Негосударственное образовательное учреждение
дополнительного профессионального образования
«ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»

УТВЕРЖДАЮ
Директор НОУ ДПО "ЦПР"
_____ В.Г.Казанцев
"23" января 2015 года

Программа повышения квалификации

«Организация технической защиты конфиденциальной информации»

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 **«Организация технической защиты конфиденциальной информации»** (далее – Программа) разработана авторским коллективом НОУ ДПО «ЦПР» в 2005 году и согласованна с Федеральной службой по техническому и экспортному контролю. Настоящая редакция Программы переработана и дополнена для приведения в соответствие 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 предприятий и организаций различных форм собственности,
- руководителей, начальников отделов и специалистов служб безопасности (информационной безопасности),
- руководителей и сотрудников отделов автоматизации, вычислительных центров, информационно-технических отделов,
- руководителей и сотрудников специализированных подразделений по защите конфиденциальной информации и по противодействию экономическому шпионажу,
- руководителей и сотрудников отделов автоматизации, вычислительных центров, информационно-технических отделов.

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.

Цели обучения:

- формирование у слушателей комплексного подхода к решению задач по организации и обеспечению защиты конфиденциальной информации;
- обновление и углубление теоретических и практических знаний, умений и навыков по защите конфиденциальной информации;
- освоение современных методов защиты конфиденциальной информации;
- теоретическая и практическая подготовка специалистов предприятий – соискателей лицензии на деятельность по технической защите конфиденциальной информации.

Программа предусматривает изучение правовых аспектов обеспечения безопасности конфиденциальной информации, определение целей и задач ее защиты, а также ознакомление с характеристиками угроз безопасности конфиденциальной информации и средствами по защите от них.

В соответствии с требованиями правовых, нормативно-методических и руководящих документов в процессе обучения рассматривается решение задач по следующим направлениям:

- оценка возможных угроз безопасности конфиденциальной информации;
- определение сведений, подлежащих защите;
- выявление и учет правовых и организационно-технических аспектов защиты конфиденциальной информации;
- выбор методов и средств защиты конфиденциальной информации и их

применение,

- оценка эффективности мер защиты конфиденциальной информации и их контроль.

Дополнительная профессиональная образовательная программа повышения квалификации «Организация технической защиты конфиденциальной информации» разработана авторским коллективом НОУ ДПО «ЦПР» в 2005 году и согласована с Федеральной службой по техническому и экспортному контролю. Содержание Программы ежегодно актуализируется в соответствии с изменениями в законодательстве по защите конфиденциальной информации, появлением нового оборудования и аппаратно-программных средств. Обучение по Программе является необходимым при получении предприятием лицензии на право проведения работ по защите конфиденциальной информации. Настоящая редакция Программы переработана и дополнена для приведения в соответствие 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». Также увеличено количество часов обучения для более полного изучения современных средств и методов технической защиты конфиденциальной информации.

Учебная Программа **«Организация технической защиты конфиденциальной информации»** 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 – 80 академических часов, 10 рабочих дней, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.
Режим обучения 40 академических часов в неделю (5 рабочих дней), в том числе:

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 обьектов 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.

В результате обучения слушатель:
а) должен знать:
- правовые основы обеспечения защиты конфиденциальной информации в Российской Федерации;
- нормативно-методические документы ФСТЭК (Гостехкомиссии России) в области защиты конфиденциальной информации;
- методику организации системы защиты конфиденциальной информации на предприятии;
- классификацию, физическую сущность и степень опасности каналов утечки конфиденциальной информации;
- организационные методы и технические средства защиты конфиденциальной информации;
- методы и критерии оценки защищенности конфиденциальной информации;

б) должен уметь:
- организовывать и проводить работы по защите конфиденциальной информации от технических средств добывания конфиденциальной информации и от ее утечки по техническим каналам;
- применять технические средства защиты конфиденциальной информации;
- оценивать эффективность защиты конфиденциальной информации.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

Учебный план
программы повышения квалификации
«Организация технической защиты конфиденциальной информации»

Цель: формирование у слушателей комплексного подхода к решению задач по организации и обеспечению защиты конфиденциальной информации; обновление и углубление теоретических и практических знаний, умений и навыков по защите конфиденциальной информации; освоение современных методов защиты конфиденциальной информации; теоретическая и практическая подготовка специалистов предприятий – соискателей лицензии на деятельность по технической защите конфиденциальной информации.

