

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП.



**Дополнительная профессиональная программа
повышения квалификации**

**«Введение в работу протокола 802.1X для специалистов
по безопасности (802.1X)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	5
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	7
2.3 Рабочая программа учебных предметов	7
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.	10
3.1 Требования к педагогам	10
3.2 Материально-техническое оснащение программы	10
3.3. Учебно-методическое оснащение программы	10
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	10
V. СОСТАВИТЕЛИ ПРОГРАММЫ	11

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Введение в работу протокола 802.1X для специалистов по безопасности (802.1X)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 18.11.2014 N 896н "Об утверждении профессионального стандарта "Специалист по информационным системам"(Зарегистрировано в Минюсте России 24.12.2014 N 35361), приказом Минтруда России от 19.05.2014 N 316н «Об утверждении профессионального стандарта "Инженер-проектировщик в области связи (телекоммуникаций)", приказом Минтруда России от 03.11.2016 N 608н «Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях".

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Целью дополнительной профессиональной программы повышения квалификации «Введение в работу протокола 802.1X для специалистов по безопасности (802.1X)» является обеспечение слушателей базовыми знаниями о возможностях и функциях

протокола IEEE 802.1X, а также умением настроить Cisco Identity Services Engine (ISE) для работы протокола 802.1X. В программе описаны архитектура, компоненты и возможности сети Cisco TrustSec на базе протоколов IEEE 802.1X и RADIUS. Слушатели получают практический опыт конфигурации сетевых служб на базе 802.1X при помощи Cisco ISE, коммутаторов Cisco Catalyst, а также беспроводных продуктов Cisco.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Введение в работу протокола 802.1X для специалистов по безопасности (802.1X)».

Слушатель должен уметь:

- настраивать протоколы RADIUS и EAP.
- внедрять решение Cisco ISE в сети предприятия.

Слушатель должен знать:

- принципы работы протокола AAA;
- принципы работы протокола 802.1X.

Слушатель должен владеть:

- навыками настройки Cisco WebAuth для клиентских станций без поддержки 802.1X;
- навыками настройки компонентов 802.1X на Cisco ISE, коммутаторе, WLC и клиенте.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 24 часа, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Введение в работу протокола 802.1X для специалистов по безопасности
(802.1X)»

Срок обучения: 24 часа.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,5	0,5	0	Групповой опрос
2.	Архитектура Cisco TrustSec	1,5	1,5	0	Групповой опрос
2.1.	Обзор Cisco TrustSec	0,8	0,8	0	
2.2.	Обзор составляющих архитектуры Cisco TrustSec	0,7	0,7	0	
3.	Обзор аутентификации на уровне порта	4	3	1	Групповой опрос
3.1.	Обзор стандарта IEEE 802.1X	1,2	1,2	0	
3.2.	Обзор 802.1X и EAP	1	1	0	
3.3.	Роль протокола RADIUS в соединениях, использующих протокол EAP	0,8	0,8	0	
3.4.	Лабораторная работа 1: Предварительная настройка сети	1	0	1	
4.	Конфигурация устройств для работы с 802.1X	8	3	5	Групповой опрос
4.1.	Компоненты и топологии 802.1X	0,9	0,9	0	
4.2.	Конфигурация Cisco ISE для работы с 802.1X	1	1	0	
4.3.	Конфигурация сетевых устройств для поддержки 802.1X	0,8	0,8	0	
4.4.	Конфигурация клиентских станций для поддержки 802.1X	0,3	0,3	0	
4.5.	Лабораторная работа 2: Настройка компонентов 802.1X на Cisco ISE, коммутаторе, WLC и клиенте	5	0	5	
5.	Конфигурация гостевого доступа	5,5	1,5	4	Групповой опрос
5.1.	Конфигурация Cisco TrustSec для клиентских станций без поддержки 802.1X	0,7	0,7	0	
5.2.	Конфигурация Cisco WebAuth для клиентских станций без поддержки	0,8	0,8	0	

	802.1X				
5.3.	Лабораторная работа 3: Настройка гостевого доступа с помощью веб-аутентификации	4	0	4	
6.	Разработка дизайна сетей Cisco TrustSec на базе Cisco ISE и 802.1X	3,5	2	1,5	
6.1.	Совместимость составляющих сети с 802.1X	1	1	0	
6.2.	Обзор нюансов внедрения 802.1X, влияющих на дизайн сети	0,6	0,6	0	
6.3.	Обзор масштабируемых архитектур 802.1X	0,4	0,4	0	
6.4.	Лабораторная работа 4: Построение архитектуры Cisco TrustSec	1,5	0	1,5	
	Всего:	23	11.5	11.5	
	Итоговый контроль знаний	1	0	0	Электронное тестирование
	Итого:	24	11.5	11.5	

2.2 Календарный учебный график

Занятия проводятся 3 раза в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки	недели	1		
обучения	дни	1	1	1
Вид занятий		А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Введение в работу протокола 802.1X для специалистов по безопасности (802.1X)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,5	0,5	0	Групповой опрос

2. Архитектура Cisco TrustSec

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Архитектура Cisco TrustSec				
2.1	Обзор Cisco TrustSec	0,8	0,8	0	
2.2	Обзор составляющих архитектуры Cisco TrustSec	0,7	0,7	0	
	ИТОГО	1,5	1,5	0	Групповой опрос

3. Обзор аутентификации на уровне порта

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Обзор аутентификации на уровне порта				
3.1	Обзор стандарта IEEE 802.1X	1,2	1,2	0	
3.2	Обзор 802.1X и EAP	1	1	0	
3.3	Роль протокола RADIUS в соединениях, использующих протокол EAP	0,8	0,8	0	
3.4	Лабораторная работа 1: Предварительная настройка сети	1	0	1	
	ИТОГО	4	3	1	Групповой опрос

4. Конфигурация устройств для работы с 802.1X

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Конфигурация устройств для работы с 802.1X				
4.1	Компоненты и топологии 802.1X	0,9	0,9	0	
4.2.	Конфигурация Cisco ISE для работы с 802.1X	1	1	0	
4.3.	Конфигурация сетевых устройств для поддержки 802.1X	0,8	0,8	0	
4.4.	Конфигурация клиентских станций для поддержки 802.1X	0,3	0,3	0	
4.5.	Лабораторная работа 2: Настройка компонентов 802.1X на Cisco ISE, коммутаторе, WLC и клиенте	5	0	5	
	ИТОГО	8	3	5	Групповой опрос

5. Конфигурация гостевого доступа

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Конфигурация гостевого доступа				
5.1	Конфигурация Cisco TrustSec для клиентских станций без поддержки 802.1X	0,7	0,7	0	
5.2.	Конфигурация Cisco WebAuth для клиентских станций без поддержки 802.1X	0,8	0,8	0	
5.3.	Лабораторная работа 3: Настройка гостевого доступа с помощью веб-аутентификации	4	0	4	
	ИТОГО	5,5	1,5	4	Групповой опрос

6. Разработка дизайна сетей Cisco TrustSec на базе Cisco ISE и 802.1X

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Разработка дизайна сетей Cisco TrustSec на базе Cisco ISE и 802.1X				
6.1	Совместимость составляющих сети с 802.1X	1	1	0	
6.2.	Обзор нюансов внедрения 802.1X, влияющих на дизайн сети	0,6	0,6	0	
6.3.	Обзор масштабируемых архитектур 802.1X	0,4	0,4	0	
6.4.	Лабораторная работа 4: Построение архитектуры Cisco TrustSec	1,5	0	1,5	
	ВСЕГО	3,5	2	1,5	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

«Cisco StealthWatch 6.9 Power Workshop (CSWPW)»

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	4
1.5 Трудоемкость обучения	4
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	6
2.3 Рабочая программа учебных предметов	7
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	9
3.1 Требования к педагогам	9
3.2 Материально-техническое оснащение программы	9
3.3 Учебно-методическое оснащение программы	9
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	9
V. СОСТАВИТЕЛИ ПРОГРАММЫ	10

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Cisco StealthWatch 6.9 Power Workshop (CSWPW)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 13.10.2014 N 716н "Об утверждении профессионального стандарта "Менеджер по информационным технологиям" (Зарегистрировано в Минюсте России 14.11.2014 N 34714), приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 18.11.2014 N 896н "Об утверждении профессионального стандарта "Специалист по информационным системам" (Зарегистрировано в Минюсте России 24.12.2014 N 35361).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Cisco StealthWatch 6.9 Power Workshop (CSWPW)» - научить слушателей работать с системой StealthWatch.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Cisco StealthWatch 6.9 Power Workshop (CSWPW)».

Слушатель должен уметь:

- обнаруживать угрозы с помощью Cisco StealthWatch;
- обнаруживать угрозы в режиме реального времени.

Слушатель должен знать:

- архитектуру Cisco StealthWatch;
- необходимые компоненты и лицензии.

Слушатель должен владеть:

- навыками реакции на инциденты безопасности.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 16 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации «Cisco StealthWatch 6.9 Power Workshop (CSWPW)»

Срок обучения: 16 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Модуль 1. Введение, обзор Cisco StealthWatch				Групповой опрос
1.1	Телеметрия сетевого трафика				
1.2	Основы протокола NetFlow				
1.3	NetFlow Security Event Logging (NSEL)				
1.4	Система StealthWatch				
1.5	Мониторинг сети				
2.	Модуль 2. Архитектура и компоненты системы				Групповой опрос
2.1.	Архитектура Cisco StealthWatch				
2.2.	Необходимые компоненты и лицензии				
2.3	Дополнительные компоненты и лицензии				
2.4	Identity				
3.	Модуль 3. Руководство по дизайну				Групповой опрос
3.1.	Обнаружение угроз с помощью Cisco StealthWatch				
3.2.	Модель тревоги				
3.3	События безопасности				
3.4	Категории оповещений				
3.5	Обнаружение угроз в режиме реального времени				
3.6	Реакция на инциденты безопасности				
	Всего:				
	Итоговый контроль знаний		0	0	Электронное тестирование
	Итого:	16			

2.2 Календарный учебный график

Занятия проводятся 2 раз в неделю по 8 академических часов (1 ак. час - 45 минут).

Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки	недели	1	
обучения	дни	1	1
Вид занятий		А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Cisco StealthWatch 6.9 Power Workshop (CSWPW)».

Учебно-тематический план

1. Модуль 1. Введение, обзор Cisco StealthWatch

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Модуль 1. Введение, обзор Cisco StealthWatch				
1.1	Телеметрия сетевого трафика				
1.2	Основы протокола NetFlow				
1.3	NetFlow Security Event Logging (NSEL)				
1.4	Система StealthWatch				
1.5	Мониторинг сети				
	ИТОГО				Групповой опрос

2. Модуль 2. Архитектура и компоненты системы

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Модуль 2. Архитектура и компоненты системы				
2.1.	Архитектура Cisco StealthWatch				
2.2.	Необходимые компоненты и лицензии				
2.3	Дополнительные компоненты и лицензии				
2.4	Identity				
	ИТОГО				Групповой опрос

3. Модуль 3. Руководство по дизайну

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Модуль 3. Руководство по дизайну				
3.1.	Обнаружение угроз с помощью Cisco StealthWatch				
3.2.	Модель тревоги				
3.3.	События безопасности				
3.4.	Категории оповещений				
3.5.	Обнаружение угроз в режиме реального времени				
3.6.	Реакция на инциденты безопасности				
	ИТОГО				Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Применение системы сетевой безопасности на базе
Cisco IOS (3.0) (IINS)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	4
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	5
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	7
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	11
3.1 Требования к педагогам	11
3.2 Материально-техническое оснащение программы	11
3.3 Учебно-методическое оснащение программы	11
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	11
V. СОСТАВИТЕЛИ ПРОГРАММЫ	12

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Применение системы сетевой безопасности на базе Cisco IOS (3.0) (PNS)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 19 мая 2014 года N 316н "Об утверждении профессионального стандарта "Инженер-проектировщик в области связи (телекоммуникаций) " (Зарегистрировано в Минюсте России 10 июля 2014 года, регистрационный N 33047), приказом Минтруда России от 18.11.2014 N 896н "Об утверждении профессионального стандарта "Специалист по информационным системам"(Зарегистрировано в Минюсте России 24.12.2014 N 35361), приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Применение системы сетевой безопасности на базе Cisco IOS (3.0) (IINS)» - обучить специалистов описывать общие концепции сетевой безопасности, защищать сетевые устройства, внедрять механизмы сетевой безопасности на втором уровне модели OSI, внедрять механизмы сетевой безопасности с помощью межсетевых экранов, внедрять VPN-технологии, описывать современные технологии и архитектуры безопасности.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Применение системы сетевой безопасности на базе Cisco IOS (3.0) (IINS)».

Слушатель должен уметь:

- настраивать AAA-сервисы и безопасных протоколов управления сетью;
- управлять межсетевыми экранами Cisco ASA;

Слушатель должен знать:

- механизмы сетевой безопасности второго уровня модели OSI;
- основы построения VPN.

Слушатель должен владеть:

- навыками построения VPN-сетей с использованием Cisco IOS и Cisco ASA.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Применение системы сетевой безопасности на базе Cisco IOS (3.0) (IINS)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,5	0,5	0	Групповой опрос
2.	Концепции сетевой безопасности	1	1	0	Групповой опрос
2.1.	Обзор криптографических технологий	1	1	0	
3.	Принципы защиты сетевых устройств	8	3,5	4,5	Групповой опрос
3.1.	Защита удаленного доступа, AAA-сервисы	1	1	0	
3.2.	Безопасные методы управления сетью	1,8	1,8	0	
3.3.	Защита протоколов маршрутизации	0,7	0,7	0	
3.4.	Лабораторная работа 1: Настройка AAA-сервисов и безопасного удаленного управления устройством	1,5	0	1,5	
3.5.	Лабораторная работа 2: Настройка безопасных протоколов управления сетью	2	0	2	
3.6.	Лабораторная работа 3: Настройка механизмов безопасности в протоколах динамической маршрутизации	1	0	1	
4.	Механизмы сетевой безопасности второго уровня модели OSI	6,8	3,3	3,5	Групповой опрос
4.1.	Безопасность VLAN	1,2	1,2	0	
4.2.	ACL на коммутаторах	0,7	0,7	0	
4.3.	Технология Port Security	0,5	0,5	0	
4.4.	Технология Private VLAN Edge	0,5	0,5	0	
4.5.	Методы защиты протоколов DHCP, ARP и STP	0,4	0,4	0	
4.6.	Лабораторная работа 4: Настройка элементов защиты сетевой инфраструктуры 2-го уровня модели OSI	2	0	2	
4.7.	Лабораторная работа 5: Настройка технологий DHCP Snooping и STP Protection	1,5	0	1,5	

5.	Основы работы межсетевых экранов	9,4	4,4	5	Групповой опрос
5.1.	Обзор технологий межсетевого экранирования	1,2	1,2	0	
5.2.	Интерфейсы Cisco ASA и технология NAT	1,3	1,3	0	
5.3.	Управление доступом на Cisco ASA	1	1	0	
5.4.	Обзор функций межсетевого экрана в Cisco IOS	0,9	0,9	0	
5.5.	Лабораторная работа 6: Настройка интерфейсов и NAT на Cisco ASA	2	0	2	
5.6.	Лабораторная работа 7: Настройка политик на Cisco ASA	3	0	3	
6.	Основы построения VPN	10,3	4,3	6	
6.1.	Обзор технологий стандарта IPsec	1,3	1,3	0	
6.2.	Построение Site-to-Site VPN с использованием Cisco IOS	0,7	0,7	0	
6.3.	Построение Site-to-Site VPN с использованием Cisco ASA	0,3	0,3	0	
6.4.	Remote Access VPN с использованием ASA и AnyConnect	1	1	0	
6.5.	Clientless Remote Access VPN на Cisco ASA (портал)	1	1	0	
6.6.	Лабораторная работа 8: Настройка Site-to-Site VPN с использованием Cisco IOS	2	0	2	
6.7.	Лабораторная работа 9: Настройка AnyConnect Remote Access VPN с использованием Cisco ASA	2	0	2	
6.8.	Лабораторная работа 10: Настройка Clientless SSL VPN с использованием Cisco ASA	2	0	2	
7.	Современные технологии и архитектуры безопасности	2	2	0	
7.1.	Обзор стандарта 802.1X	2	2	0	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Применение системы сетевой безопасности на базе Cisco IOS (3.0) (IINS)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,5	0,5	0	Групповой опрос

2. Концепции сетевой безопасности

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Концепции сетевой безопасности				
2.1	Обзор криптографических технологий	1	1	0	
	ИТОГО	1	1	0	Групповой опрос

3. Принципы защиты сетевых устройств

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Принципы защиты сетевых устройств				
3.1	Защита удаленного доступа, AAA-сервисы	1	1	0	
3.2	Безопасные методы управления сетью	1,8	1,8	0	
3.3	Защита протоколов маршрутизации	0,7	0,7	0	
3.4	Лабораторная работа 1: Настройка AAA-сервисов и безопасного удаленного управления устройством	1,5	0	1,5	
3.5	Лабораторная работа 2: Настройка безопасных протоколов управления сетью	2	0	2	

