


Министерство образования и науки Челябинской области
Государственное бюджетное профессиональное образовательное учреждение
«Челябинский радиотехнический техникум»

Рассмотрено
На педагогическом совете
Протокол № 217
от 29 августа 2019г.

Утверждаю

Заместитель директора по учебной работе

 Моторина Н.М.

«» 2019г.

Программа дополнительного профессионального образования
(повышения квалификации)
«Современные сетевые технологии»

г. Челябинск

СОДЕРЖАНИЕ

1. Пояснительная записка.....	3
2. Общие положения.....	3
3. Используемые сокращения.....	3
4. Характеристика подготовки по специальности.....	3
5. Документы, определяющие содержание и организацию образовательного процесса.....	3
6. Цели и планируемые результаты Программы ДПО.....	4
7. Кадровое обеспечение реализации Программы ДПО.....	6
8. Учебно-методическое обеспечение реализации Программы ДПО.....	6
9. Материально-техническое обеспечение реализации Программы ДПО.....	8
10. Контроль качества и оценка освоения обучающимися Программы ДПО.....	9
11. Приложения к Программе ДПО.....	10
12. Примерный учебный план.....	10
13. Календарный учебный график.....	10

1. Пояснительная записка

Настоящая образовательная программа дополнительного профессионального образования (повышения квалификации) разработана Государственным бюджетным профессиональным образовательным учреждением «Челябинский радиотехнический техникум» (далее по тексту, в соответствующих - падежах ГБПОУ «Челябинский радиотехнический техникум», «Техникум»), для освоения лицами осваивающих основную образовательную программу среднего профессионального образования по специальности «Обеспечение информационной безопасности автоматизированных систем».

Право на реализацию образовательной программы дополнительного профессионального образования (повышения квалификации) по специальности «Обеспечение информационной безопасности автоматизированных систем» (далее по тексту, в соответствующих падежах – «Программа ДПО») Техникум осуществляет в соответствии с лицензией на осуществление образовательной деятельности.

Требования к слушателям – лица, получающие среднее профессиональное образование по специальности «Обеспечение информационной безопасности автоматизированных систем».

Результат освоения Программы ДПО: повышение получаемой квалификации «Техник по защите информации».

Форма документа, выдаваемого по результатам освоения Программы ДПО и прохождения итоговой аттестации – удостоверение о повышении квалификации.

2. Общие положения

Нормативно-правовую базу для разработки Образовательной программы дополнительного профессионального образования составляют:

- Федеральный Закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства образования и науки Российской Федерации от 01.07.2013 года № 499 «Об утверждении порядка и организации деятельности по дополнительным профессиональным программам»;
- Локальные акты ГБПОУ «Челябинский радиотехнический техникум».

3. Используемые сокращения

В Программе ДПО используются следующие сокращения:

- ДПО - дополнительное профессиональное образование;
- ПК - профессиональная компетенция;
- СПО - среднее профессиональное образование;
- УД - учебная дисциплина.

4. Характеристика подготовки по специальности

Требования к уровню подготовки, необходимому для освоения Программы ДПО, нормативные сроки освоения Программы ДПО при очной и заочной формах получения образования отражены в таблице 1.

Таблица 1

Требования к уровню подготовки	Нормативный срок освоения Программы ДПО
студенты 1 курса, осваивающие основную образовательную программу СПО по специальности «Обеспечение информационной безопасности автоматизированных систем»	160 часов

5. Документы, определяющие содержание и организацию образовательного процесса

В соответствии с Федеральным Законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Программа ДПО включает в себя учебный план, календарный учебный график, рабочие программы УД, фонд оценочных средств.

6. Цели и планируемые результаты Программы ДПО

Настоящая Программа ДПО направлена на освоение (совершенствование) следующих профессиональных компетенций:

ПК 1 – Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 2 – Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 3 – Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации

ПК 4 – Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 5 – Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 6 – Осуществлять изменение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 7 – Осуществлять изменение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

Студенты 1 курса, осваивающие основную образовательную программу СПО по специальности «Обеспечение информационной безопасности автоматизированных систем» в результате освоения Программы ДПО получают знания и умения, отраженные в таблице 2.