Категория слушателей: руководители предприятий и организаций различных форм собственности; руководители, начальники отделов и специалисты служб безопасности (информационной безопасности); руководители и сотрудники отделов автоматизации, вычислительных центров, информационно-технических отделов; руководители и сотрудники специализированных подразделений по защите конфиденциальной информации и по противодействию экономическому шпионажу; руководителей и сотрудников отделов автоматизации, вычислительных центров, информационно-технических отделов.

Срок освоения: 80 часов, 10 учебных дней
Режим занятий: 8 часов в день

№ п/п	Наименование тем и занятий	Всего часов	В том числе		Форма контроля
			лекции	групповые и практические занятия	
1	**Угрозы безопасности конфиденциальной информации**	**12**	**6**	**6**	
1.1	Введение в курс		2		
1.2	Каналы утечки конфиденциальной информации		2	4	
1.3	Состояние и перспективы развития технических средств добывания конфиденциальной информации		2	2	
2	**Основы защиты конфиденциальной информации**	**16**	**8**	**8**	
2.1	Правовые основы защиты конфиденциальной информации		2		
2.2	Государственная система защиты информации		2	2	
2.3	Нормативно-методические документы ФСТЭК (Гостехкомиссии России) по защите информации		2	2	

2.4	Методология обеспечения защиты конфиденциальной информации		2	4	
3	**Организация и обеспечение работ по технической защите конфиденциальной информации**	**14**	**6**	**8**	
3.1	Основы организации работ по защите конфиденциальной информации		2	2	
3.2	Основы обеспечения защиты конфиденциальной информации		2	2	
3.3	Специальные требования и рекомендации по защите конфиденциальной информации		2	4	
4	**Средства технической защиты конфиденциальной информации**	**24**	**8**	**16**	
4.1	Средства защиты от несанкционированного доступа на объекты информатизации		2	4	
4.2	Средства защиты конфиденциальной информации в автоматизированных системах		2	6	
4.3	Средства защиты конфиденциальной информации от утечки за счет ПЭМИН		2	2	
4.4	Средства защиты конфиденциальной информации от утечки по акустическому, виброакустическому и оптическому каналам		2	4	
5	**Контроль защищенности конфиденциальной информации**	**10**	**4**	**6**	
5.1	Организация контроля защищенности конфиденциальной информации		2		
5.2	Контроль защищенности конфиденциальной информации		2	6	
	Итоговая аттестация	**4**		**4**	**Зачет без оценки**
	Итого	**80**	**32**	**48**	

2.2. Содержание Программы

Учебная программа
повышения квалификации
«Организация технической защиты конфиденциальной информации»

Тема № 1. Угрозы безопасности конфиденциальной информации.

Занятие 1. Введение в курс.

Актуальность проблемы защиты конфиденциальной информации, цели, задачи и содержание курса. Основные термины и определения. Перечень угроз безопасности конфиденциальной информации и их характеристика.

Занятие 2. Каналы утечки конфиденциальной информации.

Классификация и общая характеристика каналов утечки конфиденциальной информации. Физические принципы их возникновения и способы выявления. Естественные каналы утечки конфиденциальной информации за счёт ПЭМИН, возникающих в процессе работы технических средств обработки информации. Искусственные каналы утечки конфиденциальной информации, возникающие в процессе применения технических средств добывания конфиденциальной информации

Занятие 3. Состояние и перспективы развития технических средств добывания конфиденциальной информации.

Назначение, состав и технические характеристики средств добывания конфиденциальной информации. Особенности добывания конфиденциальной информации, обрабатываемой в автоматизированных системах, в том числе в глобальных компьютерных сетях. Особенности добывания конфиденциальной информации, обрабатываемой техническими средствами обработки информации. Особенности добывания конфиденциальной информации по акустическому, виброакустическому и оптическому каналам.

Тема № 2. Основы защиты конфиденциальной информации.

Занятие 1. Правовые основы защиты конфиденциальной информации.

Нормативно-правовая база обеспечения безопасности конфиденциальной информации (Конституция РФ, Федеральные Законы, Доктрина информационной безопасности, ГК РФ, УК РФ, УПК РФ и др.) Защита конфиденциальной информации и ответственность за ее разглашение.