3.6	Лабораторная работа 3: Настройка механизмов безопасности в протоколах динамической маршрутизации	1	0	1	
	ИТОГО	8	3,5	4,5	Групповой опрос

4. Механизмы сетевой безопасности второго уровня модели OSI

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Механизмы сетевой безопасности второго уровня модели OSI				
4.1	Безопасность VLAN	1,2	1,2	0	
4.2.	ACL на коммутаторах	0,7	0,7	0	
4.3.	Технология Port Security	0,5	0,5	0	
4.4.	Технология Private VLAN Edge	0,5	0,5	0	
4.5	Методы защиты протоколов DHCP, ARP и STP	0,4	0,4	0	
4.6	Лабораторная работа 4: Настройка элементов защиты сетевой инфраструктуры 2-го уровня модели OSI	2	0	2	
4.7	Лабораторная работа 5: Настройка технологий DHCP Snooping и STP Protection	1,5	0	1,5	
	ИТОГО	6,8	3,3	3,5	Групповой опрос

5. Основы работы межсетевых экранов

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Основы работы межсетевых экранов				
5.1	Обзор технологий межсетевого экранирования	1,2	1,2	0	
5.2.	Интерфейсы Cisco ASA и технология NAT	1,3	1,3	0	
5.3	Управление доступом на Cisco ASA	1	1	0	
5.4	Обзор функций межсетевого экрана в Cisco IOS	0,9	0,9	0	
5.5	Лабораторная работа 6: Настройка интерфейсов и NAT на Cisco ASA	2	0	2	
5.6	Лабораторная работа 7: Настройка политик на Cisco ASA	3	0	3	
	ИТОГО	9,4	4,4	5	Групповой опрос

6. Основы построения VPN

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Основы построения VPN				
6.1	Обзор технологий стандарта IPsec	1,3	1,3	0	
6.2	Построение Site-to-Site VPN с использованием Cisco IOS	0,7	0,7	0	
6.3	Построение Site-to-Site VPN с использованием Cisco ASA	0,3	0,3	0	
6.4	Remote Access VPN с использованием ASA и AnyConnect	1	1	0	
6.5	Clientless Remote Access VPN на Cisco ASA (портал)	1	1	0	
6.6	Лабораторная работа 8: Настройка Site-to-Site VPN с использованием Cisco IOS	2	0	2	
6.7	Лабораторная работа 9: Настройка AnyConnect Remote Access VPN с использованием Cisco ASA	2	0	2	
6.8	Лабораторная работа 10: Настройка Clientless SSL VPN с использованием Cisco ASA	2	0	2	
	ВСЕГО	10,3	4,3	6	

7. Современные технологии и архитектуры безопасности

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
7.	Современные технологии и архитектуры безопасности				
7.1	Обзор стандарта 802.1X	2	2	0	
	ИТОГО	2	2	0	

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МИТ



**Дополнительная профессиональная программа
повышения квалификации**

**«Защита промышленных IoT сетей с помощью
технологий Cisco (ISECIN)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	4
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	5
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	8
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	12
3.1 Требования к педагогам	12
3.2 Материально-техническое оснащение программы	12
3.3 Учебно-методическое оснащение программы	12
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	12
V. СОСТАВИТЕЛИ ПРОГРАММЫ	13

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Защита промышленных IoT сетей с помощью технологий Cisco (ISECIN)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 11.04.2014 N 225н (ред. от 12.12.2016) "Об утверждении профессионального стандарта "Специалист по тестированию в области информационных технологий" (Зарегистрировано в Минюсте России 09.06.2014 N 32623), приказом Минтруда России от 19 мая 2014 года N 316н "Об утверждении профессионального стандарта "Инженер-проектировщик в области связи (телекоммуникаций) " (Зарегистрировано в Минюсте России 10 июля 2014 года, регистрационный N 33047), приказом Минтруда России от 19.05.2014 N 317н (ред. от 12.12.2016) "Об утверждении профессионального стандарта "Инженер технической поддержки в области связи (телекоммуникаций)" (Зарегистрировано в Минюсте России 09.06.2014 N 32619), приказом Минтруда России от 20.11.2014 N 915н (ред. от 12.12.2016) "Об утверждении профессионального стандарта "Менеджер продуктов в области информационных технологий" (Зарегистрировано в Минюсте России 18.12.2014 N 35273), приказом Минтруда России от 13.10.2014 N 716н "Об утверждении профессионального стандарта "Менеджер по информационным технологиям" (Зарегистрировано в Минюсте России 14.11.2014 N 34714), приказом Минтруда России от 18.11.2014 N 896н "Об утверждении профессионального стандарта "Специалист по информационным системам"(Зарегистрировано в Минюсте России 24.12.2014 N 35361), приказом Минтруда России от 31.10.2014 N 866н (ред. от 12.12.2016) "Об утверждении профессионального стандарта "Инженер связи (телекоммуникаций)" (Зарегистрировано в Минюсте России 28.11.2014 N 34971), приказом Минтруда России от 05.10.2015 N 688н "Об утверждении профессионального стандарта "Специалист по технической поддержке информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 22.10.2015 N 39412),

приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 05.10.2015 N 686н "Об утверждении профессионального стандарта "Специалист по администрированию сетевых устройств информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 30.10.2015 N 39568), приказом Минтруда России от 31.05.2017 N 465н "Об утверждении профессионального стандарта "Специалист по обслуживанию телекоммуникаций" (Зарегистрировано в Минюсте России 21.06.2017 N 47101).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Защита промышленных IoT сетей с помощью технологий Cisco (ISECIN)» - научить слушателей понимать архитектуру, компоненты и приложения конвергентных корпоративных и промышленных сетей, различать корпоративную ИТ и промышленную ИОТ безопасность, определять уровневые требования к безопасности от границы сети до я

д Для реализации цели программы необходимо решить комплекс задач:

Р • способствовать внедрению в учебный процесс современных эффективных а методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;

- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Т Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Р **Вид профессиональной деятельности:** Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В

Н

я

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Защита промышленных IoT сетей с помощью технологий Cisco (ISECIN)».

Слушатель должен уметь:

- защищать конечные станции и связь между ними как во время активности, так и во время покоя;
- бороться с часто встречающимися проблемами в IoT;

Слушатель должен знать:

- архитектуру, компоненты и приложения конвергентных корпоративных и промышленных сетей;
- протоколы, приложения и IPv6 для IoT.

Слушатель должен владеть:

- навыками определения уровневых требований к безопасности от границы сети до ядра и от уровня доступа до прикладного уровня.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является ***тест***.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Защита промышленных IoT сетей с помощью технологий Cisco (ISECIN)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Глава 1 – лекции ISECIN	38,0	19,0	19,0	Групповой опрос
1.1.	Описание конвергентных и промышленных IoT сетей, архитектур и фреймворков	1,4	1,4	0,0	
1.2.	Лабораторная работа: Исследование промышленной IoT сети	0,9	0,0	0,9	
1.3.	Описание требований к безопасности в промышленных IoT сетях	1,4	1,4	0,0	
1.4.	Лабораторная работа: Исследование компонентов промышленной IoT сети и выявление их требований к безопасности	0,9	0,0	0,9	
1.5.	Описание протоколов, использующихся в конвергированных корпоративных и промышленных IoT сетях	1,3	1,3	0,0	
1.6.	Лабораторная работа: Анализ трафика сетевых протоколов на 2 и 3 Уровнях в промышленных IoT сетях	1,0	0,0	1,0	
1.7.	Лабораторная работа: Анализ трафика протоколов OT	0,8	0,0	0,8	
1.8.	Анализ уязвимостей IoT	1,4	1,4	0,0	
1.9.	Лабораторная работа: Исследование элементов и обнаружение уязвимостей в промышленных IoT сетях	0,8	0,0	0,8	
1.10.	Исследование уязвимостей в промышленных IoT сетях	1,5	1,5	0,0	
1.11.	Лабораторная работа: Внесение паразитного устройства	1,0	0,0	1,0	
1.12.	Лабораторная работа: Проведение атаки на элемент OT	0,9	0,0	0,9	
1.13.	Лабораторная работа: Анализ атак на IoT сети	1,0	0,0	1,0	
1.14.	Описание процесса защиты	1,5	1,5	0,0	

	промышленных IoT сетей				
1.15.	Лабораторная работа: Классификация элементов и выявление взаимосвязей между элементами в промышленной IoT сети	0,9	0,0	0,9	
1.16.	Укрепление защиты устройств и описание физической безопасности в промышленных IoT сетях	1,4	1,4	0,0	
1.17.	Лабораторная работа: Внедрение безопасности на сетевом устройстве IoT	0,8	0,0	0,8	
1.18.	Внедрение защиты сетевой инфраструктуры в промышленной IoT сети	1,4	1,4	0,0	
1.19.	Лабораторная работа: Исследование функционала безопасности сетевой инфраструктуры на коммутаторах Cisco IE – часть 1	0,9	0,0	0,9	
1.20.	Лабораторная работа: Исследование функционала безопасности сетевой инфраструктуры на коммутаторах Cisco IE – часть 2	0,9	0,0	0,9	
1.21.	Описание характеристик NGFW в промышленных IoT сетях	1,3	1,3	0,0	
1.22.	Лабораторная работа: Внедрение NGFW в промышленных IoT сетях	0,9	0,0	0,9	
1.23.	Защита коммуникаций в промышленных IoT сетях с применением базового функционала NGFW и NGIPS	1,3	1,3	0,0	
1.24.	Лабораторная работа: Внедрение контроля доступа, прикладной инспекции и Unicast RPF на NGFW от Cisco	1,1	0,0	1,1	
1.25.	Лабораторная работа: Внедрение модуля Cisco FirePower с базовыми настройками	1,0	0,0	1,0	
1.26.	Внедрение продвинутых функций безопасности NGFW и NGIPS в промышленных IoT сетях	1,4	1,4	0,0	
1.27.	Лабораторная работа: Внедрение продвинутого контроля доступа и инспекции приложений OT в сегментах сети	0,9	0,0	0,9	
1.28.	Применение решения Cisco TrustSec в промышленной IoT сети	1,5	1,5	0,0	
1.29.	Лабораторная работа: Применение 802.1x на промышленных	0,9	0,0	0,9	

	коммутаторах				
1.30.	Лабораторная работа: Внедрение SGT на промышленных коммутаторах	0,9	0,0	0,9	
1.31.	Внедрение VPN решений в промышленных IoT сетях	1,3	1,3	0,0	
1.32.	Лабораторная работа: Внедрение RA VPN для управления промышленной IoT сетью	1,0	0,0	1,0	
1.33.	Фреймворки и регулирование в области защиты промышленных IoT сетей	0,9	0,9	0,0	
1.34.	Лабораторная работа: Исследование компонентов промышленной IoT сети и выявление применимых стандартов и требований безопасности	1,5	0,0	1,5	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Защита промышленных IoT сетей с помощью технологий Cisco (ISECIN)».

Учебно-тематический план

1. Глава 1 – лекции ISECIN

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	

1.	Глава 1 – лекции ISECIN				
1.1.	Описание конвергентных и промышленных IoT сетей, архитектур и фреймворков	1,4	1,4	0,0	
1.2.	Лабораторная работа: Исследование промышленной IoT сети	0,9	0,0	0,9	
1.3.	Описание требований к безопасности в промышленных IoT сетях	1,4	1,4	0,0	
1.4.	Лабораторная работа: Исследование компонентов промышленной IoT сети и выявление их требований к безопасности	0,9	0,0	0,9	
1.5.	Описание протоколов, использующихся в конвергированных корпоративных и промышленных IoT сетях	1,3	1,3	0,0	
1.6.	Лабораторная работа: Анализ трафика сетевых протоколов на 2 и 3 Уровнях в промышленных IoT сетях	1,0	0,0	1,0	
1.7.	Лабораторная работа: Анализ трафика протоколов OT	0,8	0,0	0,8	
1.8.	Анализ уязвимостей IoT	1,4	1,4	0,0	
1.9.	Лабораторная работа: Исследование элементов и обнаружение уязвимостей в промышленных IoT сетях	0,8	0,0	0,8	
1.10.	Исследование уязвимостей в промышленных IoT сетях	1,5	1,5	0,0	
1.11.	Лабораторная работа: Внесение паразитного устройства	1,0	0,0	1,0	
1.12.	Лабораторная работа: Проведение атаки на элемент OT	0,9	0,0	0,9	
1.13.	Лабораторная работа: Анализ атак на IoT сети	1,0	0,0	1,0	
1.14.	Описание процесса защиты промышленных IoT сетей	1,5	1,5	0,0	
1.15.	Лабораторная работа: Классификация элементов и выявление взаимосвязей между элементами в промышленной IoT сети	0,9	0,0	0,9	
1.16.	Укрепление защиты устройств и описание физической безопасности в промышленных IoT сетях	1,4	1,4	0,0	
1.17.	Лабораторная работа: Внедрение безопасности на сетевом устройстве IoT	0,8	0,0	0,8	
1.18.	Внедрение защиты сетевой инфраструктуры в промышленной IoT	1,4	1,4	0,0	

	сети				
1.19.	Лабораторная работа: Исследование функционала безопасности сетевой инфраструктуры на коммутаторах Cisco IE – часть 1	0,9	0,0	0,9	
1.20.	Лабораторная работа: Исследование функционала безопасности сетевой инфраструктуры на коммутаторах Cisco IE – часть 2	0,9	0,0	0,9	
1.21.	Описание характеристик NGFW в промышленных IoT сетях	1,3	1,3	0,0	
1.22.	Лабораторная работа: Внедрение NGFW в промышленных IoT сетях	0,9	0,0	0,9	
1.23.	Защита коммуникаций в промышленных IoT сетях с применением базового функционала NGFW и NGIPS	1,3	1,3	0,0	
1.24.	Лабораторная работа: Внедрение контроля доступа, прикладной инспекции и Unicast RPF на NGFW от Cisco	1,1	0,0	1,1	
1.25.	Лабораторная работа: Внедрение модуля Cisco FirePower с базовыми настройками	1,0	0,0	1,0	
1.26.	Внедрение продвинутых функций безопасности NGFW и NGIPS в промышленных IoT сетях	1,4	1,4	0,0	
1.27.	Лабораторная работа: Внедрение продвинутого контроля доступа и инспекции приложений OT в сегментах сети	0,9	0,0	0,9	
1.28.	Применение решения Cisco TrustSec в промышленной IoT сети	1,5	1,5	0,0	
1.29.	Лабораторная работа: Применение 802.1x на промышленных коммутаторах	0,9	0,0	0,9	
1.30.	Лабораторная работа: Внедрение SGT на промышленных коммутаторах	0,9	0,0	0,9	
1.31.	Внедрение VPN решений в промышленных IoT сетях	1,3	1,3	0,0	
1.32.	Лабораторная работа: Внедрение RA VPN для управления промышленной IoT сетью	1,0	0,0	1,0	
1.33.	Фреймворки и регулирование в области защиты промышленных IoT сетей	0,9	0,9	0,0	
1.34.	Лабораторная работа: Исследование компонентов промышленной IoT сети	1,5	0,0	1,5	

	и выявление применимых стандартов и требований безопасности				
	ИТОГО	38,0	19,0	19,0	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Реализация повышенной сетевой защиты с
использованием Cisco ASA (SASAA)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	4
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	6
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	12
3.1 Требования к педагогам	12
3.2 Материально-техническое оснащение программы	12
3.3 Учебно-методическое оснащение программы	12
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	12
V. СОСТАВИТЕЛИ ПРОГРАММЫ	13

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Реализация повышенной сетевой защиты с использованием Cisco ASA (SASAA)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Реализация повышенной сетевой защиты с использованием Cisco ASA (SASAA)» - обеспечить слушателей теоретическими знаниями и практическими навыками по развертыванию, продвинутой настройке и управлению расширенными функциями Cisco

Adaptive Security Appliance (ASA).

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Реализация повышенной сетевой защиты с использованием Cisco ASA (SASAA)».

Слушатель должен уметь:

- внедрять новый функционал в ASA 9.3 и 9.4;
- настраивать механизмы ASA Identity Firewall;
- настраивать кластеры Cisco ASA.

Слушатель должен знать:

- устройство брандмауэров Cisco ASA 5500-X;
- сервисы Cisco ASA Firepower на платформах 5506-X, 5508-X и 5516-X.

