Негосударственное образовательное учреждение дополнительного профессионального образования «ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»

УТВЕРЖДАЮ
Директор НОУ ДПО "ЦПР"
В.Г.Казанцев
"25" мая 2015 года

Программа повышения квалификации

«Обеспечение безопасности персональных данных на предприятии»

г. Санкт-Петербург
2015 год

Программа обсуждена и одобрена на заседании учебно-методического совета НОУ ДПО «ЦПР»
Протокол №23 от 25 июня 2015 года.

Секретарь _____ М.В.Бочков

Дополнительная профессиональная образовательная программа повышения квалификации **«Обеспечение безопасности персональных данных на предприятии»** (далее – Программа) разработана авторским коллективом НОУ ДПО «ЦПР» в соответствии с Федеральным законом Российской Федерации от 29.12.2012 г. № 273-ФЗ "Об образовании в Российской Федерации"; Приказом Минобрнауки РФ № 499 от 1 июля 2013 г. «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам». При разработке содержания настоящей дополнительной профессиональной образовательной Программы учтены требования обеспечения преемственности по отношению к федеральным государственным образовательным стандартам высшего образования (ФГОС ВПО) по направлению подготовки "Информационная безопасность", а также имеющиеся на момент формирования Программы требования профессиональных стандартов и (или) квалификационные требования, указанные в квалификационных справочниках, утверждаемых в порядке, устанавливаемом Правительством Российской Федерации, по соответствующим должностям, профессиям, специальностям (в соответствии с Общероссийским классификатором специальностей).

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель Программы

Программа предназначена для повышения квалификации:

- руководителей организаций и их структурных подразделений, в ведении которых находится обработка персональных данных;
- руководителей и специалистов, отвечающих за обеспечение информационной безопасности предприятий;
- работников кадровых органов;
- юристов предприятий-операторов персональных данных;
- специалистов, реализующих мероприятия по технической защите конфиденциальной информации.

Целью реализации Программы является совершенствование профессиональных компетенций, повышение профессионального уровня обучающихся в рамках имеющейся квалификации в условиях изменения целей, содержания, технологий, нормативно-правового обеспечения профессиональной деятельности в сфере информационной безопасности.

В процессе обучения рассматриваются цели и задачи правовых, организационных и технических аспектов обеспечения безопасности персональных данных.
Особое внимание уделено изучению требований руководящих документов ФСБ и ФСЭК РФ по обеспечению безопасности персональных данных при их обработке в информационных системах, а также работы по созданию и обеспечению функционирования системы защиты персональных данных на предприятии.

Учебная Программа **«Обеспечение безопасности персональных данных на предприятии»** рекомендована в качестве вариативного раздела (модуля) программы профессиональной переподготовки «**Комплексное обеспечение безопасности предприятия**» со специализацией «Организация защиты информации на предприятии».

Специфика Программы заключается в ее прагматической направленности. Программа повышения квалификации призвана ликвидировать разрыв между требуемыми актуальными и существующими компетенциями слушателей, который не может быть преодолен средствами самообразования и самоподготовки на рабочем месте. Этот факт определяет требования к конечным результатам обучения по Программе: формирование профессиональных компетенций работника, позволяющие ему выполнять свои трудовые функции в рамках актуальных требований к его профессиональной деятельности.

Программа характеризуется практической ориентированностью обучения, с опорой на имеющийся у слушателей трудовой опыт, высокую долю самостоятельной работы, прикладной характер содержания образования.

1.2. Характеристика подготовки по Программе

Нормативный срок освоения Программы – 40 академических часов, 5 рабочих дней, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.
Режим обучения: 40 ак.часов аудиторных занятий в неделю (8 ак.часов в день) - лекции, семинары, практические занятия.
Форма обучения – очная, с отрывом от производства.

1.3. Требования к уровню подготовки слушателя

Повышение квалификации по настоящей Программе осуществляется на базе высшего и среднего профессионального образования.
К освоению данной дополнительной профессиональной Программы допускаются лица имеющие среднее профессиональное и (или) высшее образование.

Для успешного освоения Программы повышения квалификации обучающийся должен:

1. Знать и понимать:
   - место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
   - основные нормативные правовые акты в области информационной безопасности и защиты информации;
   - правовые основы организации защиты информации,
   - принципы и методы организационной защиты информации;

2. Уметь:
   - анализировать и оценивать угрозы информационной безопасности объекта;
   - пользоваться нормативными документами по защите информации;
   - использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности.