Занятие 2. Государственная система защиты информации.

Государственная система защиты информации. Лицензирование деятельности в области защиты информации. Сертификация средств защиты и защищённых систем, средств обработки информации. Аттестация объектов информатизации по требованиям безопасности информации. Основные критерии, оценки и гребования к построению информационных и телекоммуникационных средств и систем в защищенном исполнении.

Занятие 3. Нормативно-методические документы ФСТЭК (Гостехкомиссии России) по защите информации.

Структурная схема и основные положения нормативно-методических документов ФСТЭК (Гостехкомиссии России), регламентирующих деятельность в области защиты конфиденциальной информации.

Занятие 4. Методология обеспечения защиты конфиденциальной информации.

Методологические основы обеспечения защиты конфиденциальной информации. Концепции и политики обеспечения защиты конфиденциальной информации. Анализ риска в информационных системах, угроз и уязвимостей безопасности конфиденциальной информации. Модель нарушителя. Аналитические технологии управления защитой конфиденциальной информации. Управление защитой конфиденциальной информации на основе минимизации рисков. Обеспечение защиты конфиденциальной информации в чрезвычайных ситуациях.

Разработка политики защиты конфиденциальной информации. Методика выявления и формирования сведений, являющихся конфиденциальной информацией. Методики поиска недостатков и уязвимостей систем защиты конфиденциальной информации. Методика построения модели безопасности конфиденциальной информации. План обеспечения защиты конфиденциальной информации.

Тема № 3. Организация и обеспечение работ по технической защите конфиденциальной информации.

Занятие 1. Основы организации работ по защите конфиденциальной информации.

Организация и обеспечение на предприятии режима сохранности конфиденциальной информации. Перечень и содержание мероприятий, а также основных руководящих и распорядительных документов по обеспечению защиты конфиденциальной информации (внутренние документы организации). Категорирование объектов информатизации.

Занятие 2. Основы обеспечения защиты конфиденциальной информации.

Требования и основные направления по оборудованию помещений для проведения конфиденциальных мероприятий. Направления и способы защиты речевой конфиденциальной информации, информации в каналах и линиях связи, информации в автоматизированных системах. Организация защищенного документооборота.

Занятие 3. Специальные требования и рекомендации по защите конфиденциальной информации.

Общие положения, основные требования и рекомендации по защите конфиденциальной информации, циркулирующей в защищаемых помещениях, в системах звукоусиления и звукового сопровождения, при проведении звуко- и видеозаписи, при передаче речевой акустической информации по каналам связи. Общие положения, основные требования и рекомендации по защите конфиденциальной информации при эксплуатации автоматизированных систем, в ЛВС, при межсетевом взаимодействии, при работе с СУБД, при использовании съемных накопителей конфиденциальной информации.

Тема № 4. Средства технической защиты конфиденциальной информации.

Занятие 1. Средства защиты от несанкционированного доступа на объекты информатизации.

Общие положения по защите объектов информатизации и находящихся в них конфиденциальных информационных ресурсов инженерными и техническими средствами и системами защиты. Технические средства и системы охранной сигнализации, контроля и управления доступом, видеонаблюдения.

Занятие 2. Средства защиты конфиденциальной информации в автоматизированных системах.

Основные угрозы безопасности конфиденциальной информации в автоматизированных системах и основные мероприятия по ее защите. Штатные средства защиты операционных систем. Средства защиты конфиденциальной информации на основе электронной цифровой подписи. Средства обнаружения, защиты и противодействия программным атакам. Классификация и архитектура систем обнаружения атак. Средства построения VPN. Способы создания защищенных виртуальных каналов, обзор протоколов. Средства аутентификации удаленных пользователей и распределения криптографических ключей. Сканеры, анализаторы протоколов, фильтры, межсетевые экраны. Межсетевые экраны, сравнительный анализ, достоинства и недостатки.

Занятие 3. Средства защиты конфиденциальной информации от утечки за счет ПЭМИН.

Основные угрозы безопасности конфиденциальной информации, обрабатываемой техническими средствами обработки информации, и основные мероприятия по ее защите. Защита конфиденциальной информации путем экранирования технических средств обработки информации и/или помещений. Средства защиты конфиденциальной информации за счёт использования генераторов помех.