Слушатель должен владеть:

- навыками по развертыванию, продвинутой настройке и управлению расширенными функциями Cisco Adaptive Security Appliance.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Реализация повышенной сетевой защиты с использованием Cisco ASA (SASAA)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,4	0,4	0,0	Групповой опрос
2.	Семейство продуктов Cisco ASA	8,8	2,4	6,4	Групповой опрос
2.1.	Знакомство с брандмауэрами нового поколения ASA 5500-X	0,8	0,8	0,0	
2.2.	Обзор ASA v	0,5	0,5	0,0	
2.3.	Внедрение новых возможностей ASA версий 9.3 и 9.4.1	0,6	0,6	0,0	
2.4.	Установка и настройка Cisco ASA Service Module (Cisco ASASM)	0,5	0,5	0,0	
2.5.	Лабораторная работа 1: Доступ к интерфейсу лабораторных работ	2,1	0,0	2,1	
2.6.	Лабораторная работа 2: Установка и проверка работоспособности ASA v	2,2	0,0	2,2	
2.7.	Лабораторная работа 3: Внедрение нового функционала в ASA 9.3 и 9.4	2,1	0,0	2,1	
3.	Cisco ASA Identity Firewall	7,1	3,0	4,1	Групповой опрос
3.1.	Описание решения ASA Identity Firewall	0,5	0,5	0,0	
3.2.	Установка CDA Cisco	0,6	0,6	0,0	
3.3.	Настройка CDA Cisco	0,6	0,6	0,0	
3.4.	Настройка механизмы ASA Identity Firewall	0,7	0,7	0,0	
3.5.	Проверка и устранение неполадок в работе механизма ASA Identity Firewall	0,6	0,6	0,0	
3.6.	Лабораторная работа 4: Настройка Cisco CDA	2,1	0,0	2,1	
3.7.	Лабораторная работа 5: Настройка ASA IDFW	2,0	0,0	2,0	
4.	Обзор решения Cisco ASA Firepower	6,5	2,3	4,2	Групповой опрос
4.1.	Установка модуля Cisco ASA	0,7	0,7	0,0	

	Firepower				
4.2.	Управление модулем Cisco ASA Firepower с использованием централизованной платформы Cisco FireSIGHT	0,5	0,5	0,0	
4.3.	Описание сервисов Cisco ASA Firepower на платформах 5506-X, 5508-X и 5516-X	0,6	0,6	0,0	
4.4.	Настройка новых функций в Cisco ASA Firepower Services версии 6.0	0,5	0,5	0,0	
4.5.	Лабораторная работа 6: Установка модуля Cisco ASA Firepower	2,1	0,0	2,1	
4.6.	Лабораторная работа 7: Настройка FPSc помощью платформы Cisco Firepower Management Center	2,1	0,0	2,1	
5.	Архитектура Cisco ASA Cloud Web Security (CWS)	4,8	2,8	2,0	Групповой опрос
5.1.	Знакомство с решением Cisco ASA Cisco Cloud Web Security	0,4	0,4	0,0	
5.2.	Интеграция ASA с CWS	0,5	0,5	0,0	
5.3.	Проверка работы архитектуры Cisco ASA Cloud Web Security	0,6	0,6	0,0	
5.4.	Описание политики веб-фильтрации в Cisco ScanCenter	0,6	0,6	0,0	
5.5.	Описание функционала ASA CWS AMP и CTA	0,7	0,7	0,0	
5.6.	Лабораторная работа 8: Настройка механизмов ASA CWS	2,0	0,0	2,0	
6.	Кластеризация Cisco ASA	6,9	4,6	2,3	Групповой опрос
6.1.	Описание функций кластера Cisco ASA	0,6	0,6	0,0	
6.2.	Описание терминологии кластеров Cisco ASA и потоков данных	0,8	0,8	0,0	
6.3.	Использование CLI для настройки кластера Cisco ASA	0,6	0,6	0,0	
6.4.	Использование Cisco ASDM для настройки кластера Cisco ASA	0,5	0,5	0,0	
6.5.	Проверка работоспособности кластера Cisco ASA	0,7	0,7	0,0	
6.6.	Устранение неполадок в работе кластера Cisco ASA	0,7	0,7	0,0	
6.7.	Описание возможностей и функций при кластеризации Cisco ASA версии 9.1.4 и более поздних	0,7	0,7	0,0	
6.8.	Лабораторная работа 9: Настройка кластера Cisco ASA	2,3	0,0	2,3	

7.	Cisco ASA Security Group Firewall и механизм Change of Authorization (дополнительно)	3,5	3,5	0,0	Групповой опрос
7.1.	Знакомство с Cisco Security Group Tag	0,4	0,4	0,0	
7.2.	Настройка SG Firewall	0,7	0,7	0,0	
7.3.	Описание возможностей SGT в ASA 9.2.1 и более поздних версий	0,5	0,5	0,0	
7.4.	Описание Change of Authorization (CoA) ASA 9.2.1 и более поздних версий	1,9	1,9	0,0	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Реализация повышенной сетевой защиты с использованием Cisco ASA (SASAA)».
Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,4	0,4	0,0	Групповой опрос

2. Семейство продуктов Cisco ASA

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Семейство продуктов Cisco ASA				

2.1	Знакомство с брандмауэрами нового поколения ASA 5500-X	0,8	0,8	0,0	
2.2	Обзор ASAv	0,5	0,5	0,0	
2.3	Внедрение новых возможностей ASA версий 9.3 и 9.4.1	0,6	0,6	0,0	
2.4	Установка и настройка Cisco ASA Service Module (Cisco ASASM)	0,5	0,5	0,0	
2.5	Лабораторная работа 1: Доступ к интерфейсу лабораторных работ	2,1	0,0	2,1	
2.6	Лабораторная работа 2: Установка и проверка работоспособности ASAv	2,2	0,0	2,2	
2.7	Лабораторная работа 3: Внедрение нового функционала в ASA 9.3 и 9.4	2,1	0,0	2,1	
	ИТОГО	8,8	2,4	6,4	Групповой опрос

3. Cisco ASA Identity Firewall

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Cisco ASA Identity Firewall				
3.1	Описание решения ASA Identity Firewall	0,5	0,5	0,0	
3.2	Установка CDA Cisco	0,6	0,6	0,0	
3.3	Настройка CDA Cisco	0,6	0,6	0,0	
3.4	Настройка механизмы ASA Identity Firewall	0,7	0,7	0,0	
3.5	Проверка и устранение неполадок в работе механизма ASA Identity Firewall	0,6	0,6	0,0	
3.6	Лабораторная работа 4: Настройка Cisco CDA	2,1	0,0	2,1	
3.7	Лабораторная работа 5: Настройка ASA IDFW	2,0	0,0	2,0	
	ИТОГО	7,1	3,0	4,1	Групповой опрос

4. Обзор решения Cisco ASA Firepower

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Обзор решения Cisco ASA Firepower				
4.1	Установка модуля Cisco ASA Firepower	0,7	0,7	0,0	
4.2	Управление модулем Cisco ASA Firepower с использованием централизованной платформы Cisco	0,5	0,5	0,0	

	FireSIGHT				
4.3.	Описание сервисов Cisco ASA Firepower на платформах 5506-X, 5508-X и 5516-X	0,6	0,6	0,0	
4.4.	Настройка новых функций в Cisco ASA Firepower Services версии 6.0	0,5	0,5	0,0	
4.5.	Лабораторная работа 6: Установка модуля Cisco ASA Firepower	2,1	0,0	2,1	
4.6	Лабораторная работа 7: Настройка FPSc помощью платформы Cisco Firepower Management Center	2,1	0,0	2,1	
	ИТОГО	6,5	2,3	4,2	Групповой опрос

5. Архитектура Cisco ASA Cloud Web Security (CWS)

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Архитектура Cisco ASA Cloud Web Security (CWS)				
5.1	Знакомство с решением Cisco ASA Cisco Cloud Web Security	0,4	0,4	0,0	
5.2	Интеграция ASA с CWS	0,5	0,5	0,0	
5.3	Проверка работы архитектуры Cisco ASA Cloud Web Security	0,6	0,6	0,0	
5.4	Описание политики веб-фильтрации в Cisco ScanCenter	0,6	0,6	0,0	
5.5	Описание функционала ASA CWS AMP и CTA	0,7	0,7	0,0	
5.6	Лабораторная работа 8: Настройка механизмов ASA CWS	2,0	0,0	2,0	
	ИТОГО	4,8	2,8	2,0	Групповой опрос

6. Кластеризация Cisco ASA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Кластеризация Cisco ASA				
6.1	Описание функций кластера Cisco ASA	0,6	0,6	0,0	
6.2	Описание терминологии кластеров Cisco ASA и потоков данных	0,8	0,8	0,0	
6.3	Использование CLI для настройки кластера Cisco ASA	0,6	0,6	0,0	
6.4	Использование Cisco ASDM для настройки кластера Cisco ASA	0,5	0,5	0,0	
6.5	Проверка работоспособности кластера	0,7	0,7	0,0	

	Cisco ASA				
6.6	Устранение неполадок в работе кластера Cisco ASA	0,7	0,7	0,0	
6.7	Описание возможностей и функций при кластеризации Cisco ASA версии 9.1.4 и более поздних	0,7	0,7	0,0	
6.8	Лабораторная работа 9: Настройка кластера Cisco ASA	2,3	0,0	2,3	
	ВСЕГО	6,9	4,6	2,3	Групповой опрос

7. Cisco ASA Security Group Firewall и механизм Change of Authorization

(дополнительно)

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
7.	Cisco ASA Security Group Firewall и механизм Change of Authorization (дополнительно)				
7.1	Знакомство с Cisco Security Group Tag	0,4	0,4	0,0	
7.2	Настройка SG Firewall	0,7	0,7	0,0	
7.3	Описание возможностей SGT в ASA 9.2.1 и более поздних версий	0,5	0,5	0,0	
7.4	Описание Change of Authorization (CoA) ASA 9.2.1 и более поздних версий	1,9	1,9	0,0	
	ИТОГО	3,5	3,5	0,0	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Внедрение основного функционала Cisco ASA для
обеспечения безопасности сети передачи данных
(SASAC)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	4
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	6
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	13
3.1 Требования к педагогам	13
3.2 Материально-техническое оснащение программы	13
3.3 Учебно-методическое оснащение программы	13
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	13
V. СОСТАВИТЕЛИ ПРОГРАММЫ	14

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Внедрение основного функционала Cisco ASA для обеспечения безопасности сети передачи данных (SASAC)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Внедрение основного функционала Cisco ASA для обеспечения безопасности сети передачи данных (SASAC)» - обеспечить слушателей знаниями и навыками по развертыванию, базовой настройке и управлению функциями межсетевого экрана Cisco

Adaptive Security Appliance (ASA).

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Внедрение основного функционала Cisco ASA для обеспечения безопасности сети передачи данных (SASAC)».

Слушатель должен уметь:

- проводить базовую настройку Cisco ASA;
- развертывать VPN-сети Cisco AnyConnect на Cisco ASA;
- настраивать отказоустойчивость различных конфигураций Cisco ASA.

Слушатель должен знать:

- принципы лицензирования Cisco ASA;
- различия моделей устройств Cisco ASA.

Слушатель должен владеть:

- навыками развертывания отказоустойчивых и защищенных VPN-сетей Cisco.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Внедрение основного функционала Cisco ASA для обеспечения безопасности
сети передачи данных (SASAC)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,8	0,8	0,0	Групповой опрос
2.	Обзор функционала Cisco ASA	3,5	1,9	1,6	Групповой опрос
2.1.	Развитие технологий межсетевого экранирования	0,6	0,6	0,0	
2.2.	Описание моделей устройств Cisco ASA	0,7	0,7	0,0	
2.3.	Принципы лицензирования Cisco ASA Adaptive Security Appliance	0,6	0,6	0,0	
2.4.	Лабораторная работа 1: Доступ к удаленной лабораторной среде	1,6	0,0	1,6	
3.	Базовые возможности подключения к сети и управление устройством	2,9	1,4	1,5	Групповой опрос
3.1.	Подготовка Cisco ASA для сетевой интеграции	0,7	0,7	0,0	
3.2.	Управление базовыми сетевыми настройками Cisco ASA	0,7	0,7	0,0	
3.3.	Лабораторная работа 2: Базовая настройка Cisco ASA	1,5	0,0	1,5	
4.	Сетевая интеграция	4,8	2,0	2,8	Групповой опрос
4.1.	Настройка функций NAT на устройстве Cisco ASA	0,6	0,6	0,0	
4.2.	Лабораторная работа 3: Настройка NAT	1,3	0,0	1,3	
4.3.	Настройка функций контроля доступа на Cisco ASA	0,6	0,6	0,0	
4.4.	Лабораторная работа 4: Настройка основных функций контроля доступа Cisco ASA	1,5	0,0	1,5	
4.5.	Настройка функций маршрутизации Cisco Adaptive Security Appliance	0,8	0,8	0,0	
5.	Элементы управления политикой	4,3	1,4	2,9	Групповой

	безопасности Cisco ASA				опрос
5.1.	Обзор механизма Cisco ASA MPF	0,6	0,6	0,0	
5.2.	Лабораторная работа 5: Конфигурирование MPF, Basic Stateful Inspections и QoS	1,5	0,0	1,5	
5.3.	Настройка расширенной проверки приложений на Cisco ASA	0,8	0,8	0,0	
5.4.	Лабораторная работа 6: Настройка расширенных проверок приложений MPF	1,4	0,0	1,4	
6.	Обзор VPN-компонентов для Cisco ASA	1,8	1,8	0,0	Групповой опрос
6.1.	Обзор технологий VPN	0,5	0,5	0,0	
6.2.	Реализация профилей, групповых политик и пользовательских политик	0,7	0,7	0,0	
6.3.	Внедрение сервисов PKI	0,6	0,6	0,0	
7.	Clientless VPN-доступ (портал)	7,7	3,3	4,4	Групповой опрос
7.1.	Внедрение Clientless SSL VPN	0,9	0,9	0,0	
7.2.	Развертывание базового Clientless SSL VPN на Cisco ASA	0,8	0,8	0,0	
7.3.	Лабораторная работа 7: Внедрение базового Clientless SSL VPN в Cisco ASA	1,5	0,0	1,5	
7.4.	Внедрение доступа к приложениям в Cisco ASA Clientless SSL VPN	0,8	0,8	0,0	
7.5.	Лабораторная работа 8: Настройка доступа к приложениям для Clientless SSL VPN в Cisco ASA	1,4	0,0	1,4	
7.6.	Развертывание внешней аутентификации и авторизации для клиента, подключающегося через портал	0,8	0,8	0,0	
7.7.	Лабораторная работа 9: Внедрение внешней аутентификации и авторизации в Clientless SSL VPN	1,5	0,0	1,5	
8.	VPN в режиме Full Tunnel для решения Cisco AnyConnect	7,7	3,0	4,7	Групповой опрос
8.1.	Развертывание базовой VPN-сети Cisco AnyConnect SSL на Cisco ASA	0,6	0,6	0,0	
8.2.	Лаборатория 10: Внедрение базового Cisco AnyConnect SSL VPN на Cisco ASA	1,5	0,0	1,5	
8.3.	Развертывание дополнительных функций Cisco AnyConnect SSL VPN на Cisco ASA	0,8	0,8	0,0	
8.4.	Развертывание расширенной	0,7	0,7	0,0	

	аутентификации и авторизации в VPN-сетях Cisco AnyConnect				
8.5.	Лабораторная работа 11: Настройка расширенной аутентификации и авторизации в Cisco AnyConnect VPN	1,6	0,0	1,6	
8.6.	Развертывание IPsec/IKEv2 VPN-сетей Cisco AnyConnect	0,9	0,9	0,0	
8.7.	Лабораторная работа 12: Развертывание IPsec/IKEv2 VPN-сетей Cisco AnyConnect	1,6	0,0	1,6	
9.	Принципы отказоустойчивости и виртуализация для Cisco ASA	4,5	3,4	1,1	Групповой опрос
9.1.	Настройка функций резервирования интерфейса Cisco ASA	0,7	0,7	0,0	
9.2.	Настройка отказоустойчивой пары Cisco ASA Active/Standby	0,6	0,6	0,0	
9.3.	Настройка контекстов безопасности в Cisco ASA	0,7	0,7	0,0	
9.4.	Лабораторная работа 13: настройка механизмов Active/Standby	1,1	0,0	1,1	
9.5.	Настройка отказоустойчивой пары Cisco ASA Active/ Active (дополнительно)	1,4	1,4	0,0	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Внедрение основного функционала Cisco ASA для обеспечения безопасности сети передачи данных (SASAC)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,8	0,8	0,0	Групповой опрос

2. Обзор функционала Cisco ASA

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Обзор функционала Cisco ASA				
2.1	Развитие технологий межсетевого экранирования	0,6	0,6	0,0	
2.2	Описание моделей устройств Cisco ASA	0,7	0,7	0,0	
2.3	Принципы лицензирования Cisco ASA Adaptive Security Appliance	0,6	0,6	0,0	
2.4	Лабораторная работа 1: Доступ к удаленной лабораторной среде	1,6	0,0	1,6	
	ИТОГО	3,5	1,9	1,6	Групповой опрос

3. Базовые возможности подключения к сети и управление устройством

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Базовые возможности подключения к сети и управление устройством				
3.1	Подготовка Cisco ASA для сетевой интеграции	0,7	0,7	0,0	
3.2	Управление базовыми сетевыми настройками Cisco ASA	0,7	0,7	0,0	
3.3	Лабораторная работа 2: Базовая настройка Cisco ASA	1,5	0,0	1,5	
	ИТОГО	2,9	1,4	1,5	Групповой опрос

