



Негосударственное образовательное учреждение
дополнительного профессионального образования
«ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»



УТВЕРЖДАЮ
Директор НОУ ДПО "ЦПР"
В.Г.Казанцев
" 21 " 2015 года

Программа повышения квалификации

**«Защита от утечки конфиденциальной
информации на предприятии на основе систем
контроля трафика и доступа к защищаемым
ресурсам»**

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 **«Защита от утечки конфиденциальной информации на предприятии на основе систем контроля трафика и доступа к защищаемым ресурсам»** (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).

©Негосударственное образовательное учреждения
дополнительного профессионального образования
«Центр предпринимательских рисков»

СОДЕРЖАНИЕ

1.ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	4
1.1. Цель Программы	4
1.2. Характеристика подготовки по Программе	5
1.3. Требования к уровню подготовки слушателя	5
1.4. Требования к результатам освоения Программы	6
2. СОДЕРЖАНИЕ ПРОГРАММЫ	8
2.1. Учебный план	8
2.2. Содержание Программы	9
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	10
3.1. Требования к минимальному материально-техническому обеспечению	10
3.2. Информационное обеспечение обучения	11
Перечень рекомендуемой литературы, Интернет-ресурсов	
4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ	14
Примерные вопросы для подготовки к зачету	

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель Программы

Программа предназначена для повышения квалификации:

- ведущих (главных) специалистов и специалистов служб безопасности (информационной безопасности),
- руководителей и сотрудников ИТ-подразделений,
- руководителей и сотрудников специализированных подразделений, осуществляющих защиту коммерческой тайны и противодействие экономическому шпионажу,
- администраторов безопасности компьютерных сетей.

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 изучение организационно-технических основ и программно-аппаратных средств контроля сетевого трафика. В Программе значительное внимание уделено вопросам изучения действий сотрудников при использовании средств вычислительной техники и телекоммуникаций, обеспечивающих защиту от утечки конфиденциальной информации на предприятии.

Учебная Программа «Защита от утечки конфиденциальной информации на предприятии на основе систем контроля трафика и доступа к защищаемым ресурсам» 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 деятельностью;
- 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 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-14).

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 санкционированному 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
«Защита от утечки конфиденциальной информации на предприятии на
основе систем контроля трафика и доступа к защищаемым ресурсам»

Цель: повышение компетентности специалистов в области организационно-технических основ и программно-аппаратных средств контроля сетевого трафика.

Категория слушателей: ведущие (главные) специалисты и специалисты служб безопасности (информационной безопасности), руководители и сотрудники ИТ-подразделений, руководители и сотрудники специализированных подразделений, осуществляющие защиту коммерческой тайны и противодействие экономическому шпионажу.

Срок освоения: 40 часов, 5 учебных 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 защите компьютерных сетей от внутренних угроз.	6	6		
2	Основные направления защиты компьютерных сетей от внутренних угроз.	4	2	2	
3	Контроль активности сотрудников.	6	4	2	
4	Инструментальные средства проведения аудита внутренней безопасности компьютерной сети.	4	2	2	
5	Организация сетевого взаимодействия в современных компьютерных сетях.	6	2	4	
6	Анализ содержимого сетевого трафика в компьютерных сетях.	8	4	4	
7	Использование анализатора протокола Wireshark как средства анализа сетевого трафика.	4	2	2	
	Итоговая аттестация	2		2	Зачет без оценки
	Итого	40	22	18	

2.2. Содержание Программы

Учебная программа повышения квалификации

«Защита от утечки конфиденциальной информации на предприятии на основе систем контроля трафика и доступа к защищаемым ресурсам»

Тема 1. Общие положения по защите компьютерных сетей от внутренних угроз.

Использование вредоносного ПО для осуществления утечек информации. Уязвимости сетевых протоколов используемых для проведения сетевых атак внутри компьютерной сети. Юридические аспекты защиты компьютерных сетей от внутренних угроз. Использование специального ПО для сбора информации о деструктивных информационно-технических воздействиях в компьютерной сети.

Тема 2. Основные направления защиты компьютерных сетей от внутренних угроз.

Обзор существующих технологий защиты. Обзор существующих технологий защиты. Безопасность беспроводных компьютерных сетей. Демонстрация проведения основных типов сетевых атак в беспроводных КС.

Тема 3. Контроль активности сотрудников.

Использование методики honeypot. Протоколирование действий сотрудников с помощью специальных программных средств. Контроль рабочих мест сотрудников. Использование кейлоггеров и "тройных" программ. Контроль трафика электронной почты и обращения к Web-сайтам. Виды активности, которые требуется контролировать.

Тема 4. Инструментальные средства проведения аудита внутренней безопасности компьютерной сети.

Использование утилит Autoscanner, Nmap и т.д. Аудит внутренних угроз в компьютерной сети. Демонстрация проведения основных типов сетевых атак в компьютерной сети.

Тема 5. Организация сетевого взаимодействия в современных компьютерных сетях.

Архитектура TCP/IP. Основные сервисы (службы), используемые в современных компьютерных сетях для передачи сообщений (файлов).

Тема 6. Анализ содержимого сетевого трафика в компьютерных сетях.

Существующие подходы к анализу сетевого трафика. Контроль SMTP-трафика и электронной почты. Варианты решений. Системы анализа содержимого (контента). Средство анализа протоколов Ethereal. Сниффер коммутируемых сетей Ettercap. Примеры использования снифферов.

Тема 7. Использование анализатора протокола Wireshark как средства анализа сетевого трафика.

Практика анализа сетевого трафика. Средства анализа, функционирующие на основе анализа сетевого трафика - Невод.

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 информационной 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-диск с записью учебно-методических материалов Программы (презентации преподавателей, конспекты, нормативно-правовые акты, образцы рассматриваемых 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 Составы 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

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

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

Сердюк В.А. "Организация и технологии защиты информации" 2011г.

А.М. Карминский "Информационно-аналитическая составляющая бизнеса" 2007г.

Конеев И.Р., Беляев А. 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.

Мельников В.П Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений. Под ред. Клейменова С.А. 2-е изд., стер. – М.: Академия, 2007.

Под общ. ред. Иванова С.Б Оружие и технологии России. Энциклопедия. XXI век. Том VIII. Информационная безопасность. М.: Оружие и технологии, 2003.

Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи, 2006.

Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности. – М.: Гелиос АРВ, 2005.

Хаулет Т. Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям: учебное пособие. М.: Интернет-Университет Информационных технологий, 2007. 608 с.

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/> RUBEЖ 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. Использование вредоносного ПО для осуществления утечек информации.
2. Уязвимости сетевых протоколов.
3. Юридические аспекты защиты компьютерных сетей от внутренних угроз.
4. Безопасность беспроводных компьютерных сетей.
5. Использование методики honey pot.
6. Использование кейлоггеров и "тройных" программ.
7. Контроль трафика электронной почты и обращения к Web-сайтам.
8. Виды активности, которые требуется контролировать.
9. Аудит внутренних угроз в компьютерной сети.
10. Архитектура TCP/IP.
11. Существующие подходы к анализу сетевого трафика.
12. Контроль HTTP-трафика и электронной почты.
13. Средство анализа протоколов Ethereal.
14. Примеры использования снифферов.
15. Средства анализа, функционирующие на основе анализа сетевого трафика - Певод.

УЧЕБНАЯ ПРОГРАММА
«Защита от утечки конфиденциальной информации на предприятии на основе систем контроля трафика и доступа к защищаемым ресурсам»

© Негосударственное образовательное учреждение
дополнительного профессионального образования
«Центр предпринимательских рисков»