Занятие 4. Средства защиты конфиденциальной информации от утечки по акустическому, виброакустическому и оптическому каналам.

Основные угрозы безопасности конфиденциальной речевой акустической и видеоинформации и основные мероприятия по ее защите. Средства подавления устройств несанкционированной звуко- и видеозаписи. Средства защиты конфиденциальной информации в телефонных линиях на основе скремблирования. Средства виброакустической защиты конфиденциальной информации.

Тема № 5. Контроль защищенности конфиденциальной информации.

Занятие 1. Организация контроля защищенности конфиденциальной информации.

Организация и обеспечение контроля защищенности конфиденциальной информации. Основные технологические процедуры и методика подготовки и проведения контроля. Последовательность и содержание подготовки и проведения работ по выявлению каналов утечки информации. Оценка знаний и выполнения персоналом функциональных обязанностей по защите конфиденциальной информации

Занятие 2. Контроль защищенности конфиденциальной информации.

Соблюдение требований нормативно-методических документов по технической защите конфиденциальной информации. Контроль работоспособности средств защиты конфиденциальной информации. Специальные исследования и специальные лабораторные проверки. Средства контроля защищенности конфиденциальной информации в автоматизированных системах. Средства радиомониторинга, детекторы электромагнитного поля, нелинейные радиолокаторы, средства неавтоматизированного контроля. Многофункциональный поисковый прибор ST-031 «Пиранья»

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

«Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 05.02.2014 №2-ФКЗ, от 21.07.2014 №11-ФКЗ)

«Доктрина информационной безопасности Российской Федерации» (утв. Указом Президента РФ от 09.09.2000 № Пр-1895) (действующая редакция)

Указ Президента РФ от 10.01.2000 №24 «О Концепции национальной безопасности Российской Федерации»

Указ Президента РФ от 16 августа 2004 года, № 1085, Вопросы Федеральной службы по техническому и экспортному контролю

Указ Президента РФ от 6 марта 1997 года, № 188, Перечень сведений конфиденциального характера.

Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (действующая редакция)

Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности» (действующая редакция)

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

Федеральный закон от 29 июля 2004 г. №98-ФЗ «О коммерческой тайне» (действующая редакция)

Федеральный закон от 27.12.2002 №184-ФЗ «О техническом регулировании» (действующая редакция)

Федеральный закон от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности» (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)

Постановление Правительства РФ от 26 июня 1995 года, № 608, «Положение о сертификации средств защиты информации»

Постановление Правительства РФ от 03.02.2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации» вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»

Решение Гостехкомиссии России от 3 октября 1995 года, № 42. Типовые требования к содержанию и порядку разработки руководств по защите информации на объектах

Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. решением Гостехкомиссии РФ 30.03.1992)

Нормативно-методический документ Гостехкомиссии России "Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденный Приказом Гостехкомиссии России от 30.08.2002 N 282.

РД 50-34.698-90. Методические указания. Информационная технология. Комплекс стандартов на АС. Требования к содержанию документов.

РД 50-680-88. Методические указания. Автоматизированные системы. Основные положения

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)

ГОСТ 24.703-85. Типовые проекты решения АСУ.

ГОСТ 26342-84. Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры.

ГОСТ 27990-88. Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования.

ГОСТ 34602-89. Информационная технология. Комплекс стандартов на АС. Техническое задание на создание автоматизированной системы.

ГОСТ 34936-91. Информационная технология. ЛВС. Определение услуг уровня управления доступом.

ГОСТ Р 50739-95. Защита от несанкционированного доступа к информации. Общие технические требования.

ГОСТ 31817.1.1-2012 (IEC 60839-1-1:1988). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения.

ГОСТ Р 50776-95 (МЭК 839-1-4-89). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию.

ГОСТ 50922-2006. Защита информации. Основные термины и определения

ГОСТ 53325-2009. Техника пожарная. Технические средства пожарной автоматики. Общие технические требования. Методы испытаний

ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

ГОСТ 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний

ГОСТ 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51558-2000. Системы охранные телевизионные. Общие технические требования и методы испытаний.

ГОСТ 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

Учебная литература

Автоматизированные системы. Показатели защищенности от несанкционированного доступа к информации. РД. - М.: Гостехкомиссия РФ, 1992.