4. Сетевая интеграция

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	

4.	Сетевая интеграция				
4.1	Настройка функций NAT на устройстве Cisco ASA	0,6	0,6	0,0	
4.2	Лабораторная работа 3: Настройка NAT	1,3	0,0	1,3	
4.3	Настройка функций контроля доступа на Cisco ASA	0,6	0,6	0,0	
4.4	Лабораторная работа 4: Настройка основных функций контроля доступа Cisco ASA	1,5	0,0	1,5	
4.5	Настройка функций маршрутизации Cisco Adaptive Security Appliance	0,8	0,8	0,0	
	ИТОГО	4,8	2,0	2,8	Групповой опрос

5. Элементы управления политикой безопасности Cisco ASA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Элементы управления политикой безопасности Cisco ASA				
5.1	Обзор механизма Cisco ASA MPF	0,6	0,6	0,0	
5.2	Лабораторная работа 5: Конфигурирование MPF, Basic Stateful Inspections и QoS	1,5	0,0	1,5	
5.3	Настройка расширенной проверки приложений на Cisco ASA	0,8	0,8	0,0	
5.4	Лабораторная работа 6: Настройка расширенных проверок приложений MPF	1,4	0,0	1,4	
	ИТОГО	4,3	1,4	2,9	Групповой опрос

6. Обзор VPN-компонентов для Cisco ASA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Обзор VPN-компонентов для Cisco ASA				
6.1	Обзор технологий VPN	0,5	0,5	0,0	
6.2	Реализация профилей, групповых политик и пользовательских политик	0,7	0,7	0,0	
6.3	Внедрение сервисов PKI	0,6	0,6	0,0	
	ВСЕГО	1,8	1,8	0,0	Групповой опрос

7. Clientless VPN-доступ (портал)

№	Наименование разделов и тем	Всего	В том числе	Форма
---	-----------------------------	-------	-------------	-------

тема		часов	лекции	практические занятия	контроля
7.	Clientless VPN-доступ (портал)				
7.1	Внедрение Clientless SSL VPN	0,9	0,9	0,0	
7.2	Развертывание базового Clientless SSL VPN на Cisco ASA	0,8	0,8	0,0	
7.3	Лабораторная работа 7: Внедрение базового Clientless SSL VPN в Cisco ASA	1,5	0,0	1,5	
7.4	Внедрение доступа к приложениям в Cisco ASA Clientless SSL VPN	0,8	0,8	0,0	
7.5	Лабораторная работа 8: Настройка доступа к приложениям для Clientless SSL VPN в Cisco ASA	1,4	0,0	1,4	
7.6	Развертывание внешней аутентификации и авторизации для клиента, подключающегося через портал	0,8	0,8	0,0	
7.7	Лабораторная работа 9: Внедрение внешней аутентификации и авторизации в Clientless SSL VPN	1,5	0,0	1,5	
	ИТОГО	7,7	3,3	4,4	Групповой опрос

8. VPN в режиме Full Tunnel для решения Cisco AnyConnect

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
8.	VPN в режиме Full Tunnel для решения Cisco AnyConnect				
8.1	Развертывание базовой VPN-сети Cisco AnyConnect SSL на Cisco ASA	0,6	0,6	0,0	
8.2	Лаборатория 10: Внедрение базового Cisco AnyConnect SSL VPN на Cisco ASA	1,5	0,0	1,5	
8.3	Развертывание дополнительных функций Cisco AnyConnect SSL VPN на Cisco ASA	0,8	0,8	0,0	
8.4	Развертывание расширенной аутентификации и авторизации в VPN-сетях Cisco AnyConnect	0,7	0,7	0,0	
8.5	Лабораторная работа 11: Настройка расширенной аутентификации и авторизации в Cisco AnyConnect VPN	1,6	0,0	1,6	
8.6	Развертывание IPsec/IKEv2 VPN-сетей Cisco AnyConnect	0,9	0,9	0,0	
8.7	Лабораторная работа 12: Развертывание IPsec/IKEv2 VPN-сетей	1,6	0,0	1,6	

	Cisco AnyConnect				
	ИТОГО	7,7	3,0	4,7	Групповой опрос

9. Принципы отказоустойчивости и виртуализация для Cisco ASA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
9.	Принципы отказоустойчивости и виртуализация для Cisco ASA				
9.1	Настройка функций резервирования интерфейса Cisco ASA	0,7	0,7	0,0	
9.2	Настройка отказоустойчивой пары Cisco ASA Active/Standby	0,6	0,6	0,0	
9.3	Настройка контекстов безопасности в Cisco ASA	0,7	0,7	0,0	
9.4	Лабораторная работа 13: настройка механизмов Active/Standby	1,1	0,0	1,1	
9.5	Настройка отказоустойчивой пары Cisco ASA Active/ Active (дополнительно)	1,4	1,4	0,0	
	ИТОГО	4,5	3,4	1,1	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

М.П.



**Дополнительная профессиональная программа
повышения квалификации**

**«Изучение принципов кибер-безопасности Cisco
(SECFND)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	4
1.5 Трудоемкость обучения	4
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	7
2.3 Рабочая программа учебных предметов	7
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	10
3.1 Требования к педагогам	10
3.2 Материально-техническое оснащение программы	10
3.3 Учебно-методическое оснащение программы	10
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	10
V. СОСТАВИТЕЛИ ПРОГРАММЫ	11

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Изучение принципов кибер-безопасности Cisco (SECFND)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 28.10.2014 N 809н (ред. от 12.12.2016) "Об утверждении профессионального стандарта "Системный аналитик" (Зарегистрировано в Минюсте России 24.11.2014 N 34882), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Изучение принципов кибер-безопасности Cisco (SECFND)» - познакомить слушателей с основами администрирования Центров Управления Безопасностью (SOC - Security Operations Centers).

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Изучение принципов кибер-безопасности Cisco (SECFND)».

Слушатель должен уметь:

- описать концепции информационной безопасности;
- анализировать события информационной безопасности.

Слушатель должен знать:

- принципы сетевых атак;
- базовые принципы криптографии.

Слушатель должен владеть:

- навыками мониторинга событий информационной безопасности.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Изучение принципов кибер-безопасности Cisco (SECFND)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	1,2	1,2	0,0	Групповой опрос
2.	Знакомство с сетями TCP/IP и основами криптографии	12,5	4,9	7,6	Групповой опрос
2.1.	Знакомство со стеком протоколов TCP/IP	1,3	1,3	0,0	
2.2.	Общее представление о сетевой инфраструктуре	1,4	1,4	0,0	
2.3.	Понимание принципов сетевых атак	1,1	1,1	0,0	
2.4.	Знакомство с базовыми принципами криптографии	1,1	1,1	0,0	
2.5.	Лабораторная работа 1: Исследование стека протоколов TCP/IP	1,9	0,0	1,9	
2.6.	Лабораторная работа 2: Исследование сетевой инфраструктуры	1,9	0,0	1,9	
2.7.	Лабораторная работа 3: Исследование основных распространенных атак на стек TCP/IP	2,0	0,0	2,0	
2.8.	Лабораторная работа 4: Знакомство с базовыми принципами криптографии	1,8	0,0	1,8	
3.	Сетевые приложения и защита оконечных устройств	19,8	10,1	9,7	Групповой опрос
3.1.	Описание концепций информационной безопасности	1,3	1,3	0,0	
3.2.	Знакомство с сетевыми приложениями	1,3	1,3	0,0	
3.3.	Понимание основных атак, связанных с работой сетевых приложений	1,3	1,3	0,0	
3.4.	Знакомство с основами операционной системы Windows	1,4	1,4	0,0	
3.5.	Знакомство с основами операционной системы Linux	1,3	1,3	0,0	
3.6.	Знакомство с основными атаками на оконечные устройства	1,2	1,2	0,0	
3.7.	Представление о сетевых технологиях защиты	1,1	1,1	0,0	
3.8.	Изучение технологий защиты	1,2	1,2	0,0	

	оконечных устройств				
3.9.	Лабораторная работа 5: Исследование сетевых приложений	2,0	0,0	2,0	
3.10.	Лабораторная работа 6: Исследование основных атак, связанных с работой сетевых приложений	1,9	0,0	1,9	
3.11.	Лабораторная работа 7: ОС Windows	1,8	0,0	1,8	
3.12.	Лабораторная работа 8: ОС Linux	2,1	0,0	2,1	
3.13.	Лабораторная работа 9: Атаки на конечные устройства	1,9	0,0	1,9	
4.	Мониторинг и анализ безопасности	4,5	2,8	1,7	Групповой опрос
4.1.	Описание механизмов сбора данных о безопасности	1,4	1,4	0,0	
4.2.	Рассмотрение процесса анализа события информационной безопасности	1,4	1,4	0,0	
4.3.	Лабораторная работа 10: Мониторинг событий информационной безопасности	1,7	0,0	1,7	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Изучение принципов кибер-безопасности Cisco (SECFND)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	1,2	1,2	0,0	Групповой опрос

2. Знакомство с сетями TCP/IP и основами криптографии

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Знакомство с сетями TCP/IP и основами криптографии				
2.1.	Знакомство со стеком протоколов TCP/IP	1,3	1,3	0,0	
2.2.	Общее представление о сетевой инфраструктуре	1,4	1,4	0,0	
2.3.	Понимание принципов сетевых атак	1,1	1,1	0,0	
2.4.	Знакомство с базовыми принципами криптографии	1,1	1,1	0,0	
2.5.	Лабораторная работа 1: Исследование стека протоколов TCP/IP	1,9	0,0	1,9	
2.6.	Лабораторная работа 2: Исследование сетевой инфраструктуры	1,9	0,0	1,9	
2.7.	Лабораторная работа 3: Исследование основных распространенных атак на стек TCP/IP	2,0	0,0	2,0	
2.8	Лабораторная работа 4: Знакомство с базовыми принципами криптографии	1,8	0,0	1,8	
	ИТОГО	12,5	4,9	7,6	Групповой опрос

3. Сетевые приложения и защита оконечных устройств

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Сетевые приложения и защита оконечных устройств				
3.1.	Описание концепций информационной безопасности	1,3	1,3	0,0	
3.2.	Знакомство с сетевыми приложениями	1,3	1,3	0,0	
3.3.	Понимание основных атак, связанных с работой сетевых приложений	1,3	1,3	0,0	
3.4.	Знакомство с основами операционной системы Windows	1,4	1,4	0,0	
3.5.	Знакомство с основами операционной системы Linux	1,3	1,3	0,0	

3.6.	Знакомство с основными атаками на оконечные устройства	1,2	1,2	0,0	
3.7.	Представление о сетевых технологиях защиты	1,1	1,1	0,0	
3.8.	Изучение технологий защиты оконечных устройств	1,2	1,2	0,0	
3.9.	Лабораторная работа 5: Исследование сетевых приложений	2,0	0,0	2,0	
3.10.	Лабораторная работа 6: Исследование основных атак, связанных с работой сетевых приложений	1,9	0,0	1,9	
3.11.	Лабораторная работа 7: ОС Windows	1,8	0,0	1,8	
3.12.	Лабораторная работа 8: ОС Linux	2,1	0,0	2,1	
3.13.	Лабораторная работа 9: Атаки на конечные устройства	1,9	0,0	1,9	
	ИТОГО	19,8	10,1	9,7	Групповой опрос

4. Мониторинг и анализ безопасности

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Мониторинг и анализ безопасности				
4.1.	Описание механизмов сбора данных о безопасности	1,4	1,4	0,0	
4.2.	Рассмотрение процесса анализа события информационной безопасности	1,4	1,4	0,0	
4.3.	Лабораторная работа 10: Мониторинг событий информационной безопасности	1,7	0,0	1,7	
	ИТОГО	4,5	2,8	1,7	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Технологии обеспечения кибер-безопасности Cisco
(SECOPS)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	4
1.5 Трудоемкость обучения	4
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	7
2.3 Рабочая программа учебных предметов	7
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	10
3.1 Требования к педагогам	10
3.2 Материально-техническое оснащение программы	10
3.3 Учебно-методическое оснащение программы	10
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	10
V. СОСТАВИТЕЛИ ПРОГРАММЫ	11

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Технологии обеспечения кибер-безопасности Cisco (SECOPS)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 28.10.2014 N 809н (ред. от 12.12.2016) "Об утверждении профессионального стандарта "Системный аналитик" (Зарегистрировано в Минюсте России 24.11.2014 N 34882), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Технологии обеспечения кибер-безопасности Cisco (SECOPS)» - познакомить слушателей с дополнительными функциями администрирования Центров Управления Безопасностью (SOC - Security Operations Centers).

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Технологии обеспечения кибер-безопасности Cisco (SECOPS)».

Слушатель должен уметь:

- определять общие векторы атак;
- определять паттерны подозрительного поведения.

Слушатель должен знать:

- определение Security Operations Center;
- инструменты NSM.

Слушатель должен владеть:

- навыками расследования инцидентов безопасности.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Технологии обеспечения кибер-безопасности Cisco (SECOPS)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	1,3	1,3	0,0	Групповой опрос
2.	Обзор SOC	12,5	5,0	7,5	Групповой опрос
2.1.	Определение Security Operations Center	1,3	1,3	0,0	
2.2.	Понимание инструментов NSM	1,2	1,2	0,0	
2.3.	Представление об анализе инцидентов и SOC, основанном на анализе угроз	1,3	1,3	0,0	
2.4.	Определение ресурсов, необходимых для обнаружения киберугроз	1,2	1,2	0,0	
2.5.	Лабораторная работа 1: Исследование механизмов мониторинга	3,8	0,0	3,8	
2.6.	Лабораторная работа 2: Исследование методологии атаки	3,7	0,0	3,7	
3.	Расследования инцидентов безопасности	13,6	6,2	7,4	Групповой опрос
3.1.	Определение корреляции событий и нормализации	1,2	1,2	0,0	
3.2.	Определение общих векторов атак	1,4	1,4	0,0	
3.3.	Определение злонамеренной активности	1,0	1,0	0,0	
3.4.	Определение паттернов подозрительного поведения	1,3	1,3	0,0	
3.5.	Проведение расследования инцидентов	1,3	1,3	0,0	
3.6.	Лабораторная работа 3: Сбор трафика с вредоносным ПО	3,7	0,0	3,7	
3.7.	Лабораторная работа 4: Исследование PCAP-файлов	3,7	0,0	3,7	
4.	Работа SOC	10,6	6,5	4,1	Групповой опрос
4.1.	Описание SOC Playbook	1,1	1,1	0,0	
4.2.	Представление о метриках SOC	1,3	1,3	0,0	
4.3.	Представление о SOC WMS и автоматизации	1,3	1,3	0,0	

4.4.	Описание плана реакции на инциденты	1,3	1,3	0,0	
4.5.	Лабораторная работа 5: Исследование различных типов атак, определение реакции на инциденты безопасности	4,1	0,0	4,1	
4.6.	Приложение А—Описание роли команды, реагирующей на инциденты безопасности	1,3	1,3	0,0	
4.7.	Приложение В—Использование VERIS	0,2	0,2	0,0	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Технологии обеспечения кибер-безопасности Cisco (SECOPS)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	1,3	1,3	0,0	Групповой опрос

2. Обзор SOC

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические	

				занятия	
2.	Обзор SOC				
2.1.	Определение Security Operations Center	1,3	1,3	0,0	
2.2.	Понимание инструментов NSM	1,2	1,2	0,0	
2.3.	Представление об анализе инцидентов и SOC, основанном на анализе угроз	1,3	1,3	0,0	
2.4.	Определение ресурсов, необходимых для обнаружения киберугроз	1,2	1,2	0,0	
2.5.	Лабораторная работа 1: Исследование механизмов мониторинга	3,8	0,0	3,8	
2.6.	Лабораторная работа 2: Исследование методологии атаки	3,7	0,0	3,7	
	ИТОГО	12,5	5,0	7,5	Групповой опрос

3. Расследования инцидентов безопасности

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Расследования инцидентов безопасности				
3.1.	Определение корреляции событий и нормализации	1,2	1,2	0,0	
3.2.	Определение общих векторов атак	1,4	1,4	0,0	
3.3.	Определение злонамеренной активности	1,0	1,0	0,0	
3.4.	Определение паттернов подозрительного поведения	1,3	1,3	0,0	
3.5.	Проведение расследования инцидентов	1,3	1,3	0,0	
3.6.	Лабораторная работа 3: Сбор трафика с вредоносным ПО	3,7	0,0	3,7	
3.7.	Лабораторная работа 4: Исследование PCAP-файлов	3,7	0,0	3,7	
	ИТОГО	13,6	6,2	7,4	Групповой опрос

4. Работа SOC

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Работа SOC				
4.1.	Описание SOC Playbook	1,1	1,1	0,0	
4.2.	Представление о метриках SOC	1,3	1,3	0,0	
4.3.	Представление о SOC WMS и автоматизации	1,3	1,3	0,0	

4.4	Описание плана реакции на инциденты	1,3	1,3	0,0	
4.5	Лабораторная работа 5: Исследование различных типов атак, определение реакции на инциденты безопасности	4,1	0,0	4,1	
4.6	Приложение А—Описание роли команды, реагирующей на инциденты безопасности	1,3	1,3	0,0	
4.7	Приложение В—Использование VERIS	0,2	0,2	0,0	
	ИТОГО	10,6	6,5	4,1	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Развертывание решений Cisco по обеспечению
безопасности периметра сети (SENSS)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	5
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	6
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	12
3.1 Требования к педагогам	12
3.2 Материально-техническое оснащение программы	12
3.3 Учебно-методическое оснащение программы	12
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	12
V. СОСТАВИТЕЛИ ПРОГРАММЫ	13

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Развертывание решений Cisco по обеспечению безопасности периметра сети (SENSS)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Развертывание решений Cisco по обеспечению безопасности периметра сети (SENSS)» - предоставление знаний и практического опыта по настройке решений защиты границ сети, с использованием коммутаторов и маршрутизаторов, шлюзов Cisco и

межсетевых экранов Cisco ASA. Слушатели получают практический опыт работы по настройке различных вариантов защиты периметра для смягчения последствий внешних угроз и обеспечения безопасности различных зон сети.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Развертывание решений Cisco по обеспечению безопасности периметра сети (SENSS)».

