль 2 «Основные положения закона о персональных данных»	*Лекция №2 – 1 час;* *семинар №2 – 1 час;* *семинар №3 – 1 час;* *семинар №4 – 1 час*	
Модуль 3 «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»	*Лекция №3 – 1 час;* *семинар №5 – 1 час*	*Семинар №6 – 1 час;* *семинар №7 – 1 час;* *семинар №8 – 1 час*
Модуль 4 «Реализация требования ФЗ «О персональных данных» в рамках предприятия»		*Лекция №1 – 1 час;* *семинар №9 – 1 час;* *семинар №10 – 1 час;* *семинар №11 – 1 час*
Итоговая аттестация		*Тест 1 час*

4. ПРОГРАММЫ УЧЕБНЫХ МОДУЛЕЙ

Наименование модулей или тем программы	Содержание учебного материала, практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся		Кол-во акад. часов
1	*2*		*3*
Модуль 1 «Информация и информационная безопасность»	**Содержание:**	**Уровень освоения**	2
	1. Понятие информационной безопасности и безопасности информации	1	
	2. Актуальность обеспечения информационной безопасности	2	
	3. Угрозы информационной безопасности	2	
	4. Основные направления обеспечения информационной безопасности	2	
	5. Основные понятия в области безопасности информационных технологий	1	
	6. Законодательные акты в области информационной безопасности	2	
	Тематика учебных занятий		
	Лекция 1 «Термины и определения»		1
	Семинар 1 «Анализ информационных отношений. Работа с угрозами»		1
Модуль 2 «Основные положения закона о персональных данных»	**Содержание:**	**Уровень освоения**	4
	1. Основы обработки персональных данных в организации по 153-ФЗ: сбор, запись, систематизация, накопление, хранение, уточнение, извлечение, использование, передача, обезличивание, блокирование, удаление, уничтожение	1	
	2. Общедоступные, подлежащие опубликованию или обязательному раскрытию персональные данные	1	
	3. Права субъектов персональных данных и их соблюдение при обработке	2	
	4. Разъяснения по вопросам получения согласия на обработку персональных данных	2	
	5. Основные обязанности оператора персональных данных	2	
	6. Система государственных контрольно-надзорных органов РФ, контролирующих вопросы безопасности персональных данных в организации	2	
	Тематика учебных занятий		
	Лекция 2 «Основы обработки персональных данных»		1
	Семинар 2 «Разбор прав субъектов персональных данных»		1

	Семинар 3 «Анализ обязанностей оператора персональных данных»		1
	Семинар 4 «Контроль и надзор за обработкой персональных данных, подготовка нормативных документов»		1
Модуль 3 «Обеспечение безопасности персональных данных»	**Содержание:**	**Уровень освоения**	5
	1. Разработка политики оператора персональных данных	2	
	2. Общие требования по обеспечению безопасности персональных данных	1	
	3. Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями. Контроля за его соблюдением.	1	
	4. Процедура работы с уведомлением об обработке персональных данных	2	
	5. Виды гражданской, административной и уголовной ответственности за нарушение законодательства в сфере персональных данных. Краткий обзор.	2	
	Тематика учебных занятий		
	Лекция 3 «Подзаконные акты в области обработки персональных данных»		1
	Семинар 5 «Неавтоматизированная обработка, обработка специальных категорий персональных данных»		1
	Семинар 6 «Правила работы с документами Роскомнадзора»		1
	Семинар 7 «Анализ приказов и методических документов ФСТЭК и ФСБ»		1
	Семинар 8 «Виды гражданской, административной и уголовной ответственности при выявлении инцидентов»		1
Модуль 4 «реализация требований ФЗ «О персональных данных» в рамках предприятия»	**Содержание:**	**Уровень освоения**	4
	1. Основные локальные акты по вопросам обработки персональных данных, установленные в соответствии с законодательством РФ	1	
	2. Локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений, их содержание	1	
	3. Порядок разработки и ввода в действие основных локальных актов, регламентирующих безопасность персональных данных в организации	1	
	4. Особенности разработки и внедрения локальным нормативных актов по БПД в государственных и муниципальных учреждениях.	2	
	5. Общий порядок планирования и организации плановых и внеплановых проверок контролирующих органов.	2	

	6.Порядок работы с заявлениями граждан, связанных с нарушением их прав в сфере БПД.	2	
	7. Рекомендации по прохождению проверок контролирующими органами. Порядок судебного и внесудебного обжалования итогов проверок. Обзор актуальной судебной практики.	2	
	8. Меры, принимаемые контролирующими органами в случае выявления нарушений в сфере БПД в организации.	2	
	Тематика учебных занятий		
	Лекция 4 «Основные локальные акты по вопросам обработки персональных данных»		1
	Семинар 9 «Разработка модели угроз и классификация информационной системы персональных данных»		1
	Семинар 10 «Разработка мероприятий по обеспечению безопасности персональных данных»		1
	Семинар 11 «Анализ действий при прохождении проверок контролирующими органами»		1

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

5. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

5.1. Материально-техническое обеспечение

Реализация программы предполагает для проведения лекций, семинаров и тестирования наличие аудитории, оснащенной специализированным оборудованием.