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

Гусев В.С., Демин В.А., Кузин Б.И. и др. Экономика и организация безопасности хозяйствующих субъектов. 2-е изд. – СПб.: Питер, 2004.

Карпов Е.А., Котенко И.В., Котухов М.М. и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей. Под ред. Котенко И.В. – СПб.: ВУС, 2000.

Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Энциклопедия промышленного шпионажа. Под общ. ред. Куренкова Е.В. – СПб.: Полигон, 1999

Полонский Н.Б., Чехович В.В. Рекомендации по применению, устройству и монтажу экранированных помещений и кабин. – М.: Связь, 1966.

Липатников В.А., Стародубцев Ю.И. Защита информации. – СПб.: ВУС, 2001

Сабынин В.Н. Разведзащищенность, радиоэлектронная защита и безопасность информации: Учебное пособие. Вып. 1, 2, 3. – СПб.: ВАС, 1998.

Технические средства охраны. Под ред. М.Л.Мелик-Адамова и Н.В.Андрианова. М.: ВИПТШ МВД СССР, 1978.

Соколов А.В. Шпионские штучки. Новое и лучшее. – СПб.: Полигон, 2000.

Ярочкин В.И Информационная безопасность: Учебник для студентов вузов. 2-е изд. М.: Академический Проект; Гаудеамус, 2004.

В.А. Северин "Комплексная защита информации на предприятии" 2008г.

Шаньгин В.Ф. "Защита информации в компьютерных системах и сетях" 2012.

Конеев И.Р., Беляев А.В Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003.

Корнеев И.К., Степанов Е.А. Защита информации в офисе: учеб. М.: Проспект, 2008.

Липатников В.А., Стародубцев Ю.И. Защита информации. – СПб.: ВУС. 2001.

Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия - Телеком, 2004

А.Е. Давыдов Р.В. Максимов О.К. Савицкий Технические средства и методы защиты информации от утечки по техническим каналам на объектах информатизации. С-Пб 2012.

М.А.Борисов. О.А.Романов Основы организационно-правовой защиты информации Москва URSS книжный дом "ЛИБРОКОМ" 2012

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 ОПССС TV 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. Актуальность проблемы защиты конфиденциальной информации. Перечень угроз безопасности конфиденциальной информации и их характеристика. Основные термины и определения.
2. Классификация и общая характеристика каналов утечки конфиденциальной информации. Физические принципы их возникновения и способы выявления.
3. Естественные каналы утечки конфиденциальной информации за счёт ПЭМИН, возникающих в процессе работы технических средств обработки информации.
4. Искусственные каналы утечки конфиденциальной информации, возникающие в процессе применения технических средств добывания конфиденциальной информации.
5. Состояние и перспективы развития технических средств добывания конфиденциальной информации.
6. Назначение, состав и технические характеристики средств добывания конфиденциальной информации.
7. Особенности добывания конфиденциальной информации, обрабатываемой в автоматизированных системах, в том числе в глобальных компьютерных сетях.
8. Особенности добывания конфиденциальной информации, обрабатываемой техническими средствами обработки информации.
9. Особенности добывания конфиденциальной информации по акустическому, виброакустическому и оптическому каналам.
10. Правовые основы защиты конфиденциальной информации. Нормативно-правовая база обеспечения безопасности конфиденциальной информации.
11. Защита конфиденциальной информации и ответственность за ее разглашение.
12. Государственная система защиты информации. Основные термины и определения.
13. Лицензирование деятельности в области защиты информации.
14. Сертификация средств защиты и защищённых систем, средств обработки информации.
15. Нормативно-методические документы ФСТЭК (Гостехкомиссии России) по защите информации.
16. Структурная схема и основные положения нормативно-методических документов ФСТЭК (Гостехкомиссии России), регламентирующих деятельность в области защиты конфиденциальной информации.
17. Аттестация объектов информатизации по требованиям безопасности информации.