Слушатель должен уметь:

- развертывать защиту сетевой инфраструктуры;
- развертывать NAT на устройствах с ОС Cisco IOS и межсетевых экранах Cisco ASA.

Слушатель должен знать:

- принципы защиты периметра сети;
- принципы работы политики фильтрации трафика на Cisco ASA;

Слушатель должен владеть:

- навыками настройки решений защиты границ сети, с использованием коммутаторов и маршрутизаторов, шлюзов Cisco и межсетевых экранов Cisco ASA.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Развертывание решений Cisco по обеспечению безопасности периметра сети
(SENSS)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,9	0,9	0,0	Групповой опрос
2.	Принципы защиты периметра сети	3,7	3,7	0,0	Групповой опрос
2.1.	Обзор основных зон (модулей) сети	0,8	0,8	0,0	
2.2.	Модульная Архитектура Безопасности Cisco	0,9	0,9	0,0	
2.3.	Архитектура Cisco SecureX	1,0	1,0	0,0	
2.4.	Архитектура Cisco TrustSec	1,0	1,0	0,0	
3.	Развертывание защиты сетевой инфраструктуры	12,7	6,2	6,5	Групповой опрос
3.1.	Введение в защиту сетевой инфраструктуры Cisco	0,9	0,9	0,0	
3.2.	Внедрение механизмов безопасности Control Plane для Cisco IOS	0,9	0,9	0,0	
3.3.	Внедрение механизмов безопасности Management Plane для Cisco IOS	1,0	1,0	0,0	
3.4.	Внедрение механизмов безопасности Management Plane для Cisco ASA	1,0	1,0	0,0	
3.5.	Лабораторная работа 1: Внедрение механизмов безопасности для Control Plane и Management Plane	1,7	0,0	1,7	
3.6.	Методы сбора телеметрии трафика	0,8	0,8	0,0	
3.7.	Лабораторная работа 2: Настройка различных методов телеметрии трафика	1,6	0,0	1,6	
3.8.	Внедрение механизмов безопасности Data Plane (L2) для устройств с ОС Cisco IOS	0,9	0,9	0,0	
3.9.	Лабораторная работа 3: Настройка защиты Data Plane (L2) для устройств с ОС Cisco IOS	1,6	0,0	1,6	
3.10.	Настройка элементов защиты Data Plane (L3) для устройств с ОС Cisco	0,7	0,7	0,0	

	IOS				
3.11.	Лабораторная работа 4: Настройка защиты Data Plane (L3) для устройств с ОС Cisco IOS	1,6	0,0	1,6	
4.	Развертывание NAT на устройствах с ОС Cisco IOS и межсетевых экранах Cisco ASA	6,0	2,6	3,4	Групповой опрос
4.1.	Введение в механизмы преобразования сетевых адресов (NAT)	0,8	0,8	0,0	
4.2.	Развертывание NAT на Cisco ASA	1,0	1,0	0,0	
4.3.	Лабораторная работа 5: Настройка NAT на Cisco ASA	1,7	0,0	1,7	
4.4.	Развертывание NAT на Cisco IOS	0,8	0,8	0,0	
4.5.	Лабораторная работа 6: Настройка NAT на Cisco IOS	1,7	0,0	1,7	
5.	Настройка политик фильтрации трафика на Cisco ASA	10,7	4,6	6,1	Групповой опрос
5.1.	Введение в механизмы фильтрации на Cisco ASA	1,1	1,1	0,0	
5.2.	Развертывание базовых политик доступа на Cisco ASA	0,7	0,7	0,0	
5.3.	Лабораторная работа 7: Настройка базовых политик доступа Cisco ASA	1,5	0,0	1,5	
5.4.	Развертывание расширенных политик доступа на Cisco ASA	0,9	0,9	0,0	
5.5.	Лабораторная работа 8: Настройка расширенных политик доступа на Cisco ASA	1,5	0,0	1,5	
5.6.	Развертывание политик доступа Cisco ASA на основе репутации	1,0	1,0	0,0	
5.7.	Лабораторная работа 9: Настройка фильтра трафика Botnet на Cisco ASA	1,6	0,0	1,6	
5.8.	Развертывание политик доступа Cisco ASA на основе идентификационных данных	0,9	0,9	0,0	
5.9.	Лабораторная работа 10: Настройка Cisco ASA Identity Firewall	1,5	0,0	1,5	
6.	Технология ZBFW на Cisco IOS	4,0	1,0	3,0	Групповой опрос
6.1.	Обзор функций зонowego межсетевого экрана на Cisco IOS	0,8	0,8	0,0	
6.2.	Лабораторная работа 11: Базовая настройка Cisco IOS Zone-Based Firewall	1,5	0,0	1,5	
6.3.	Развертывание расширенных политик доступа на Cisco IOS Zone-Based	0,2	0,2	0,0	

	Firewall				
6.4.	Лабораторная работа 12: Настройка расширенных политик доступа на Cisco IOS Zone-Based Firewall	1,5	0,0	1,5	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации
«Развертывание решений Cisco по обеспечению безопасности периметра сети (SENSS)».
Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,9	0,9	0,0	Групповой опрос

2. Принципы защиты периметра сети

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Принципы защиты периметра сети				
2.1	Обзор основных зон (модулей) сети	0,8	0,8	0,0	
2.2	Модульная Архитектура Безопасности Cisco	0,9	0,9	0,0	
2.3	Архитектура Cisco SecureX	1,0	1,0	0,0	

2.4	Архитектура Cisco TrustSec	1,0	1,0	0,0	
	ИТОГО	3,7	3,7	0,0	Групповой опрос

3. Развертывание защиты сетевой инфраструктуры

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Развертывание защиты сетевой инфраструктуры				
3.1	Введение в защиту сетевой инфраструктуры Cisco	0,9	0,9	0,0	
3.2	Внедрение механизмов безопасности Control Plane для Cisco IOS	0,9	0,9	0,0	
3.3	Внедрение механизмов безопасности Management Plane для Cisco IOS	1,0	1,0	0,0	
3.4	Внедрение механизмов безопасности Management Plane для Cisco ASA	1,0	1,0	0,0	
3.5	Лабораторная работа 1: Внедрение механизмов безопасности для Control Plane и Management Plane	1,7	0,0	1,7	
3.6	Методы сбора телеметрии трафика	0,8	0,8	0,0	
3.7	Лабораторная работа 2: Настройка различных методов телеметрии трафика	1,6	0,0	1,6	
3.8	Внедрение механизмов безопасности Data Plane (L2) для устройств с ОС Cisco IOS	0,9	0,9	0,0	
3.9	Лабораторная работа 3: Настройка защиты Data Plane (L2) для устройств с ОС Cisco IOS	1,6	0,0	1,6	
3.10	Настройка элементов защиты Data Plane (L3) для устройств с ОС Cisco IOS	0,7	0,7	0,0	
3.11	Лабораторная работа 4: Настройка защиты Data Plane (L3) для устройств с ОС Cisco IOS	1,6	0,0	1,6	
	ИТОГО	12,7	6,2	6,5	Групповой опрос

4. Развертывание NAT на устройствах с ОС Cisco IOS и межсетевых экранах Cisco

ASA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Развертывание NAT на устройствах с ОС Cisco IOS и межсетевых экранах Cisco ASA				
4.1	Введение в механизмы	0,8	0,8	0,0	

	преобразования сетевых адресов (NAT)				
4.2	Развертывание NAT на Cisco ASA	1,0	1,0	0,0	
4.3.	Лабораторная работа 5: Настройка NAT на Cisco ASA	1,7	0,0	1,7	
4.4.	Развертывание NAT на Cisco IOS	0,8	0,8	0,0	
4.5.	Лабораторная работа 6: Настройка NAT на Cisco IOS	1,7	0,0	1,7	
	ИТОГО	6,0	2,6	3,4	Групповой опрос

5. Настройка политик фильтрации трафика на Cisco ASA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Настройка политик фильтрации трафика на Cisco ASA				
5.1	Введение в механизмы фильтрации на Cisco ASA	1,1	1,1	0,0	
5.2	Развертывание базовых политик доступа на Cisco ASA	0,7	0,7	0,0	
5.3	Лабораторная работа 7: Настройка базовых политик доступа Cisco ASA	1,5	0,0	1,5	
5.4	Развертывание расширенных политик доступа на Cisco ASA	0,9	0,9	0,0	
5.5	Лабораторная работа 8: Настройка расширенных политик доступа на Cisco ASA	1,5	0,0	1,5	
5.6	Развертывание политик доступа Cisco ASA на основе репутации	1,0	1,0	0,0	
5.7	Лабораторная работа 9: Настройка фильтра трафика Botnet на Cisco ASA	1,6	0,0	1,6	
5.8	Развертывание политик доступа Cisco ASA на основе идентификационных данных	0,9	0,9	0,0	
5.9	Лабораторная работа 10: Настройка Cisco ASA Identity Firewall	1,5	0,0	1,5	
	ИТОГО	10,7	4,6	6,1	Групповой опрос

6. Технология ZBFW на Cisco IOS

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Технология ZBFW на Cisco IOS				
6.1	Обзор функций зонового межсетевого экрана на Cisco IOS	0,8	0,8	0,0	
6.2	Лабораторная работа 11: Базовая	1,5	0,0	1,5	

	настройка Cisco IOS Zone-Based Firewall				
6.3	Развертывание расширенных политик доступа на Cisco IOS Zone-Based Firewall	0,2	0,2	0,0	
6.4	Лабораторная работа 12: Настройка расширенных политик доступа на Cisco IOS Zone-Based Firewall	1,5	0,0	1,5	
	ВСЕГО	4,0	1,0	3,0	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Технологии защиты электронных сообщений от спама
и вирусов (v.2.1) (SESA)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	5
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	9
2.3 Рабочая программа учебных предметов	10
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	16
3.1 Требования к педагогам	16
3.2 Материально-техническое оснащение программы	16
3.3 Учебно-методическое оснащение программы	16
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	16
V. СОСТАВИТЕЛИ ПРОГРАММЫ	17

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Технологии защиты электронных сообщений от спама и вирусов (v.2.1) (SESA)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 19 мая 2014 года N 316н "Об утверждении профессионального стандарта "Инженер-проектировщик в области связи (телекоммуникаций) " (Зарегистрировано в Минюсте России 10 июля 2014 года, регистрационный N 33047), приказом Минтруда России от 05.10.2015 N 686н "Об утверждении профессионального стандарта "Специалист по администрированию сетевых устройств информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 30.10.2015 N 39568), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Технологии защиты электронных сообщений от спама и вирусов (v.2.1) (SESA)» –

предоставить слушателям знания о том, как устанавливать, настраивать и администрировать устройства Cisco Email Security Appliance. В результате обучения слушатели будут обладать навыками и знаниями, необходимыми для использования Cisco Email Security Appliances, выявления и устранения проблем при прохождении почтовых сообщений. Слушатели получают подробные сведения о наиболее часто используемых функциях и особенностях продукта. Интенсивные лабораторные упражнения предоставляют слушателям необходимый опыт по установке, настройке и администрированию устройств Cisco Email Security Appliance.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Технологии защиты электронных сообщений от спама и вирусов (v.2.1) (SESA)».

Слушатель должен уметь:

- устанавливать и настраивать Cisco Email Security Appliance;
- настраивать и использовать Cisco ESA антиспам;
- модифицировать почтовые политики для конечных пользователей.

Слушатель должен знать:

- архитектуру AsyncOS;
- принцип работы и запросы протокола LDAP.

Слушатель должен владеть:

- навыками предотвращения утечки информации.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 24 часа, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Технологии защиты электронных сообщений от спама и вирусов (v.2.1) (SESA)»

Срок обучения: 24 часа.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,2	0,2	0,0	Групповой опрос
2.	Обзор Cisco Email Security Appliance	1,7	1,0	0,7	Групповой опрос
2.1.	Обзор Cisco SMA	0,2	0,2	0,0	
2.2.	Обмен данными по протоколу SMTP	0,1	0,1	0,0	
2.3.	Термины и определения	0,3	0,3	0,0	
2.4.	Обработка писем (рабочая очередь), конвейер обработки писем	0,2	0,2	0,0	
2.5.	Модели Cisco Email Security Appliance и лицензирование	0,2	0,2	0,0	
2.6.	Лабораторная работа 1: Подключение к лабораторному стенду	0,7	0,0	0,7	
3.	Установка Cisco Email Security Appliance	0,9	0,4	0,5	Групповой опрос
3.1.	Обзор Listeners	0,1	0,1	0,0	
3.2.	Архитектура AsyncOS	0,1	0,1	0,0	
3.3.	Установка Cisco Email Security Appliance	0,2	0,2	0,0	
3.4.	Лабораторная работа 2: Установка ESA	0,5	0,0	0,5	
4.	Администрирование Cisco ESA	1,8	1,3	0,5	Групповой опрос
4.1.	Локальное отслеживание сообщений и создание отчетов	0,2	0,2	0,0	
4.2.	Централизованное отслеживание сообщений и создание отчетов	0,3	0,3	0,0	
4.3.	Настройка Cisco SMA	0,4	0,4	0,0	
4.4.	Администрирование Cisco ESA	0,2	0,2	0,0	
4.5.	Управление файлами логов	0,1	0,1	0,0	
4.6.	Создание и управление учетными записями администраторов	0,1	0,1	0,0	
4.7.	Лабораторная работа 3: Администрирование	0,5	0,0	0,5	
5.	Контролирование доменов отправителей и получателей	1,1	0,7	0,4	Групповой опрос
5.1.	Настройка публичных и частных	0,1	0,1	0,0	

	Listeners				
5.2.	Таблица отправителей (HAT)	0,2	0,2	0,0	
5.3.	Таблица получателей (RAT)	0,3	0,3	0,0	
5.4.	Разрешение проблем с использованием Mail Logs	0,1	0,1	0,0	
5.5.	Лабораторная работа 4: Тестирование настроек Listeners	0,4	0,0	0,4	
6.	Контролирование спама с использование SensorBase и антиспам	1,7	1,1	0,6	Групповой опрос
6.1.	Сеть SenderBase	0,2	0,2	0,0	
6.2.	Настройка и использование Cisco ESA антиспам	0,2	0,2	0,0	
6.3.	Карантин для спама	0,1	0,1	0,0	
6.4.	Белые и черные списки	0,3	0,3	0,0	
6.5.	Централизованный карантин спама на Cisco SMA	0,2	0,2	0,0	
6.6.	Настройка проверки возвратов писем	0,1	0,1	0,0	
6.7.	Лабораторная работа 5: Защита от спама при помощи SenderBase и антиспам фильтром	0,6	0,0	0,6	
7.	Использование антивируса и фильтров Outbreak	1,1	0,5	0,6	
7.1.	Антивирус	0,2	0,2	0,0	
7.2.	Фильтры Outbreak	0,3	0,3	0,0	
7.3.	Лабораторная работа 6: Защита от вирусов	0,6	0,0	0,6	
8.	Использование политик обработки почты	1,1	0,4	0,7	Групповой опрос
8.1.	Обзор Email Security Manager	0,1	0,1	0,0	
8.2.	Пользовательские почтовые политики	0,2	0,2	0,0	
8.3.	Расщепление сообщений по получателям	0,1	0,1	0,0	
8.4.	Лабораторная работа 7: Модификация почтовых политик для конечных пользователей	0,7	0,0	0,7	
9.	Использование фильтрации содержимого	0,9	0,4	0,5	Групповой опрос
9.1.	Обзор фильтрации содержимого	0,1	0,1	0,0	
9.2.	Настройка фильтрации содержимого	0,2	0,2	0,0	
9.3.	Применения фильтрации содержимого	0,1	0,1	0,0	
9.4.	Лабораторная работа 8: Применение бизнес политик для доставки почты	0,5	0,0	0,5	
10.	Предотвращение утечки информации	0,9	0,4	0,5	Групповой опрос
10.1.	Проблема утечки информации	0,1	0,1	0,0	
10.2.	Решение DLP на Cisco ESA	0,1	0,1	0,0	