Таблица 2

Наименование учебных дисциплин	Наименование учебных циклов, разделов, модулей, требования к знаниям, умениям, практическому опыту	Всего максимальной учебной нагрузки обучающегося
Основы программирования отраслевых приложений	<p>уметь:</p> <ul style="list-style-type: none"> – разрабатывать программный код серверной части веб-приложений. – производить тестирование разработанного веб приложения. – размещать веб приложения в сети в соответствии с техническим заданием <p>знать:</p> <ul style="list-style-type: none"> – язык программирования Python для разработки серверной части веб-приложений. 	20
Основы математического анализа в сетевых технологиях	<p>уметь:</p> <ul style="list-style-type: none"> – решать задачи математического анализа; – применять методы дифференциального исчисления. <p>знать:</p> <ul style="list-style-type: none"> – основы математического анализа; – основы дифференциального исчисления. 	20
Основы сетевых технологий	<p>уметь:</p> <ul style="list-style-type: none"> – выполнять задачи проектирования, развертывания и технического сопровождения локальных и глобальных сетей; – использовать общепризнанные мировые стандарты и решения в своей работе; – выполнять типовые задачи развертывания и технического сопровождения малой сети предприятия или ее фрагмента. 	40

	<p>знать:</p> <ul style="list-style-type: none"> – создание и настройка одноранговой сети, компьютерной сети с помощью маршрутизатора, беспроводной сети; – создание подсетей и настройка обмена данными; – использования основных команд для проверки подключения к сети Интернет, отслеживания сетевых пакетов, параметров IP-адресации.; 	
<p>Комплексная система защиты информационных систем и критической информационной инфраструктуры</p>	<p>уметь:</p> <ul style="list-style-type: none"> – выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. – осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. – планировать и реализовывать собственное профессиональное и личностное развитие. – использовать информационные технологии в профессиональной деятельности. – пользоваться профессиональной документацией на государственном и иностранном языках. – обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами – осуществлять обработку, хранение и передачу информации ограниченного доступа. <p>знать:</p> <ul style="list-style-type: none"> – нормативные правовые акты в области информационной безопасности и защиты информационных систем и критической информационной инфраструктуры, методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; – основы организации комплексных систем защиты информации и информационных систем; – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; 	<p>40</p>
<p>Защита данных от утечек информации средствами InfoWatch Traffic Monitor</p>	<p>уметь:</p> <ul style="list-style-type: none"> – производить подбор необходимого программного обеспечения, обслуживать и администрировать операционную систему; – определять минимальные права доступа для наибольшей безопасности; – анализировать показания файлов журналов с целью выявления наступающих угроз; <p>знать:</p> <ul style="list-style-type: none"> – классификацию, назначение и область применения дистрибутивов операционной системы; – базовые знания об архитектурном строении ядра 	<p>38</p>

	операционной системы и его функционировании; – методы обслуживания операционной системы, поиска неполадок, администрировании ОС	
Итоговая аттестация		2

7. Кадровое обеспечение реализации Программы ДПО

Реализация Программы ДПО обеспечивается педагогическими кадрами, имеющими высшее профессиональное образование по направлению подготовки «Образование и педагогика» или в области, соответствующей преподаваемой дисциплины, без предъявления требований к стажу работы, либо высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательном учреждении без предъявления требований к стажу работы.

8. Учебно-методическое обеспечение реализации Программы ДПО

Реализация Программы ДПО обеспечивается доступом каждого обучающегося к базам данных и библиотечным фондам, формируемым по полному перечню учебных дисциплин.

Во время самостоятельной подготовки обучающиеся обеспечены доступом к информационно-телекоммуникационной сети «Интернет».

Библиотечный фонд укомплектован печатными и электронными изданиями учебной литературы по дисциплинам, изданными за последние 5 лет.

Библиотечный фонд помимо учебной литературы включает официальные, справочно-библиографические издания.

Перечень используемых учебных изданий, интернет-ресурсов, дополнительной литературы:

1. Федеральный закон от 27.12.2002 г. № 184-ФЗ «О техническом регулировании»
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
5. Постановление Правительства Российской Федерации от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Постановление Правительства РФ от 6.07.2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»
7. Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
8. Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»
9. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
10. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
11. Приказ ФСТЭК России №227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»
12. Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к

созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»

13. Приказ ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

14. Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»

15. Информационное сообщение ФСТЭК России №240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ»

16. Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

17. Приказ ФСБ России №366 от 24.07.2018 «О НКЦКИ»

18. Приказ ФСБ России №367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»

19. Приказ ФСБ России №368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

20. Приказ ФСБ России №196 от 06.05.2019 «Об утверждении требований к средствам ГосСОПКА»

21. Приказ ФСБ России №281 от 19.06.2019 «Об утверждении Порядка, технических условий установки и эксплуатации средств ГосСОПКА»

22. Приказ ФСБ России №282 от 19.06.2019 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении ЗО КИИ РФ»

23. Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах».