3. Владеть:
   - навыками работы с нормативными правовыми актами в сфере экономической и информационной безопасности;
   - навыками компьютерной обработки служебной документации, статистической информации и деловой графики; работы с информационно-поисковыми и информационно-справочными системами и базами данных, используемыми профессиональной деятельности;
   - навыками организации и обеспечения режима секретности;
   - навыками обоснования, выбора, реализации и контроля результатов управленческого решения.

1.4. Требования к результатам освоения Программы

Программа направлена на совершенствование и (или) освоение следующих профессиональных компетенций:

- способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-1);
- способность использовать нормативные правовые документы в своей профессиональной деятельности (ПК-2);
- способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-3);
- способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-4);
- способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-5);
- способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-6);
- способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-7);
- способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-8);
- способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-9);
- способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-10);
- способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-11);
- способность участвовать в работах по реализации политики информационной безопасности (ПК-12);
- способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-13);
- способность организовать работу малого коллектива исполнителей с учетом требований защиты информации (ПК-14);
- способность организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю (ПК-15).

В результате освоения Программы слушатель должен приобрести и (или) усовершенствовать следующие знания и умения, необходимые для качественного изменения компетенций:

- выявление потенциальных и реальных угроз информационной безопасности; умение проводить их ранжирование по вероятности реализации и величине ущерба;
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей с учетом требований защиты информации;
- совершенствование системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;
- контроль эффективности реализации политики информационной безопасности объекта.
- участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
- знание методов и средств выявления угроз безопасности автоматизированным системам;
- знание методов технической защиты информации;
- знание методов формирования требований по защите информации;
- знание методов организации и управления деятельностью служб защиты информации на предприятии;
- знание методик проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- изучение технических каналов утечки информации, возможностей технических разведок, способов и средств защиты информации от утечки по техническим каналам, методов и средств контроля эффективности технической защиты информации;
- изучение принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- изучение принципов организации информационных систем в соответствии с требованиями по защите информации.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

Учебный план
программы повышения квалификации
«Организация конфиденциального делопроизводства на предприятии»

Цель: повышение компетентности специалистов в области обеспечения безопасности персональных данных предприятия.

Категория слушателей: руководители организаций и их структурных подразделений, в ведении которых находится обработка персональных данных; руководители и специалисты, отвечающие за обеспечение информационной безопасности предприятий; работники кадровых органов; юристы предприятий - операторы персональных данных; специалисты, реализующие мероприятия по технической защите конфиденциальной информации.

Срок освоения: 40 часов, 5учебных дней

Режим занятий: 8 часов в день

№ п/п	Наименование учебных тем	Количество часов на курс подготовки			
		Всего	в том числе:		
			Лекции, семинары	Практические занятия	Формы контроля
1	**Общие положения по обеспечению безопасности персональных данных на предприятии**	4	4		
2	**Нормативная правовая база по обеспечению безопасности персональных данных**	6	6		
3	**Основные направления деятельности должностных лиц, отделов и служб предприятия по обеспечению безопасности персональных данных**	8	4	4	
4	**Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных**	6	4	2	
5	**Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации**	6	4	2	

6	**Методы и средства контроля безопасности персональных данных**	**2**	**2**		
7	**Практические рекомендации. Изучение, подбор и расстановка кадров, принимающих участие в обеспечении безопасности персональных данных**	**6**	**2**	**4**	
	Итоговая аттестация	**2**		**2**	**Зачет без оценки**
	Итого	**40**	**26**	**14**	

2.2. Содержание Программы

Учебная программа
повышения квалификации
«Организация конфиденциального делопроизводства на предприятии»

Тема 1. Общие положения.

Персональные данные, как составная часть информации ограниченного доступа на предприятии, категории персональных данных, права и обязанности граждан РФ в отношении своих персональных данных, базы персональных данных как объект интеллектуальной собственности предприятия, работа с персональными данными (принципы работы с персональными данными, условия работы с персональными данными, специальные категории персональных данных, биометрические персональные данные), угрозы безопасности и модель угроз безопасности персональных данных, государственная система защиты информации ограниченного доступа, обеспечение безопасности персональных данных — обязательная составляющая защиты на предприятии информации ограниченного доступа.

Тема 2. Нормативная правовая база по обеспечению безопасности персональных данных.

Нормативные правовые акты, нормативные и методические документы ФСТЭК и ФСБ России, регламентирующие обеспечение безопасности персональных данных, Гражданский и Трудовой кодексы РФ о порядке работы с персональными данными, основные положения Федерального Закона «О персональных данных», основные требования «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», введенного в действие Постановлением Правительства РФ № 687 от 15 сентября 2008 года, основные требования «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», введенного в действие Постановлением Правительства РФ № 781 от 17 ноября 2007 года, структура и содержание методических документов ФСТЭК России по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, ответственность за нарушение требований законодательства по обеспечению безопасности персональных данных.