10.3.	Настройка DLP	0,1	0,1	0,0	
10.4.	Глубокий анализ при помощи RSA DLP	0,1	0,1	0,0	
10.5.	Лабораторная работа 9: Настройка DLP	0,5	0,0	0,5	
11.	Использование LDAP	3,8	1,4	2,4	Групповой опрос
11.1.	Обзор LDAP	0,3	0,3	0,0	
11.2.	Запросы LDAP	0,2	0,2	0,0	
11.3.	Настройка профиля LDAP	0,2	0,2	0,0	
11.4.	Настройка SMTP Call-Ahead	0,2	0,2	0,0	
11.5.	Примеры использования	0,2	0,2	0,0	
11.6.	Использование запросов LDAP группы	0,3	0,3	0,0	
11.7.	Лабораторная работа 10: Настройка LDAP Accepт	0,5	0,0	0,5	
11.8.	Лабораторная работа 11: Настройка SMTP Call-Ahead	0,6	0,0	0,6	
11.9.	Лабораторная работа 12: Настройка LDAP доменов	0,7	0,0	0,7	
11.10.	Лабораторная работа 13: Контроль политик обработки почты при помощи LDAP Group запросов	0,6	0,0	0,6	
12.	Использование аутентификации и шифрования	2,3	0,5	1,8	Групповой опрос
12.1.	Использование Cisco RES	0,1	0,1	0,0	
12.2.	Настройка TLS	0,3	0,3	0,0	
12.3.	Использование SPF для аутентификации писем	0,1	0,1	0,0	
12.4.	Лабораторная работа 14: Настройка внешнего шифрования	0,6	0,0	0,6	
12.5.	Лабораторная работа 15: Шифрование почты с использованием TLS	0,6	0,0	0,6	
12.6.	Лабораторная работа 16: SPF и SIDF	0,6	0,0	0,6	
13.	Использование фильтров сообщений	0,9	0,4	0,5	Групповой опрос
13.1.	Обзор фильтров сообщений	0,1	0,1	0,0	
13.2.	Регулярные выражения для фильтров	0,1	0,1	0,0	
13.3.	Примеры фильтров сообщений	0,2	0,2	0,0	
13.4.	Лабораторная работа 17: Перенаправление писем, используя функционал Message Filters	0,5	0,0	0,5	
14.	Использование системного карантина и способов доставки	1,5	0,9	0,6	Групповой опрос
14.1.	Обзор технологии карантин	0,2	0,2	0,0	
14.2.	Управление системными карантинами	0,1	0,1	0,0	
14.3.	Настройка ограничений по доставке писем	0,1	0,1	0,0	

14.4.	Настройка виртуального шлюза	0,3	0,3	0,0	
14.5.	Настройка профиля обработки возврата писем	0,2	0,2	0,0	
14.6.	Лабораторная работа 18: Настройка виртуального шлюза	0,6	0,0	0,6	
15.	Кластеризация	1,2	0,6	0,6	Групповой опрос
15.1.	Создание кластеров	0,2	0,2	0,0	
15.2.	Присоединение к существующему кластеру	0,1	0,1	0,0	
15.3.	Управление кластерами	0,1	0,1	0,0	
15.4.	Администрирование кластеров через GUI	0,2	0,2	0,0	
15.5.	Лабораторная работа 19: Настройка кластера	0,6	0,0	0,6	
16.	Разрешение проблем	1,9	1,3	0,6	Групповой опрос
16.1.	Категории проблем, связанных с устройством	0,1	0,1	0,0	
16.2.	Мониторинг системы	0,2	0,2	0,0	
16.3.	Диагностика проблем	0,3	0,3	0,0	
16.4.	Наиболее распространенные проблемы и их решения	0,7	0,7	0,0	
16.5.	Лабораторная работа 20: Разрешение проблем	0,6	0,0	0,6	
	Всего:	23	11,5	11,5	
	Итоговый контроль знаний	1	0	0	Электронное тестирование
	Итого:	24	11,5	11,5	

2.2 Календарный учебный график

Занятия проводятся 3 раза в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1		
	дни	1	1	1
Вид занятий		А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Технологии защиты электронных сообщений от спама и вирусов (v.2.1) (SESA)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,2	0,2	0,0	Групповой опрос

2. Обзор Cisco Email Security Appliance

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Обзор Cisco Email Security Appliance				
2.1	Обзор Cisco SMA	0,2	0,2	0,0	
2.2	Обмен данными по протоколу SMTP	0,1	0,1	0,0	
2.3	Термины и определения	0,3	0,3	0,0	
2.4	Обработка писем (рабочая очередь), конвейер обработки писем	0,2	0,2	0,0	
2.5	Модели Cisco Email Security Appliance и лицензирование	0,2	0,2	0,0	
2.6	Лабораторная работа 1: Подключение к лабораторному стенду	0,7	0,0	0,7	
	ИТОГО	1,7	1,0	0,7	Групповой опрос

3. Установка Cisco Email Security Appliance

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Установка Cisco Email Security Appliance				
3.1	Обзор Listeners	0,1	0,1	0,0	
3.2	Архитектура AsyncOS	0,1	0,1	0,0	
3.3	Установка Cisco Email Security Appliance	0,2	0,2	0,0	
3.4	Лабораторная работа 2: Установка ESA	0,5	0,0	0,5	
	ИТОГО	0,9	0,4	0,5	Групповой опрос

4. Администрирование Cisco ESA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические	

				занятия	
4.	Администрирование Cisco ESA				
4.1	Локальное отслеживание сообщений и создание отчетов	0,2	0,2	0,0	
4.2	Централизованное отслеживание сообщений и создание отчетов	0,3	0,3	0,0	
4.3	Настройка Cisco SMA	0,4	0,4	0,0	
4.4	Администрирование Cisco ESA	0,2	0,2	0,0	
4.5	Управление файлами логов	0,1	0,1	0,0	
4.6	Создание и управление учетными записями администраторов	0,1	0,1	0,0	
4.7	Лабораторная работа 3: Администрирование	0,5	0,0	0,5	
	ИТОГО	1,8	1,3	0,5	Групповой опрос

5. Контролирование доменов отправителей и получателей

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Контролирование доменов отправителей и получателей				
5.1	Настройка публичных и частных Listeners	0,1	0,1	0,0	
5.2.	Таблица отправителей (HAT)	0,2	0,2	0,0	
5.3	Таблица получателей (RAT)	0,3	0,3	0,0	
5.4	Разрешение проблем с использованием Mail Logs	0,1	0,1	0,0	
5.5	Лабораторная работа 4: Тестирование настроек Listeners	0,4	0,0	0,4	
	ИТОГО	1,1	0,7	0,4	Групповой опрос

6. Контролирование спама с использование SensorBase и антиспам

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Контролирование спама с использование SensorBase и антиспам				
6.1	Сеть Senderbase	0,2	0,2	0,0	
6.2	Настройка и использование Cisco ESA антиспам	0,2	0,2	0,0	
6.3	Карантин для спама	0,1	0,1	0,0	
6.4	Белые и черные списки	0,3	0,3	0,0	
6.5	Централизованный карантин спама на Cisco SMA	0,2	0,2	0,0	
6.6	Настройка проверки возвратов писем	0,1	0,1	0,0	
6.7	Лабораторная работа 5: Защита от спама при помощи SenderBase и	0,6	0,0	0,6	

	антиспам фильтром				
	ИТОГО	1,7	1,1	0,6	Групповой опрос

7. Использование антивируса и фильтров Outbreak

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
7.	Использование антивируса и фильтров Outbreak				
7.1	Антивирус	0,2	0,2	0,0	
7.2	Фильтры Outbreak	0,3	0,3	0,0	
7.3	Лабораторная работа 6: Защита от вирусов	0,6	0,0	0,6	
	ИТОГО	1,1	0,5	0,6	Групповой опрос

8. Использование политик обработки почты

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
8.	Использование политик обработки почты				
8.1	Обзор Email Security Manager	0,1	0,1	0,0	
8.2.	Пользовательские почтовые политики	0,2	0,2	0,0	
8.3	Расщепление сообщений по получателям	0,1	0,1	0,0	
8.4	Лабораторная работа 7: Модификация почтовых политик для конечных пользователей	0,7	0,0	0,7	
	ИТОГО	1,1	0,4	0,7	Групповой опрос

9. Использование фильтрации содержимого

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
9.	Использование фильтрации содержимого				
9.1	Обзор фильтрации содержимого	0,1	0,1	0,0	
9.2	Настройка фильтрации содержимого	0,2	0,2	0,0	
9.3	Применения фильтрации содержимого	0,1	0,1	0,0	
9.4	Лабораторная работа 8: Применение бизнес политик для доставки почты	0,5	0,0	0,5	
	ИТОГО	0,9	0,4	0,5	Групповой опрос

10. Предотвращение утечки информации

№	Наименование разделов и тем	Всего	В том числе	Форма
---	-----------------------------	-------	-------------	-------

тема		часов	лекции	практические занятия	контроля
10.	Предотвращение утечки информации				
10.1	Проблема утечки информации	0,1	0,1	0,0	
10.2	Решение DLP на Cisco ESA	0,1	0,1	0,0	
10.3	Настройка DLP	0,1	0,1	0,0	
10.4	Глубокий анализ при помощи RSA DLP	0,1	0,1	0,0	
10.5	Лабораторная работа 9: Настройка DLP	0,5	0,0	0,5	
	ИТОГО	0,9	0,4	0,5	Групповой опрос

11. Использование LDAP

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
11.	Использование LDAP				
11.1	Обзор LDAP	0,3	0,3	0,0	
11.2	Запросы LDAP	0,2	0,2	0,0	
11.3	Настройка профиля LDAP	0,2	0,2	0,0	
11.4	Настройка SMTP Call-Ahead	0,2	0,2	0,0	
11.5	Примеры использования	0,2	0,2	0,0	
11.6	Использование запросов LDAP группы	0,3	0,3	0,0	
11.7	Лабораторная работа 10: Настройка LDAP Ассерпт	0,5	0,0	0,5	
11.8	Лабораторная работа 11: Настройка SMTP Call-Ahead	0,6	0,0	0,6	
11.9	Лабораторная работа 12: Настройка LDAP доменов	0,7	0,0	0,7	
11.10	Лабораторная работа 13: Контроль политик обработки почты при помощи LDAP Group запросов	0,6	0,0	0,6	
	ИТОГО	3,8	1,4	2,4	Групповой опрос

12. Использование аутентификации и шифрования

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
12.	Использование аутентификации и шифрования				
12.1	Использование Cisco RES	0,1	0,1	0,0	
12.2	Настройка TLS	0,3	0,3	0,0	
12.3	Использование SPF для аутентификации писем	0,1	0,1	0,0	
12.4	Лабораторная работа 14: Настройка	0,6	0,0	0,6	

	внешнего шифрования				
12.5	Лабораторная работа 15: Шифрование почты с использованием TLS	0,6	0,0	0,6	
12.6	Лабораторная работа 16: SPF и SIDF	0,6	0,0	0,6	
	ИТОГО	2,3	0,5	1,8	Групповой опрос

13. Использование фильтров сообщений

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
13.	Использование фильтров сообщений				
13.1	Обзор фильтров сообщений	0,1	0,1	0,0	
13.2	Регулярные выражения для фильтров	0,1	0,1	0,0	
13.3	Примеры фильтров сообщений	0,2	0,2	0,0	
13.4	Лабораторная работа 17: Перенаправление писем, используя функционал Message Filters	0,5	0,0	0,5	
	ИТОГО	0,9	0,4	0,5	Групповой опрос

14. Использование системного карантина и способов доставки

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
14.	Использование системного карантина и способов доставки				
14.1	Обзор технологии карантин	0,2	0,2	0,0	
14.2	Управление системными карантинами	0,1	0,1	0,0	
14.3	Настройка ограничений по доставке писем	0,1	0,1	0,0	
14.4	Настройка виртуального шлюза	0,3	0,3	0,0	
14.5	Настройка профиля обработки возврата писем	0,2	0,2	0,0	
14.6	Лабораторная работа 18: Настройка виртуального шлюза	0,6	0,0	0,6	
	ИТОГО	1,5	0,9	0,6	Групповой опрос

15. Кластеризация

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
15.	Кластеризация				
15.1	Создание кластеров	0,2	0,2	0,0	
15.2	Присоединение к существующему кластеру	0,1	0,1	0,0	
15.3	Управление кластерами	0,1	0,1	0,0	

15.4	Администрирование кластеров через GUI	0,2	0,2	0,0	
15.5	Лабораторная работа 19: Настройка кластера	0,6	0,0	0,6	
	ИТОГО	1,2	0,6	0,6	Групповой опрос

16. Разрешение проблем

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
16.	Разрешение проблем				
16.1	Категории проблем, связанных с устройством	0,1	0,1	0,0	
16.2	Мониторинг системы	0,2	0,2	0,0	
16.3	Диагностика проблем	0,3	0,3	0,0	
16.4	Наиболее распространенные проблемы и их решения	0,7	0,7	0,0	
16.5	Лабораторная работа 20: Разрешение проблем	0,6	0,0	0,6	
	ИТОГО	1,9	1,3	0,6	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Внедрение решений Cisco для безопасной мобильности
(SIMOS)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	4
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	6
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	11
3.1 Требования к педагогам	11
3.2 Материально-техническое оснащение программы	11
3.3 Учебно-методическое оснащение программы	11
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	11
V. СОСТАВИТЕЛИ ПРОГРАММЫ	12

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Внедрение решений Cisco для безопасной мобильности (SIMOS)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 05.10.2015 N 686н "Об утверждении профессионального стандарта "Специалист по администрированию сетевых устройств информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 30.10.2015 N 39568), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Внедрение решений Cisco для безопасной мобильности (SIMOS)» - подготовить слушателей, предоставив им знания и опыт, необходимые для защиты данных, проходящих по разделяемой среде, такой как Internet, посредством внедрения и поддержки решений Cisco VPN. Слушатели программы получают практический опыт настройки и диагностики

решений удаленного доступа на основе многофункциональных устройств Cisco ASA и маршрутизаторов, работающих под управлением Cisco IOS.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Внедрение решений Cisco для безопасной мобильности (SIMOS)».

Слушатель должен уметь:

- внедрять защищенные решения для соединений Site-to-Site;
- внедрять решения Site-to-Site FlexVPN на основе Cisco IOS;
- внедрять AnyConnect VPN для удаленного доступа.

Слушатель должен знать:

- основы технологий VPN и криптографии.