24. Государственный реестр сертифицированных средств защиты информации ФСТЭК России.

25. Банк данных угроз безопасности информации ФСТЭК России

26. Гришина Н.В. Комплексная система защиты информации на предприятии: Учебное пособие. — М.: Издательский центр «Инфра-М», 2014. — 240 с.

27. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822, 3-е издание — Б.: Издательство «Вильямс, 2013».

28. Олифер Н. Олифер В. Компьютерные сети. Принципы, протоколы, технологии. СПб, Питер, 2011 г.

29. Смелянский Р.Л. Компьютерные сети. Системы передачи данных. Москва, Академия, 2017 г.

30. Торвальдс Д.С. Linux. Канада. 2015 г.

31. Денис Колисниченко. Администрирование ОС Linux. Москва, 2012г.

32. Парфилова Н. И., Пылькин А. Н., Трусков Б. Г. Программирование: Основы алгоритмизации и программирования: учебник / под ред. Б. Г. Трускова. — М.: 2014

33. Великович Л.С., Цветкова М.С. Программирование для начинающих: учеб. издание. — М., 2015.

Дополнительные печатные источники:

34. Шевцова А.М., Пантюхин П.Я. Введение в автоматизированное проектирование: учеб. пособие с приложением на компакт диске учебной версии системы АДЕМ. — М., 2015.

35. InfoWatch Traffic Monitor 6.11. Руководство пользователя

36. InfoWatch Traffic Monitor 6.11. Руководство администратора

37. InfoWatch Traffic Monitor 6.11. Руководство по установке

38. InfoWatch. Работа в Консоли Управления Device Monitor

Интернет-ресурсы:

39. <http://netacad.com>

40. <http://window.edu> (Единое окно доступа к образовательным ресурсам)
41. <http://www.edu.ru> (Федеральный портал «Российское образование»)
42. <http://school.edu.ru> (Российский общеобразовательный портал)
43. <http://ege.edu.ru> (Портал информационной поддержки единого государственного экзамена)
44. <http://algotlist.manual.ru> (Алгоритмы, методы, исходники)
45. <http://alglib.sources.ru> (Библиотека алгоритмов)
46. <http://www.mathprog.narod.ru> (Математика и программирование)
47. <http://cyber-net.spb.ru> (Олимпиада по кибернетике для школьников)
48. <http://www.olimpiads.ru> (Олимпиадная информатика)
49. <http://www.informatics.ru> (Олимпиады по информатике: сайт Мытищинской школы программистов)
50. <http://ips.ifmo.ru> (Российская Интернет-школа информатики и программирования)
51. <http://www.sprint-inform.ru> (Справочная интерактивная система по информатике «Спринт-информ»)
52. <http://www.junior.ru/wwwexam/> (Тесты по информатике и информационным технологиям. Центр образования «Юниор»).

9. Материально-техническое обеспечение реализации Программы ДПО

Техникум располагает материально-технической базой, обеспечивающей проведение всех видов аудиторных и практических занятий, предусмотренных учебным планом образовательной организации.

Реализация ДПО обеспечивает:

- выполнение обучающимися практических занятий, включая как обязательный компонент практические задания с использованием персональных компьютеров;
- освоение обучающимися учебных дисциплин в условиях созданной соответствующей образовательной среды в зависимости от специфики вида деятельности.

Материально-техническая база соответствует действующим санитарно-эпидемиологическим нормам и нормам пожарной безопасности.

Перечень помещений, используемых при реализации Программы ДПО:

Таблица 3

Перечень помещений	Наименование
Кабинеты	Кабинет для проведения аудиторных занятий;
	Компьютерный класс, оборудованный средствами ввода и вывода информации на разные виды источников, мастерская «Корпоративная защита от внутренних угроз информационной безопасности»
Залы	Библиотека, читальный зал с выходом в сеть Интернет;

При использовании электронных изданий техникум обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин.

Во всех компьютерных лабораториях установлено лицензионное и бесплатное программное обеспечение.

Перечень программного обеспечения, используемого при реализации Программы ДПО:

Архиваторы: 7-Zip

Браузеры: Internet Explorer, Google Chrome, Mozilla Firefox

Графические приложения: CorelDRAW Graphics Suite X7 (Лицензия), Autodesk 3ds Max, Autodesk Maya, Autodesk AutoCAD, Autodesk AutoCAD Electrical, Autodesk Inventor Professional, GIMP (GNU GPL), Inkscape (GNU GPL), КОМПАС-3D (Лицензия), Paint.NET, Scribus (GNU GPL), Adobe Photoshop, Adobe Premiere, Adobe Illustrator, Adobe After Effects.