Тема 3. Основные направления деятельности должностных лиц, отделов и служб предприятия по обеспечению безопасности персональных данных.

Структура, цели и задачи системы защиты информации ограниченного доступа на предприятии, основные документы предприятия по защите информации ограниченного доступа, правовое оформление работы с персональными данными в рамках трудовых отношений, правовое оформление работы с персональными данными в рамках гражданско-правовых отношений, подготовка объектов информатизации, на которых происходит обработка персональных данных, к проведению аттестации по требованиям безопасности информации, проведение на предприятии служебных расследований по фактам нарушений требований законодательства по обеспечению безопасности персональных данных и порядок обращения в суд по их результатам.

Тема 4. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

Основные мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, методика выявления актуальных угроз и формирование модели угроз безопасности персональных данных, обрабатываемых в информационных системах, организация работ по созданию

системы технической защиты персональных данных при их обработке в информационных системах, проведение спец.исследований и спец.проверок информационных систем персональных данных.

Тема 5. Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации.

Типовые формы кадрового учета и порядок их ведения, журналы учета персональных данных и порядок их ведения, порядок уничтожения материальных носителей с информацией о персональных данных граждан, порядок реализации мер по обеспечению безопасности персональных данных.

Тема 6. Методы и средства контроля безопасности персональных данных.

Организационный и технический контроль соблюдения требований законодательства по обеспечению безопасности персональных данных, надзор за соблюдением требований законодательства по обеспечению безопасности персональных данных.

Тема 7. Практические рекомендации. Изучение, подбор и расстановка кадров, принимающих участие в обеспечении безопасности персональных данных.

Совместная работа с предприятиями контрагентами в области обеспечения безопасности персональных данных, совместная работа с персоналом предприятия по обеспечению безопасности персональных данных, разработка организационно-распорядительных документов по технической защите персональных данных, выбор и применение аппаратно-программных средств, используемых в системах технической защиты персональных данных при их обработке в информационных системах (VPN, межсетевые экраны, средства обнаружения атак, сканеры уязвимости).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Обучение проводится на учебно-методической базе Негосударственного образовательного учреждения дополнительного профессионального образования «Центр предпринимательских рисков».

К преподаванию учебной Программы привлекаются преподаватели, имеющие большой опыт педагогической деятельности(более 5 лет) в сфере экономической безопасности и практический опыт работы по этой тематике.

В процессе обучения применяются современные технические средства обучения и методические пособия, разработанные по темам учебной Программы.

3.1. Требования к минимальному материально-техническому обеспечению

Реализация Программы дисциплины требует наличия учебного кабинета с необходимыми техническими средствами обучения.

Оборудование учебного кабинета:

- рабочие места по количеству обучающихся (стол, стул, необходимые для работы в аудитории канцелярские принадлежности);
- рабочее место преподавателя (стол, стул, необходимые для работы в аудитории канцелярские принадлежности);
- доска для записей с принадлежностями (маркеры для письма, указка).

Технические средства обучения:

- персональный компьютер преподавателя с периферийными устройствами и доступом к сети Интернет;
- мультимедиа-проектор с экраном;
- персональные компьютеры (ноутбуки) по количеству обучающихся с доступом к сети Интернет.

Каждый обучающийся обеспечивается раздаточным материалом и компакт-диском с записью учебно-методических материалов Программы (презентации преподавателей, конспекты, нормативно-правовые акты, образцырассматриваемых на занятиях документов, примеры решения практических задач, статьи и другие материалы по темам Программы).

3.2. Информационное обеспечение обучения

Перечень рекомендуемой литературы, Интернет-ресурсов

Законы и нормативные акты

Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (действующая редакция)

«Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09.09.2000 N Пр-1895) (действующая редакция)

Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) «О безопасности» (действующая редакция)

Закон РФ «О государственной тайне» от 21.07.1993г. №5485-1 (действующая редакция)

Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. N 98-ФЗ (действующая редакция)

Федеральный закон «О персональных данных» от 27 июля 2006 г. N 152-ФЗ (действующая редакция)

Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. N 63-ФЗ (действующая редакция)

Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375) (действующая редакция)

Учебная литература

Сердюк В.А. «Организация и технологии защиты информации» 2011г

Некраха А.В. «Организация конфиденциального делопроизводства и защита информации» учебное пособие. М. Академический проект, 2007