Слушатель должен владеть:

- навыками обеспечения безопасности оконечных устройств и настройки DAP.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Внедрение решений Cisco для безопасной мобильности (SIMOS)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	1,2	1,2	0,0	Групповой опрос
2.	Основы технологий VPN и криптография	2,4	2,4	0,0	Групповой опрос
2.1.	Роль VPN в сетевой безопасности	1,1	1,1	0,0	
2.2.	VPN и основы криптография	1,3	1,3	0,0	
3.	Внедрение защищенных решений для соединений Site-to-Site	10,3	4,7	5,6	Групповой опрос
3.1.	Введение в решения Cisco для защищенных соединений Site-to-Site	1,2	1,2	0,0	
3.2.	Внедрение Point-to-Point IPsec VPN на Cisco ASA	1,2	1,2	0,0	
3.3.	Внедрение решений VTI Point-to-Point IPsec VPN на устройствах с ОС Cisco IOS	1,3	1,3	0,0	
3.4.	Внедрение Cisco IOS DMVPNs	1,0	1,0	0,0	
3.5.	Лабораторная работа 1: Осуществление безопасного соединения Site-to-Site на Cisco ASA	1,9	0,0	1,9	
3.6.	Лабораторная работа 2: Развертывание Cisco IOS Static VTI Point-to-Point туннелей	1,7	0,0	1,7	
3.7.	Лабораторная работа 3: Реализация DMVPN	2,0	0,0	2,0	
4.	Внедрение решений Site-to-Site FlexVPN на основе Cisco IOS	10,1	4,5	5,6	Групповой опрос
4.1.	Введение в решение Cisco FlexVPN	1,2	1,2	0,0	
4.2.	Внедрение Point-to-Point IPsec VPN с использованием Cisco IOS FlexVPN	1,2	1,2	0,0	
4.3.	Внедрение Hub-and-Spoke IPsec VPN	1,1	1,1	0,0	
4.4.	Внедрение Spoke-and-Spoke IPsec VPN	1,0	1,0	0,0	
4.5.	Лабораторная работа 4: Внедрение туннеля Site-to-Site с помощью Cisco IOS FlexVPN	1,9	0,0	1,9	
4.6.	Лабораторная работа 5: Внедрение	1,9	0,0	1,9	

	топологии Hub-to-Spoke				
4.7.	Лабораторная работа 6: Внедрение топологии Spoke-to-Spoke	1,8	0,0	1,8	
5.	Внедрение AnyConnect VPN для удаленного доступа	10,4	4,7	5,7	Групповой опрос
5.1.	Обзор Clientless SSL VPN (портал без клиента)	1,2	1,2	0,0	
5.2.	Внедрение базовых решений по Clientless SSL VPN	1,2	1,2	0,0	
5.3.	Внедрение механизмов доступа к приложениям в Clientless SSL VPN	1,1	1,1	0,0	
5.4.	Внедрение расширенной аутентификации в Clientless SSL VPN	1,2	1,2	0,0	
5.5.	Лабораторная работа 7: Реализация базового Clientless SSL VPN на ASA	2,0	0,0	2,0	
5.6.	Лабораторная работа 8: Доступ к приложениям через Clientless SSL	1,9	0,0	1,9	
5.7.	Лабораторная работа 9: Расширенное использование AAA для Clientless SSL VPN	1,8	0,0	1,8	
6.	Обеспечение безопасности оконечных устройств и настройка DAP	3,6	1,5	2,1	Групповой опрос
6.1.	Реализация механизмов сканирования узлов	1,1	1,1	0,0	
6.2.	Внедрение DAP для SSL VPN	0,4	0,4	0,0	
6.3.	Лабораторная работа 10: Настройка Hostscan и DAP для AnyConnect SSL VPN	2,1	0,0	2,1	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Внедрение решений Cisco для безопасной мобильности (SIMOS)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	1,2	1,2	0,0	Групповой опрос

2. Основы технологий VPN и криптография

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Основы технологий VPN и криптография				
2.1	Роль VPN в сетевой безопасности	1,1	1,1	0,0	
2.2	VPN и основы криптография	1,3	1,3	0,0	
	ИТОГО	2,4	2,4	0,0	Групповой опрос

3. Внедрение защищенных решений для соединений Site-to-Site

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Внедрение защищенных решений для соединений Site-to-Site				
3.1	Введение в решения Cisco для защищенных соединений Site-to-Site	1,2	1,2	0,0	
3.2	Внедрение Point-to-Point IPsec VPN на Cisco ASA	1,2	1,2	0,0	
3.3	Внедрение решений VTI Point-to-Point IPsec VPN на устройствах с ОС Cisco IOS	1,3	1,3	0,0	
3.4	Внедрение Cisco IOS DMVPNs	1,0	1,0	0,0	
3.5	Лабораторная работа 1: Осуществление безопасного соединения Site-to-Site на Cisco ASA	1,9	0,0	1,9	
3.6	Лабораторная работа 2: Развертывание Cisco IOS Static VTI Point-to-Point туннелей	1,7	0,0	1,7	
3.7	Лабораторная работа 3: Реализация DMVPN	2,0	0,0	2,0	
	ИТОГО	10,3	4,7	5,6	Групповой опрос

4. Внедрение решений Site-to-Site FlexVPN на основе Cisco IOS

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Внедрение решений Site-to-Site FlexVPN на основе Cisco IOS				
4.1	Введение в решение Cisco FlexVPN	1,2	1,2	0,0	
4.2	Внедрение Point-to-Point IPsec VPN с использованием Cisco IOS FlexVPN	1,2	1,2	0,0	
4.3.	Внедрение Hub-and-Spoke IPsec VPN	1,1	1,1	0,0	
4.4.	Внедрение Spoke-and-Spoke IPsec VPN	1,0	1,0	0,0	
4.5.	Лабораторная работа 4: Внедрение туннеля Site-to-Site с помощью Cisco IOS FlexVPN	1,9	0,0	1,9	
4.6	Лабораторная работа 5: Внедрение топологии Hub-to-Spoke	1,9	0,0	1,9	
4.7	Лабораторная работа 6: Внедрение топологии Spoke-to-Spoke	1,8	0,0	1,8	
	ИТОГО	10,1	4,5	5,6	Групповой опрос

5. Внедрение AnyConnect VPN для удаленного доступа

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Внедрение AnyConnect VPN для удаленного доступа				
5.1	Обзор Clientless SSL VPN (портал без клиента)	1,2	1,2	0,0	
5.2	Внедрение базовых решений по Clientless SSL VPN	1,2	1,2	0,0	
5.3	Внедрение механизмов доступа к приложениям в Clientless SSL VPN	1,1	1,1	0,0	
5.4	Внедрение расширенной аутентификации в Clientless SSL VPN	1,2	1,2	0,0	
5.5	Лабораторная работа 7: Реализация базового Clientless SSL VPN на ASA	2,0	0,0	2,0	
5.6	Лабораторная работа 8: Доступ к приложениям через Clientless SSL	1,9	0,0	1,9	
5.7	Лабораторная работа 9: Расширенное использование AAA для Clientless SSL VPN	1,8	0,0	1,8	
	ИТОГО	10,4	4,7	5,7	Групповой опрос

6. Обеспечение безопасности оконечных устройств и настройка DAP

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Обеспечение безопасности оконечных устройств и настройка DAP				
6.1	Реализация механизмов сканирования узлов	1,1	1,1	0,0	
6.2	Внедрение DAP для SSL VPN	0,4	0,4	0,0	
6.3	Лабораторная работа 10: Настройка Hostscan и DAP для AnyConect SSL VPN	2,1	0,0	2,1	
	ВСЕГО	3,6	1,5	2,1	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Внедрение решений Cisco для контроля доступа в сети
(SISAS)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	5
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	6
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	11
3.1 Требования к педагогам	11
3.2 Материально-техническое оснащение программы	11
3.3 Учебно-методическое оснащение программы	11
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	11
V. СОСТАВИТЕЛИ ПРОГРАММЫ	12

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Внедрение решений Cisco для контроля доступа в сети (SISAS)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Внедрение решений Cisco для контроля доступа в сети (SISAS)» - предоставить слушателям знания и навыки в объеме, достаточном для развертывания устройств Cisco ISE и внедрению решений по контролю доступа в сети на основе стандарта 802.1X. Студенты получают практический опыт настройки наиболее эффективных решений Cisco для защиты

от внешних угроз и обеспечения безопасности устройств, подключенных к сети. По окончании курса, слушатели смогут уменьшить риски для их ИТ-инфраструктуры и приложений с помощью сервисов платформы Cisco ISE, предоставить оперативную поддержку и контроль доступа к сети на основе идентификации.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Внедрение решений Cisco для контроля доступа в сети (SISAS)».

Слушатель должен уметь:

- внедрять и настраивать системы Cisco ISE;
- настраивать параметры гостевого доступа;
- устранять неполадки в работе системы контроля доступа.

Слушатель должен знать:

- механизмы аутентификации на Cisco ISE;
- расширенные функции контроля доступа в сети.

Слушатель должен владеть:

- навыками уменьшения рисков для ИТ-инфраструктуры и приложений с помощью сервисов платформы Cisco ISE.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Внедрение решений Cisco для контроля доступа в сети (SISAS)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	1,1	1,1	0,0	Групповой опрос
2.	Предотвращение угроз посредством служб идентификации	5,0	3,2	1,8	Групповой опрос
2.1.	Службы идентификации	1,0	1,0	0,0	
2.2.	Протокол 802.1 X и EAP	1,1	1,1	0,0	
2.3.	Внедрение системы Cisco ISE	1,1	1,1	0,0	
2.4.	Лабораторная работа 1: Внедрение и базовая настройка Cisco ISE	1,8	0,0	1,8	
3.	Основы системы Cisco ISE	8,1	4,2	3,9	Групповой опрос
3.1.	Обзор Cisco ISE	1,0	1,0	0,0	
3.2.	Cisco ISE в инфраструктуре PKI	1,1	1,1	0,0	
3.3.	Механизмы аутентификации на Cisco ISE	1,1	1,1	0,0	
3.4.	Настройка Cisco ISE для внешней аутентификации	1,0	1,0	0,0	
3.5.	Лабораторная работа 2: Ввод Cisco ISE в PKI	1,9	0,0	1,9	
3.6.	Лабораторная работа 3: Аутентификация на основе MAC-адреса (MAB) с использованием внутренней базы	2,0	0,0	2,0	
4.	Расширенные функции контроля доступа в сети	6,8	3,3	3,5	Групповой опрос
4.1.	Аутентификация на основе сертификатов пользователей	1,1	1,1	0,0	
4.2.	Авторизация	1,1	1,1	0,0	
4.3.	Использование SGA и применение технологии MACsec	1,1	1,1	0,0	
4.4.	Лабораторная работа 4: Использование метода EAP-TLS для работы системы контроля доступа	1,6	0,0	1,6	
4.5.	Лабораторная работа 5: Настройка политик авторизации	1,9	0,0	1,9	

5.	Веб-аутентификация, гостевые порталы	7,2	3,3	3,9	Групповой опрос
5.1.	Знакомство с веб-аутентификацией	1,2	1,2	0,0	
5.2.	Лабораторная работа 6: Настройка гостевого доступа	1,9	0,0	1,9	
5.3.	Знакомство с компонентами гостевых порталов	1,1	1,1	0,0	
5.4.	Настройка параметров гостевого доступа	1,0	1,0	0,0	
5.5.	Лабораторная работа 7: Настройка гостевого доступа	2,0	0,0	2,0	
6.	Расширенные методы контроля доступа для периферийных устройств	7,3	3,3	4,0	Групповой опрос
6.1.	Posture-сервис	1,0	1,0	0,0	
6.2.	Сервис профилирования	1,2	1,2	0,0	
6.3.	Архитектура BYOD	1,1	1,1	0,0	
6.4.	Лабораторная работа 8: Настройка Posture-сервиса	2,1	0,0	2,1	
6.5.	Лабораторная работа 9: Настройка сервиса профилирования	1,9	0,0	1,9	
7.	Устранение неполадок в системе	2,5	0,6	1,9	Групповой опрос
7.1.	Устранение неполадок в работе системы контроля доступа	0,6	0,6	0,0	
7.2.	Лабораторная работа 10: Поиск и устранение неполадок в лабораторной сети	1,9	0,0	1,9	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Внедрение решений Cisco для контроля доступа в сети (SISAS)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	1,1	1,1	0,0	Групповой опрос

2. Предотвращение угроз посредством служб идентификации

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Предотвращение угроз посредством служб идентификации				
2.1	Службы идентификации	1,0	1,0	0,0	
2.2	Протокол 802.1 X и EAP	1,1	1,1	0,0	
2.3	Внедрение системы Cisco ISE	1,1	1,1	0,0	
2.4	Лабораторная работа 1: Внедрение и базовая настройка Cisco ISE	1,8	0,0	1,8	
	ИТОГО	5,0	3,2	1,8	Групповой опрос

3. Основы системы Cisco ISE

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Основы системы Cisco ISE				
3.1	Обзор Cisco ISE	1,0	1,0	0,0	
3.2	Cisco ISE в инфраструктуре PKI	1,1	1,1	0,0	
3.3	Механизмы аутентификации на Cisco ISE	1,1	1,1	0,0	
3.4	Настройка Cisco ISE для внешней аутентификации	1,0	1,0	0,0	
3.5	Лабораторная работа 2: Ввод Cisco ISE в PKI	1,9	0,0	1,9	
3.6	Лабораторная работа 3: Аутентификация на основе MAC-адреса (MAV) с использованием внутренней базы	2,0	0,0	2,0	
	ИТОГО	8,1	4,2	3,9	Групповой

					опрос
--	--	--	--	--	--------------

4. Расширенные функции контроля доступа в сети

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Расширенные функции контроля доступа в сети				
4.1	Аутентификация на основе сертификатов пользователей	1,1	1,1	0,0	
4.2	Авторизация	1,1	1,1	0,0	
4.3.	Использование SGA и применение технологии MACsec	1,1	1,1	0,0	
4.4.	Лабораторная работа 4: Использование метода EAP-TLS для работы системы контроля доступа	1,6	0,0	1,6	
4.5.	Лабораторная работа 5: Настройка политик авторизации	1,9	0,0	1,9	
	ИТОГО	6,8	3,3	3,5	Групповой опрос

5. Веб-аутентификация, гостевые порталы

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Веб-аутентификация, гостевые порталы				
5.1	Знакомство с веб-аутентификацией	1,2	1,2	0,0	
5.2	Лабораторная работа 6: Настройка гостевого доступа	1,9	0,0	1,9	
5.3	Знакомство с компонентами гостевых порталов	1,1	1,1	0,0	
5.4	Настройка параметров гостевого доступа	1,0	1,0	0,0	
5.5	Лабораторная работа 7: Настройка гостевого доступа	2,0	0,0	2,0	
	ИТОГО	7,2	3,3	3,9	Групповой опрос

6. Расширенные методы контроля доступа для периферийных устройств

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Расширенные методы контроля доступа для периферийных устройств				
6.1	Posture-сервис	1,0	1,0	0,0	
6.2	Сервис профилирования	1,2	1,2	0,0	
6.3	Архитектура BYOD	1,1	1,1	0,0	
6.4	Лабораторная работа 8: Настройка	2,1	0,0	2,1	

	Posture-сервиса				
6.5	Лабораторная работа 9: Настройка сервиса профилирования	1,9	0,0	1,9	
	ВСЕГО	7,3	3,3	4,0	Групповой опрос

7. Технология ZBFW на Cisco IOS

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
7.	Устранение неполадок в системе				
7.1	Устранение неполадок в работе системы контроля доступа	0,6	0,6	0,0	
7.2	Лабораторная работа 10: Поиск и устранение неполадок в лабораторной сети	1,9	0,0	1,9	
	ВСЕГО	2,5	0,6	1,9	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Внедрение и настройка решения Cisco Identity Services
Engine (SISE)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	4
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	5
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	9
2.3 Рабочая программа учебных предметов	9
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	14
3.1 Требования к педагогам	14
3.2 Материально-техническое оснащение программы	14
3.3 Учебно-методическое оснащение программы	14
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	14
V. СОСТАВИТЕЛИ ПРОГРАММЫ	15

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Внедрение и настройка решения Cisco Identity Services Engine (SISE)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 19 мая 2014 года N 316н "Об утверждении профессионального стандарта "Инженер-проектировщик в области связи (телекоммуникаций) " (Зарегистрировано в Минюсте России 10 июля 2014 года, регистрационный N 33047), приказом Минтруда России от 18.11.2014 N 896н "Об утверждении профессионального стандарта "Специалист по информационным системам"(Зарегистрировано в Минюсте России 24.12.2014 N 35361), приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Внедрение и настройка решения Cisco Identity Services Engine (SISE)» – обеспечить слушателей практическими навыками по установке, развертыванию и управлению решением Cisco Identity Services Engine (ISE), с целью поддержки аутентификации, авторизации, работы с аккаунтами и политиками сети для пользователей и устройств. Студенты пройдут через весь процесс установки, конфигурирования сети и устройств, используя ISE в качестве устройства контроля доступа в сети.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Внедрение и настройка решения Cisco Identity Services Engine (SISE)».

Слушатель должен уметь:

- настраивать политики доступа на Cisco ISE;
- настраивать гостевой доступ;
- работать с функционалом TACACS+.

Слушатель должен знать:

- архитектуру и возможности Cisco ISE;
- стандарт 802.1X.

