Негосударственное образовательное учреждение дополнительного профессионального образования «ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»

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

Программа повышения квалификации

«Организация расследования нарушений информационной безопасности 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 **«Организация расследования нарушений информационной безопасности 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 и сотрудников подразделений безопасности и IT-подразделений, ответственных за информационную безопасность.

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.

Программа направлена на формирование у слушателей теоретических знаний в области управления информационной безопасностью на предприятии в аспекте применения средств контроля защищенности; изучение целей и задач управления политикой безопасности и исследования компьютерной техники в соответствии с требованиями, предусмотренными законодательными и правовыми актами Российской Федерации, регламентирующими вопросы решения задач в области управления информационной безопасностью на предприятии.
Особое внимание уделено изучению организации расследования компьютерных инцидентов и преступлений в области компьютерной информации.

Учебная Программа **«Организация расследования нарушений информационной безопасности 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 расследования нарушений информационной безопасности на предприятии»

Цель: повышение компетентности специалистов в области управления информационной безопасностью на предприятии.
Категория слушателей: руководители и сотрудники подразделений безопасности и IT-подразделений, ответственные за информационную безопасность; специалисты.
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	Основные понятия в области расследования компьютерных инцидентов и преступлений	6	4	2	
2	Документальное оформление политики безопасности, как гарантия доказательности факта ее нарушения	6	2	4	
3	Контроль защищенности информации в компьютерной сети предприятия	6		6	
4	Минимизация ущерба и сбора данных при расследовании нарушений политики информационной безопасности	6	2	4	
5	Оценка ущерба, нанесенного предприятию в результате нарушения политики информационной безопасности	8	4	4	

6	**Методика и средства исследования компьютерной техники при проведении расследований**	**6**	**2**	**4**	
	Итоговая аттестация	**2**		**2**	**Зачет без оценки**
	Итого	**40**	**14**	**26**	

2.2. Содержание Программы

Учебная программа
повышения квалификации
«Организация расследования нарушений информационной безопасности на предприятии»

Тема 1. Основные понятия в области расследования компьютерных инцидентов и преступлений.

Основные источники угроз безопасности информации на предприятии и предпосылки возникновения инцидентов информационной безопасности. Виды правонарушений в области компьютерной информации. Примеры нарушений политики информационной безопасности. Судебная практика преступлений в области компьютерной информации, основные причины и тенденции. Роль политик информационной безопасности в обеспечении защиты информации на предприятии.

Тема 2. Документальное оформление политики безопасности, как гарантия доказательности факта ее нарушения.

Общее содержание и порядок разработки основных организационно-распорядительных документов предприятия по обеспечению политики информационной безопасности на предприятии. Правовые основания контроля защищенности информации, коммуникаций и средств вычислительной техники.

Тема 3. Контроль защищенности информации в компьютерной сети предприятия.

Контроль доступа пользователей к ресурсам компьютерной сети предприятия. Контроль использования ресурсов электронных коммуникаций сотрудниками предприятия. Программно-аппаратные средства защиты от утечки конфиденциальной информации на предприятии. Построение системы контроля защищенности информации и управления инцидентами нарушения информационной безопасности на предприятии.

Тема 4. Минимизация ущерба и сбора данных при расследовании нарушений политики информационной безопасности.

Порядок изъятия компьютерной техники и носителей информации. Правовые аспекты проведения службой безопасности предприятия служебных расследований. Действия службы безопасности при возникновении (обнаружении) инцидента нарушения политики информационной безопасности. Взаимодействие службы безопасности предприятия с правоохранительными органами.

Тема 5. Оценка ущерба, нанесенного предприятию в результате нарушения политики информационной безопасности.

Способы и средства сбора и документирования доказательств нарушения политики информационной безопасности с использованием средств вычислительной техники. Доказательное значение регистрационных журналов средств защиты информации при проведении официального и частного расследований.

Тема 6. Методика и средства исследования компьютерной техники при проведении расследований.

Порядок подготовки документов, полученных в результате проведения службой безопасности предприятия служебного расследования нарушения политики информационной безопасности к их передаче в правоохранительные и судебные органы. Порядок проведения на предприятии служебных расследований по фактам нарушения политики информационной безопасности и привлечения нарушителей к административной или уголовной ответственности. Практические методы выявления злоумышленников при проведении официального и корпоративного расследования.

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

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

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

Меньшаков Ю.К «Защита объектов и информации от технических средств разведки» – М.: РГГУ, 2002.

Петренко С.А., Симонов С.В. «Управление информационными рисками. Экономически оправданная безопасность» – М. Компания АйТи; ДМК Пресс, 2005

Ющук Е.Л. «Интернет-разведка: руководство к действию» – М. Вершина, 2007

Зима В.М., Молдовян А.А., Молдовян Н.А «Безопасность глобальных сетевых технологий» – СПб. СПбГУ, 1999

Ховард М., Лебланк Д., Вьега Дж. «24 смертных греха компьютерной безопасности» СПб. Питер, 2010

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. Расследование компьютерных преступлений и инцидентов.
2. Функция защиты информации ограниченного доступа.
3. Основные нарушения информационной безопасности на предприятии.
4. Обеспечение управления инцидентами и проведения расследований.
5. Построение системы контроля защищенности информации на предприятии.
6. Методы обнаружения инцидентов информационной безопасности в компьютерной сети предприятия.
7. Начальное реагирование службы безопасности при возникновении инцидентов или обнаружении признаков компьютерного преступления.
8. Обнаружение и фиксация признаков и следов сетевого вторжения.
9. Критерии надежности персонала. Факторы риска персонала.
10. Действия при проведении расследований.
11. Психодиагностика причастности лица к правонарушению в отсутствие доказательств.
12. Методика и средства исследования компьютерной техники при проведении расследований.
13. Анализ файловой системы с использованием поисковых систем.
14. Средства исследования компьютерной техники.
15. Выведывание информации на основе непроизвольных высказываний собеседника.
16. Порядок взаимодействия с правоохранительными органами в случае выявления признаков преступления в сфере высоких технологий.
17. Диагностика лжи при проведении расследований.
18. Приемы манипулирования обследуемым при расследованиях.
19. Тактика получения признаний от подозреваемого при проведении служебных расследований.
20. Проблемы информационной безопасности на предприятиях ТЭК.

УЧЕБНАЯ ПРОГРАММА
«Организация расследования нарушений информационной безопасности на предприятии»