Зубов А.Ю «Криптографические методы защиты информации» Совершенные шифры: Учебное пособие. М. Гелиос АРВ, 2005

Волостных В.А., Киреев В.С., Стародубцев Ю.И «Основы защищенного делопроизводства» СПб. ВУС, 2002

Спивак В.А «Документирование управленческой деятельности (Делопроизводство)» – СПб. Питер, 2005

Гугуева Т. А «Конфиденциальное делопроизводство» учебное пособие. М. Альфа-М: ИНФРА-М, 2012

«Конфиденциальное делопроизводство и защищенный электронный документооборот»

Хореев П.Б. «Криптографические интерфейсы и их использование» М. Горячая линия Телеком, 2007

С.В. Запечников «Криптографические протоколы и их применение в финансовой и коммерческой деятельности» Учебное пособие для вузов. М. Горячая линия Телеком, 2007

Рекомендованные Интернет-ресурсы:

http://www.consultant.ru/Справочная правовая система «Консультант Плюс»

http://www.garant.ru/Справочная правовая система «Гарант»

http://www.s-director.ru/ Журнал«Директор по безопасности» специализированное ежемесячное издание, ориентированное на освещение полного комплекса проблем корпоративной безопасности: экономической, физической, технической, информационной, кадровой, юридической и т.п., а также их взаимного влияния

http://bezopasnost-chel.ru/ Всероссийский специализированный журнал «Безопасность» отраслевое издание на рынке систем безопасности в России и Ближнем Зарубежье

http://www.algoritm.org/Журнал «Алгоритм безопасности»– информационно-аналитическое издание, освещающее вопросы технического обеспечения безопасности объектов

http://www.tzmagazine.ru/ Журнал «Технология защиты» - отраслевое издание рынка технических систем безопасности. Всё о комплексных системах безопасности СКУД ОПС CCTV системах пожаротушения и о других сегментах рынка ТСБ

http://ru-bezh.ru/RUБЕЖ информационно-аналитический журнал по теме безопасности

http://www.mirbez.ru/ Специализированный журнал по безопасности «Мир и безопасность»

http://www.plusworld.ru/ Информационно-аналитический журнал ПЛАС

http://www.id-mb.ru/ Аналитический медиапортал «Мир безопасности»

http://tek.securitymedia.ru/ Отраслевой специализированный журнал «Безопасность объектов ТЭК»

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

По окончании обучения по Программе проводится итоговая аттестация в форме зачёта без оценки.

Примерные вопросы для подготовки к зачёту

1. Права и обязанности граждан РФ в отношении своих персональных данных.
2. Правовое оформление режима коммерческой тайны и работы с персональными данными в рамках трудовых отношений.
3. Коммерческая тайна и базы персональных данных как объекты интеллектуальной собственности предприятия.
4. Правовое оформление режима коммерческой тайны.работы с персональными данными в рамках гражданско-правовых отношений.
5. Работа с персональными данными в рамках гражданско-правовых отношений.
6. Режим защиты персональных данных на предприятии.
7. Обоснование системы технической защиты персональных данных на предприятии.
8. Базовые технологии и средства технической защиты персональных данных.
9. Применение криптографических сервисов для защиты персональных данных.
10. Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации.
11. Порядок проведения проверок территориальными подразделениями Роскомнадзора.
12. Разработка частных моделей угроз ИСПД.
13. Разработка требований безопасности к ИСПД и внедрение защитных мероприятий.
14. Оценка соответствия ИСПД требованиям безопасности.
15. Приведение эксплуатируемых информационных систем персональных данных в соответствие с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
16. Разработка организационно-распорядительных документов по защите персональных данных на предприятии.
17. Основные положения Федерального Закона «О персональных данных».
18. Основные требования «Положения об обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».
19. Структура методических документов ФСТЭК России по обеспечению безопасности персональных данных.
20. Угрозы безопасности персональным данным при их обработке в информационных системах персональных данных.
21. Модель угроз безопасности персональным данным. Методика выявления актуальных угроз безопасности персональным данным.

22. Формирование модели угроз безопасности персональным данным.
23. Организация работ по созданию системы технической защиты персональных данных при их обработке в информационных системах. Рекомендации по разработке организационно-распорядительных документов по технической защите персональных данных.
24. Выбор и применение аппаратно-программных средств, используемых в системах технической защиты персональных данных при их обработке в информационных системах.

УЧЕБНАЯ ПРОГРАММА
«Обеспечение безопасности персональных данных на предприятии»