Для показа презентаций во время лекций и семинаров требуется проекционное оборудование (разрешение 1024 х 768 или выше);

Для проведения итогового тестирования компьютерный класс должен быть оснащен следующим оборудованием:

- доступ в Интернет с гарантированной полосой пропускания минимум 250 кбит/с;
- персональный компьютер.

Реализация программы в очном формате с применением дистанционных образовательных технологий предполагает проведение занятий с использованием системы дистанционного обучения.

5.2. Информационное обеспечение обучения

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".
3. Федеральный закон от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности".
4. Федеральный закон от 27.12.2002 № 184-ФЗ "О техническом регулировании".
5. Указ Президента Российской Федерации от 16.08.2004 № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю".
6. Перечень сведений конфиденциального характера. Утверждён Указом Президента Российской Федерации от 06.03.1997 № 188.
7. Постановление правительства РФ «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 года № 687
8. Постановление Правительства РФ от 6.07.2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"
9. Постановление правительства РФ от 21.03.2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных"
10. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
11. Постановление Правительства РФ от 16.04.2012 № 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных

систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) ".
12. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
13. Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
14. Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 г. N 378 г. "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".
15. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России, 1992.
16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30.08.2002 № 282.
17. Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом Гостехкомиссии России от 27.10.1995 № 199.
18. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждён решением председателя Гостехкомиссии России от 30.03.1992.
19. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждён решением председателя Гостехкомиссии России от 30.03.1992.
20. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Утверждён решением председателя Гостехкомиссии России от 25.07.1997.
21. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Утверждён решением председателя Гостехкомиссии России от 25.07.1997.
22. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждён приказом председателя Гостехкомиссии России от 04.06.1999 № 114.

Дополнительные источники:

1. *Внуков, А. А.* Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9.
2. *Внуков, А. А.* Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6.

3. Нестеров С.А. Основы информационной безопасности: Учебное пособие. Учебник для вузов. СПБ.:ЛАНЬ, 2016, 324 с. ISBN: 978-5-8114-2290-6.
4. *Нестеров, С. А.* Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4.
5. Ерохин В.В, Погонышева Д.А., Степченко И.Г. Безопасность информационных систем. Учебное пособие, Флинта, 2015, 184 с. ISBN 978-5-9765-1904-6.
6. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8.
7. Зайцев А. П., Мещеряков Р. В., Шелупанов А. А. Технические средства и методы защиты информации. Учебник для вузов. 7-е изд. испр., - М: Горячая линия - Телеком, 2015, 442 с. ISBN: 978-5-9912-0233-6
8. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности: Учебное пособие. - СПБ.:ПИТЕР, 2016, 256 с. ISBN: 978-5-496-02434-1
9. Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Защита персональных данных: Учебное пособие - СПб.: НИУ ИТМО, 2013
10. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности: Учебное пособие. - СПб.: НИУ ИТМО, 2013
11. Федеральный закон «О персональных данных»: научно-практический комментарий. Под редакцией заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. - М.: Редакция «Российской газеты», 2015. Вып. 11. — 176 с.

5.3. Организация образовательного процесса

Реализация программы предполагает сочетание лекционных занятий и семинаров.

В начале изучения каждого модуля проводятся лекции, которые позволяют слушателям получить информацию и определить подходы к решению задач, предусмотренных семинарами. Лекции в полном объеме могут проводиться очно или с использованием дистанционных образовательных технологий. Семинарские занятия проводятся в форме разбора примеров из практики, решения кейсов, проблемных ситуаций, разработки нормативных документов, обсуждения актуальных вопросов по тематике программы.

5.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров: высшее образование, опыт работы в области обеспечения информационной безопасности.

6. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ КУРСА

Формы итоговой аттестации.
Электронное тестирование.
Общая характеристика итоговой аттестации.
К итоговой аттестации допускаются слушатели, выполнившие все задания семинаров, предусмотренные учебной программой. В ходе электронного тестирования слушателю предлагается ответить на 20 вопросов. Тест считается пройденным при результате: 14 правильных ответов.

Результаты (освоенные профессиональные и общие компетенции)	Основные показатели оценки результата
ПК 1. Управление защитой персональных данных в автоматизированных системах; ПК 2. Разработка архитектуры системы защиты персональных данных в автоматизированной системе; ПК 3. Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов; ПК 4. Проведение сертификационных испытаний на соответствие требованиям по безопасности информации программных (программно-технических) средств защиты персональных данных от несанкционированного доступа; ПК 5. Создание системы защиты персональных данных в организации.	Показатели качества текущих семинаров (экспертная оценка): - корректное определение правил и процедур выявления инцидентов - грамотная разработка проектов нормативных документов, регламентирующих работу по защите персональных данных - разработка комплекса мер для защиты персональных данных в автоматизированных системах - определение эффективности принятых мер по защите персональных данных - правильное использование рисковой методологии управления защитой персональных данных - разработка моделей угроз безопасности персональных данных Показатели качества итогового электронного тестирования: - точные ответы на вопросы итогового тестирования