Создание и разработка сайтов: Adobe Dreamweaver, Open Server Panel.

Офисные приложения: Microsoft Office (Лицензия), Microsoft Visio (Лицензия), Skype

для Windows, LibreOffice, Notepad++, Scilab (GNU GPL), Adobe Reader
 Средства разработки: Microsoft SQL Server, Microsoft Visual Studio, National Instruments LabVIEW, Eclipse (GNU GPL), Unity.
 Тестовые программы: 3DMark, CPU-Z, GPU-Z
 Электроника: AVR Studio, Altium Designer, Atmel Studio.
 Виртуализация: Microsoft Hyper-V, VMware Workstation Player, VMware ESXi
 Файловые менеджеры: Far manager, Total commander.
 Антивирусы: Антивирус Касперского
 Проигрыватели: AIMP, VLC media player, DaumPotPlayer, gom player.

10. Контроль качества и оценка освоения обучающимися Программы ДПО

Контроль качества и оценка освоения Программы ДПО включает итоговую аттестацию обучающихся:

Итоговая аттестация освоения Программы ДПО проводится в форме итогового зачета.

Таблица 4

Результаты освоения Программы ДПО (освоенные профессиональные компетенции)	Основные показатели оценки результата
ПК 1 – Администрировать программные и программно-аппаратные компоненты автоматизированной информационной системы в защищенном исполнении..	Создание и настройка одноранговой сети, компьютерной сети с помощью маршрутизатора, беспроводной сети; создание подсетей и настройка обмена данными; использования основных команд для проверки подключения к сети Интернет, отслеживания сетевых пакетов, параметров IP-адресации.;
ПК 2 – Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Основные типы средств программной защиты информации.
ПК 3 – Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Создание и настройка одноранговой сети, компьютерной сети с помощью маршрутизатора, беспроводной сети; создание подсетей и настройка обмена данными; использования основных команд для проверки подключения к сети Интернет, отслеживания сетевых пакетов, параметров IP-адресации.
ПК 4 – Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Общие принципы построения алгоритмов;
ПК 5 – Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Основные понятия, алгоритмические конструкции языка программирования.
ПК 6 – Осуществлять изменение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	Знать основы математического анализа.
ПК 7 – Осуществлять изменение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Знать основы дифференциального исчисления

Для аттестации обучающихся на соответствие их персональным достижений при

освоении Программы ДПО используются фонды оценочных средств, позволяющие оценить умения, знания, практический опыт и освоенные компетенции.

11. Приложения к Программе ДПО

- Приложение №1 – Учебный план;
- Приложение №2 – Календарный учебный график;
- Приложение №3 – Рабочие программы учебных дисциплин;
- Приложение №4 – Фонд оценочных средств.

12. Примерный учебный план

Примерный учебный план (таблица 5) является основой для разработки учебного плана, непосредственно используемого при освоении Программы ДПО.

Примерный учебный план для студентов, осваивающих основную образовательную программу среднего профессионального образования по специальности «Обеспечение информационной безопасности автоматизированных систем» отражен в таблице 5.

Примерный учебный план регламентирует примерный порядок реализации Программы ДПО и определяет примерные количественные и качественные характеристики реализации Программы ДПО:

- объемные параметры учебной нагрузки в целом, по семестрам и годам обучения;
- перечень, последовательность изучения и объемы учебной нагрузки по учебным дисциплинам;

Таблица 5

Наименование дисциплин	Период реализации Программы ДПО	Количество часов по учебным дисциплинам в соответствии с образовательной программой дополнительного профессионального образования (учебный план)
Основы программирования отраслевых приложений	1 курс	20
Основы математического анализа в информационной безопасности	1 курс	20
Основы сетевых технологий	2 курс	40
Комплексная система защиты информационных систем и критической информационной инфраструктуры	3 курс	40
Защита данных от утечек информации средствами InfoWatch Traffic Monitor	4 курс	38
Итоговая аттестация. Зачет.	4 курс	2
Всего		160

13. Календарный учебный график

Календарный учебный график составляется по всем курсам обучения и утверждается директором техникума сроком на один учебный год.

Календарный учебный график устанавливает последовательность и продолжительность теоретического обучения практических занятий.

Таблица «Календарный учебный график» отражает объемы часов на освоение учебных дисциплин.

Сумма часов учебной нагрузки в неделю составляет: 4 часа.