18. Основные критерии, оценки и требования к построению информационных и телекоммуникационных средств и систем в защищенном исполнении.
19. Методологические основы обеспечения защиты конфиденциальной информации. Концепции и политики обеспечения защиты конфиденциальной информации.
20. Анализ риска в информационных системах, угроз и уязвимостей безопасности конфиденциальной информации.
21. Аналитические технологии управления защитой конфиденциальной информации. Модель нарушителя.
22. Управление защитой конфиденциальной информации на основе минимизации рисков.
23. Обеспечение защиты конфиденциальной информации в чрезвычайных ситуациях.
24. Разработка политики защиты конфиденциальной информации. Методика выявления и формирования сведений, являющихся конфиденциальной информацией.
25. Методики поиска недостатков и уязвимостей систем защиты конфиденциальной информации.
26. Методика построения модели безопасности конфиденциальной информации. План обеспечения защиты конфиденциальной информации.
27. Основы организации работ по защите конфиденциальной информации. Организация и обеспечение на предприятии режима сохранности конфиденциальной информации.
28. Перечень и содержание мероприятий, а также основных руководящих и распорядительных документов по обеспечению защиты конфиденциальной информации (внутренние документы организации).
29. Категорирование объектов информатизации.
30. Основы обеспечения защиты конфиденциальной информации.
31. Требования и основные направления по оборудованию помещений для проведения конфиденциальных мероприятий. Направления и способы защиты речевой конфиденциальной информации, информации в каналах и линиях связи, информации в автоматизированных системах.
32. Организация защищенного документооборота.
33. Общие положения, основные требования и рекомендации по защите конфиденциальной информации, циркулирующей в защищаемых помещениях, в системах звукоусиления и звукового сопровождения, при проведении звуко- и видеозаписи, при передаче речевой акустической информации по каналам связи.
34. Общие положения, основные требования и рекомендации по защите конфиденциальной информации при эксплуатации автоматизированных систем, в ЛВС, при межсетевом взаимодействии, при работе с СУБД, при использовании съемных накопителей конфиденциальной информации
35. Общие положения по защите объектов информатизации и находящихся в них конфиденциальных информационных ресурсов инженерными и техническими средствами и системами защиты.

36. Технические средства и системы охранной сигнализации, контроля и управления доступом, видеонаблюдения.
37. Основные угрозы безопасности конфиденциальной информации в автоматизированных системах и основные мероприятия по ее защите. Штатные средства защиты операционных систем.
38. Средства защиты конфиденциальной информации на основе электронной цифровой подписи.
39. Средства обнаружения, защиты и противодействия программным атакам. Классификация и архитектура систем обнаружения атак.
40. Средства построения VPN. Способы создания защищенных виртуальных каналов, обзор протоколов.
41. Средства аутентификации удаленных пользователей и распределения криптографических ключей.
42. Сканеры, анализаторы протоколов, фильтры, межсетевые экраны: сравнительный анализ, достоинства и недостатки.
43. Средства защиты конфиденциальной информации от утечки за счет ПЭМИН.
44. Основные угрозы безопасности конфиденциальной информации, обрабатываемой техническими средствами обработки информации, и основные мероприятия по ее защите.
45. Защита конфиденциальной информации путем экранирования технических средств обработки информации и/или помещений. Средства защиты конфиденциальной информации за счёт использования генераторов помех.
46. Основные угрозы безопасности конфиденциальной речевой акустической и видеоинформации и основные мероприятия по ее защите.
47. Средства защиты конфиденциальной информации от утечки по акустическому, виброакустическому и оптическому каналам.
48. Средства подавления устройств несанкционированной звуко- и видеозаписи.
49. Средства защиты конфиденциальной информации в телефонных линиях на основе скремблирования.
50. Средства виброакустической защиты конфиденциальной информации.
51. Организация контроля защищенности конфиденциальной информации.
52. Организация и обеспечение контроля защищенности конфиденциальной информации.
53. Основные технологические процедуры и методика подготовки и проведения контроля. Последовательность и содержание подготовки и проведения работ по выявлению каналов утечки информации.
54. Оценка знаний и выполнения персоналом функциональных обязанностей по защите конфиденциальной информации.
55. Соблюдение требований нормативно-методических документов по технической защите конфиденциальной информации.
56. Контроль работоспособности средств защиты конфиденциальной информации. Специальные исследования и специальные лабораторные проверки.

57. Средства контроля защищенности конфиденциальной информации в автоматизированных системах.
58. Средства радиомониторинга, детекторы электромагнитного поля, нелинейные радиолокаторы, средства неавтоматизированного контроля. Многофункциональный поисковый прибор ST-031 «Пиранья» - основные свойства и характеристики.

УЧЕБНАЯ ПРОГРАММА
«Организация технической защиты конфиденциальной информации»