

Учреждение дополнительного профессионального образования  
«Энергетический институт повышения квалификации  
Публичного акционерного общества энергетики  
и электрификации Кубани»

**УТВЕРЖДАЮ**

Ректор

УДПО «Энергетический институт  
повышения квалификации  
ПАО «Кубаньэнерго»



**Е.В. Рудь**

«\_\_\_\_\_» 2017 г.

**ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА**  
(дополнительная образовательная программа)  
«Сертифицированный профессионал по безопасности сетей Huawei»  
(120 час.)

Краснодар, 2017

## Пояснительная записка

### 1. Общие положения.

1.1. Программа повышения квалификации по безопасности сетей Huawei, состоящая из трех курсов уровня «Professional»:

- 1) Построение инфраструктуры сетевой безопасности Huawei
- 2) Построение безопасной инфраструктуры терминального доступа Huawei
- 3) Построение безопасных сервисных сетей Huawei

1.2. Цель обучения: Формирование знаний и навыков, необходимых для работы с технологиями и оборудованием корпоративных локальных сетей на профессиональном уровне.

1.3. Категория слушателей: администраторы сетей, сетевые инженеры и специалисты.

Последовательность изучения некоторых тем в случае необходимости разрешается изменять, но при обязательном условии, что программа будет выполнена полностью по содержанию и объему количества часов.

К концу обучения каждый слушатель должен уметь выполнять работы, предусмотренные квалификационной характеристикой, в соответствии с требованиями производства или предприятия.

### 2. Организация обучения.

2.1. Обучение организуется УДПО «Энергетический институт повышения квалификации ПАО «Кубаньэнерго», в соответствии с прилагаемой программой обучения.

2.2. Для проведения занятий приглашаются преподаватели вузов и наиболее подготовленные специалисты.

2.3. Начальный уровень подготовленности слушателей, для которых предназначена данная программа - высшее или среднее специальное образование. Опыт работы на профессиональном уровне с оборудованием корпоративных сетей других вендоров.

2.4. Формы обучения: лекция, работа в группах, обучение на ситуациях, заполнение документов, письменные опросы, индивидуальные консультации, тренажерная подготовка. При обучении используются технические средства, наглядные и раздаточные материалы.

2.5. В процессе самостоятельной подготовки слушатели изучают материал в объеме основных положений нормативных и инструктивных документов с учетом рекомендаций преподавателя, проводившего консультацию по самостоятельной подготовке.

2.6. Продолжительность обучения – 120 часов.

2.7. Теоретическое обучение осуществляется в учебных группах численностью 5 – 60 человек, производственное – численностью 5 – 30 человек, а обучение по профессиям тренажерной подготовки, 2 – 10 человек.

2.8. Последовательность изучения некоторых тем в случае необходимости разрешается изменять, но при обязательном условии, что программа будет выполнена полностью по содержанию и объему количества часов.

2.9. К концу обучения каждый слушатель должен уметь выполнять работы, предусмотренные квалификационной характеристикой, в соответствии с требованиями производства или предприятия.

2.10. В конце обучения по курсу: «Сертифицированный профессионал по безопасности сетей Huawei» каждый обучаемый проходит итоговый контроль знаний.

2.11. По итогам обучения слушатели получают удостоверение о повышении квалификации установленного образца.

**УЧЕБНЫЙ ПЛАН**  
 дополнительной образовательной программы  
 «Сертифицированный профессионал по безопасности сетей Huawei»  
 (120 час.)

№ п/п	Дисциплины	Всего (час.)	Объемы занятий, часов		Дистанционная подготовка	Форма контроля
			лекц.	практ. зан.		
1.	Введение в курс	4	2	2		
2.	Принципы работы и конфигурации firewall packet fragmentation, firewall IP CAR, firewall DHCP Snooping, системы Dual-system hot backup.	10	2	8		
3.	Принципы и конфигурации IP-link, Eth-Trunk, Link-group.	10	4	6		
4.	Принципы и технологии виртуального брандмауэра.	10	4	6		
5.	Принципы работы базовых сетевых атак.	10	2	8		
6.	Построение сетей решения anti-DDoS.	12	4	8		
7.	Устранение неполадок в VPN.	10	2	8		
8.	Основные принципы обеспечения безопасности терминала.	10	2	8		
9.	Политики безопасности в процессе аутентификации.	12	4	8		
10.	Принципы применения контроля множественного доступа устройств.	10	2	8		
11.	Принципы работы и поддержания Policy Center system.	10	2	8		
12.	Принципы использования средств диагностики для устранения неполадок в процессе обеспечения безопасности.	10	2	8		
13.	Итоговая аттестация	2				Зачет
<b>Всего часов:</b>		<b>120</b>	<b>32</b>	<b>86</b>		<b>2</b>

Первый проректор



Т. З. Пономаренко