Слушатель должен владеть:

- навыками внедрения Cisco ISE в сети предприятия.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Внедрение и настройка решения Cisco Identity Services Engine (SISE)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,7	0,7	0,0	Групповой опрос
2.	Знакомство с архитектурой и системой Cisco ISE	2,3	1,3	1,0	Групповой опрос
2.1.	Обзор возможностей платформы Cisco ISE	0,6	0,6	0,0	
2.2.	Знакомство с моделями развертывания Cisco ISE	0,7	0,7	0,0	
2.3.	Лабораторная работа 1: Первоначальная настройка Cisco ISE, работа с GUI, введение устройства в PKI	1,0	0,0	1,0	
3.	Политики доступа на Cisco ISE	7,6	4,2	3,4	Групповой опрос
3.1.	Знакомство со стандартом 802.1X. Обзор MAB-доступа для проводной и беспроводной сети	0,5	0,5	0,0	
3.2.	Источники идентификационных данных	0,7	0,7	0,0	
3.3.	Работа с сертификатами	0,7	0,7	0,0	
3.4.	Лабораторная работа 2: интеграция Cisco ISE с Active Directory	0,7	0,0	0,7	
3.5.	Знакомство с политиками	0,7	0,7	0,0	
3.6.	Настройка Policy Set	0,5	0,5	0,0	
3.7.	Знакомство с Cisco TrustSec	0,3	0,3	0,0	
3.8.	Знакомство с EasyConnect	0,8	0,8	0,0	
3.9.	Лабораторная работа 3: Настройка базовых политик	0,9	0,0	0,9	
3.10.	Лабораторная работа 4: Переход от базовой политики к Policy Set	0,8	0,0	0,8	
3.11.	Лабораторная работа 5: Настройка политики доступа для Easy Connect	1,0	0,0	1,0	
4.	Веб-аутентификация, гостевые порталы	4,8	2,9	1,9	Групповой опрос
4.1.	Знакомство с веб-аутентификацией	0,5	0,5	0,0	
4.2.	Лабораторная работа 6: Настройка	0,9	0,0	0,9	

	гостевого доступа				
4.3.	Знакомство с компонентами гостевых порталов	0,6	0,6	0,0	
4.4.	Настройка параметров гостевого доступа	0,7	0,7	0,0	
4.5.	Лабораторная работа 7: Настройка гостевого доступа	1,0	0,0	1,0	
4.6.	Обзор разных типов порталов: спонсорские/гостевые с подтверждением	0,6	0,6	0,0	
4.7.	Создание отчетов о гостевых пользователях	0,5	0,5	0,0	
5.	Профилирование устройств	4,0	1,3	2,7	Групповой опрос
5.1.	Введение в профилирование	0,7	0,7	0,0	
5.2.	Настройка профилирования на Cisco ISE	0,6	0,6	0,0	
5.3.	Лабораторная работа 9: Настройка сервисов профилирования	0,9	0,0	0,9	
5.4.	Лабораторная работа 10: Настройка различных проб для активного профилирования	1,0	0,0	1,0	
5.5.	Лабораторная работа 11: Создание отчетов о работе сервиса профилирования	0,8	0,0	0,8	
6.	Архитектура BYOD	3,9	2,2	1,7	Групповой опрос
6.1.	Введение в BYOD	0,5	0,5	0,0	
6.2.	Описание работы цикла BYOD на ISE	0,6	0,6	0,0	
6.3.	Настройка параметров портала My Devices Portal	0,6	0,6	0,0	
6.4.	Работа с сертификатами в рамках архитектуры BYOD	0,5	0,5	0,0	
6.5.	Лабораторная работа 12: Настройка основных параметров для работы архитектуры BYOD	0,7	0,0	0,7	
6.6.	Лабораторная работа 13: Помещение пользовательских устройств в Черный список	1,0	0,0	1,0	
7.	Проверка устройств на соответствие корпоративной политике безопасности (Posture)	5,8	1,2	4,6	Групповой опрос
7.1.	Введение в сервис Posture	0,6	0,6	0,0	
7.2.	Лабораторная работа 14: Настройка сервиса Posture	1,0	0,0	1,0	
7.3.	Обзор клиентов для проведения проверки конечного устройства	0,6	0,6	0,0	
7.4.	Лабораторная работа 15: Настройка	0,8	0,0	0,8	

	сервиса Client Provisioning				
7.5.	Лабораторная работа 16: Настройка политики для проверки конечного устройства	0,9	0,0	0,9	
7.6.	Лабораторная работа 17: Проверка работоспособности сервиса Posture	0,9	0,0	0,9	
7.7.	Лабораторная работа 18: Создание отчетов	1,0	0,0	1,0	
8.	Использование Cisco ISE с сервисами AMP и VPN	2,5	0,8	1,7	Групповой опрос
8.1.	Введение в VPN-доступ с использованием Cisco ISE	0,5	0,5	0,0	
8.2.	Лабораторная работа 19: Настройка Cisco ISE для аутентификации VPN-пользователей	0,7	0,0	0,7	
8.3.	Интеграция Cisco AMP с ISE	0,3	0,3	0,0	
8.4.	Лабораторная работа 20: Настройка контроля доступа к сети с использованием механизмов Cisco AMP	1,0	0,0	1,0	
9.	Решения интеграции Cisco ISE с использованием API	2,2	1,4	0,8	Групповой опрос
9.1.	Введение в авторизацию на основе местоположения конечного устройства	0,7	0,7	0,0	
9.2.	Знакомство с Cisco ISE 2.x pxGrid	0,7	0,7	0,0	
9.3.	Лабораторная работа 21: Настройка Cisco ISE pxGrid для интеграции с Cisco WSA	0,8	0,0	0,8	
10.	Работа с функционалом TACACS+	1,8	0,6	1,2	Групповой опрос
10.1.	Настройка TACACS + для администрирования устройств	0,6	0,6	0,0	
10.2.	Лабораторная работа 22: Настройка Cisco ISE для базового администрирования устройств	1,0	0,0	1,0	
10.3.	Лабораторная работа 23: Настройка commands set	0,2	0,0	0,2	
11.	Рекомендации для внедрения Cisco ISE (Опционально/Самообучение)	1,2	1,2	0,0	Групповой опрос
11.1.	Проектирование и внедрение: рекомендации	0,5	0,5	0,0	
11.2.	Механизмы отказоустойчивости и высокой доступности	0,7	0,7	0,0	
12.	Настройка NAD сторонних разработчиков (Опционально/Самообучение)	1,2	1,2	0,0	Групповой опрос
12.1.	Настройка NAD сторонних	1,2	1,2	0,0	

	разработчиков				
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раза в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки	недели	1				
обучения	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Внедрение и настройка решения Cisco Identity Services Engine (SISE)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,7	0,7	0,0	Групповой опрос

2. Знакомство с архитектурой и системой Cisco ISE

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Знакомство с архитектурой и системой Cisco ISE				
2.1	Обзор возможностей платформы Cisco ISE	0,6	0,6	0,0	
2.2	Знакомство с моделями развертывания Cisco ISE	0,7	0,7	0,0	
2.3	Лабораторная работа 1: Первоначальная настройка Cisco ISE, работа с GUI, введение устройства в	1,0	0,0	1,0	

	PKI				
	ИТОГО	2,3	1,3	1,0	Групповой опрос

3. Политики доступа на Cisco ISE

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Политики доступа на Cisco ISE				
3.1	Знакомство со стандартом 802.1X. Обзор MAB-доступа для проводной и беспроводной сети	0,5	0,5	0,0	
3.2	Источники идентификационных данных	0,7	0,7	0,0	
3.3	Работа с сертификатами	0,7	0,7	0,0	
3.4	Лабораторная работа 2: интеграция Cisco ISE с Active Directory	0,7	0,0	0,7	
3.5	Знакомство с политиками	0,7	0,7	0,0	
3.6	Настройка Policy Set	0,5	0,5	0,0	
3.7	Знакомство с Cisco TrustSec	0,3	0,3	0,0	
3.8	Знакомство с EasyConnect	0,8	0,8	0,0	
3.9	Лабораторная работа 3: Настройка базовых политик	0,9	0,0	0,9	
3.10	Лабораторная работа 4: Переход от базовой политики к Policy Set	0,8	0,0	0,8	
3.11	Лабораторная работа 5: Настройка политики доступа для EasyConnect	1,0	0,0	1,0	
	ИТОГО	7,6	4,2	3,4	Групповой опрос

4. Веб-аутентификация, гостевые порталы

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Веб-аутентификация, гостевые порталы				
4.1	Знакомство с веб-аутентификацией	0,5	0,5	0,0	
4.2	Лабораторная работа 6: Настройка гостевого доступа	0,9	0,0	0,9	
4.3	Знакомство с компонентами гостевых порталов	0,6	0,6	0,0	
4.4	Настройка параметров гостевого доступа	0,7	0,7	0,0	
4.5	Лабораторная работа 7: Настройка гостевого доступа	1,0	0,0	1,0	
4.6	Обзор разных типов порталов: спонсорские/гостевые с подтверждением	0,6	0,6	0,0	

4.7	Создание отчетов о гостевых пользователях	0,5	0,5	0,0	
	ИТОГО	4,8	2,9	1,9	Групповой опрос

5. Профилирование устройств

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Профилирование устройств				
5.1	Введение в профилирование	0,7	0,7	0,0	
5.2.	Настройка профилирования на Cisco ISE	0,6	0,6	0,0	
5.3	Лабораторная работа 9: Настройка сервисов профилирования	0,9	0,0	0,9	
5.4	Лабораторная работа 10: Настройка различных проб для активного профилирования	1,0	0,0	1,0	
5.5	Лабораторная работа 11: Создание отчетов о работе сервиса профилирования	0,8	0,0	0,8	
	ИТОГО	4,0	1,3	2,7	Групповой опрос

6. Архитектура BYOD

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Архитектура BYOD				
6.1	Введение в BYOD	0,5	0,5	0,0	
6.2	Описание работы цикла BYOD на ISE	0,6	0,6	0,0	
6.3	Настройка параметров портала My Devices Portal	0,6	0,6	0,0	
6.4	Работа с сертификатами в рамках архитектуры BYOD	0,5	0,5	0,0	
6.5	Лабораторная работа 12: Настройка основных параметров для работы архитектуры BYOD	0,7	0,0	0,7	
6.6	Лабораторная работа 13: Помещение пользовательских устройств в Черный список	1,0	0,0	1,0	
	ИТОГО	3,9	2,2	1,7	Групповой опрос

7. Проверка устройств на соответствие корпоративной политике безопасности (Posture)

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	

7.	Проверка устройств на соответствие корпоративной политике безопасности (Posture)				
7.1	Введение в сервис Posture	0,6	0,6	0,0	
7.2	Лабораторная работа 14: Настройка сервиса Posture	1,0	0,0	1,0	
7.3	Обзор клиентов для проведения проверки конечного устройства	0,6	0,6	0,0	
7.4	Лабораторная работа 15: Настройка сервиса Client Provisioning	0,8	0,0	0,8	
7.5	Лабораторная работа 16: Настройка политики для проверки конечного устройства	0,9	0,0	0,9	
7.6	Лабораторная работа 17: Проверка работоспособности сервиса Posture	0,9	0,0	0,9	
7.7	Лабораторная работа 18: Создание отчетов	1,0	0,0	1,0	
	ИТОГО	5,8	1,2	4,6	Групповой опрос

8. Использование Cisco ISE с сервисами AMP и VPN

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
8.	Использование Cisco ISE с сервисами AMP и VPN				
8.1	Введение в VPN-доступ с использованием Cisco ISE	0,5	0,5	0,0	
8.2.	Лабораторная работа 19: Настройка Cisco ISE для аутентификации VPN-пользователей	0,7	0,0	0,7	
8.3	Интеграция Cisco AMP с ISE	0,3	0,3	0,0	
8.4	Лабораторная работа 20: Настройка контроля доступа к сети с использованием механизмов Cisco AMP	1,0	0,0	1,0	
	ИТОГО	2,5	0,8	1,7	Групповой опрос

9. Решения интеграции Cisco ISE с использованием API

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
9.	Решения интеграции Cisco ISE с использованием API				
9.1	Введение в авторизацию на основе местоположения конечного устройства	0,7	0,7	0,0	
9.2	Знакомство с Cisco ISE 2.x pxGrid	0,7	0,7	0,0	
9.3	Лабораторная работа 21: Настройка Cisco ISE pxGrid для интеграции с Cisco WSA	0,8	0,0	0,8	

	ИТОГО	2,2	1,4	0,8	Групповой опрос
--	--------------	------------	------------	------------	----------------------------

10. Работа с функционалом TACACS+

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
10.	Работа с функционалом TACACS+				
10.1	Настройка TACACS + для администрирования устройств	0,6	0,6	0,0	
10.2	Лабораторная работа 22: Настройка Cisco ISE для базового администрирования устройств	1,0	0,0	1,0	
10.3	Лабораторная работа 23: Настройка commands set	0,2	0,0	0,2	
	ИТОГО	1,8	0,6	1,2	Групповой опрос

11. Рекомендации для внедрения Cisco ISE (Опционально/Самообучение)

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
11.	Рекомендации для внедрения Cisco ISE (Опционально/Самообучение)				
11.1	Проектирование и внедрение: рекомендации	0,5	0,5	0,0	
11.2	Механизмы отказоустойчивости и высокой доступности	0,7	0,7	0,0	
	ИТОГО	1,2	1,2	0,0	Групповой опрос

12. Настройка NAD сторонних разработчиков (Опционально/Самообучение)

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
12.	Настройка NAD сторонних разработчиков (Опционально/Самообучение)				
12.1	Настройка NAD сторонних разработчиков	1,2	1,2	0,0	
	ИТОГО	1,2	1,2	0,0	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Развертывание решений Cisco по контролю за
угрозами в сети (SITCS)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность.....	3
1.2 Цель и задачи реализации программы.....	3
1.3 Планируемые результаты обучения.....	4
1.4 Требования к слушателям.....	5
1.5 Трудоемкость обучения.....	5
1.6 Форма аттестации.....	5
1.7 Форма обучения.....	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план.....	6
2.2 Календарный учебный график	6
2.3 Рабочая программа учебных предметов.....	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.....	12
3.1 Требования к педагогам.....	12
3.2 Материально-техническое оснащение программы.....	12
3.3. Учебно-методическое оснащение программы.....	12
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	12
V. СОСТАВИТЕЛИ ПРОГРАММЫ	13

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Развертывание решений Cisco по контролю за угрозами в сети (SITCS)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 19 мая 2014 года N 316н "Об утверждении профессионального стандарта "Инженер-проектировщик в области связи (телекоммуникаций) " (Зарегистрировано в Минюсте России 10 июля 2014 года, регистрационный N 33047), приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Развертывание решений Cisco по контролю за угрозами в сети (SITCS)» - дать слушателям

знания по внедрению Cisco FirePOWER NGIPS (система предотвращения вторжений следующего поколения) и Cisco AMP (Advanced Malware Protection), а также рассказывает о веб безопасности, безопасности электронной почты и облачной веб безопасности. Вы получите практический опыт в настройке различных усовершенствованных решений безопасности Cisco для устранения внешних угроз и обеспечения безопасности трафика, проходящего через брандмауэр.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Развертывание решений Cisco по контролю за угрозами в сети (SITCS)».

Слушатель должен уметь:

- настраивать Explicit Proxy и пользовательскую аутентификацию на WSA;
- настраивать базовые политики Cisco Email Security Appliance;
- внедрять IPS Cisco FirePOWER следующего поколения.

Слушатель должен знать:

- идентификаторы устройств Cisco Web Security и средства проверки подлинности пользователя;
- технологии обнаружения устройств и объектов в сети.

Слушатель должен владеть:

- навыками настройки различных усовершенствованных решений безопасности Cisco для устранения внешних угроз и обеспечения безопасности трафика.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Развертывание решений Cisco по контролю за угрозами в сети (SITCS)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,5	0,5	0,0	Групповой опрос
2.	Платформа Cisco Web Security Appliance	6,1	4,9	1,2	Групповой опрос
2.1.	Описание решений Cisco Web Security Appliance	0,8	0,8	0,0	
2.2.	Интеграция Cisco Web Security Appliance	0,7	0,7	0,0	
2.3.	Настройка идентификаторов устройств Cisco Web Security и средств проверки подлинности пользователя	0,7	0,7	0,0	
2.4.	Настройка элементов Anti-Malware для Cisco Web Security	0,6	0,6	0,0	
2.5.	Дешифрование трафика	0,7	0,7	0,0	
2.6.	Настройка элементов безопасности Cisco Web Security Appliance	0,7	0,7	0,0	
2.7.	Описание решений Cisco Web Security Appliance	0,7	0,7	0,0	
2.8.	Лабораторная работа 1: Настройка Explicit Proxy и пользовательской аутентификации на WSA	1,2	0,0	1,2	
3.	Cisco Email Security Appliance	3,2	1,8	1,4	Групповой опрос
3.1.	Описание решений Cisco для защиты электронной почты	0,8	0,8	0,0	
3.2.	Описание компонентов и базовой настройки Cisco Email Security Appliance	0,4	0,4	0,0	
3.3.	Настройка политики для входящих и исходящих почтовых сообщений	0,6	0,6	0,0	
3.4.	Лабораторная работа 2: Настройка базовых политик на ESA	1,4	0,0	1,4	
4.	Расширенная защита от вредоносных программ для конечных точек	10,1	3,5	6,6	Групповой опрос

4.1.	Обзор AMP для конечных точек	0,7	0,7	0,0	
4.2.	Настройка обнаружения и политики AMP	0,6	0,6	0,0	
4.3.	IOC и IOC Scanning	0,7	0,7	0,0	
4.4.	Внедрение AMP Connectors в сети	0,8	0,8	0,0	
4.5.	Инструменты анализа	0,7	0,7	0,0	
4.6.	Лабораторная работа 3: Консоль AMP Public Cloud	1,3	0,0	1,3	
4.7.	Лабораторная работа 4: Настройка политики AMP	1,1	0,0	1,1	
4.8.	Лабораторная работа 5: IOC и IOC Scanning	1,4	0,0	1,4	
4.9.	Лабораторная работа 6: Внедрение AMP Connectors	1,4	0,0	1,4	
4.10.	Лабораторная работа 7: Расширенные механизмы анализа AMP	1,4	0,0	1,4	
5.	IPS Cisco FirePOWER следующего поколения	17,5	7,7	9,8	Групповой опрос
5.1.	Описание системы Cisco FireSIGHT	0,7	0,7	0,0	
5.2.	Настройка и управление устройствами Cisco FirePOWER	0,7	0,7	0,0	
5.3.	Внедрение политики контроля доступа	0,7	0,7	0,0	
5.4.	Понимание технологии обнаружения устройств и объектов в сети	0,8	0,8	0,0	
5.5.	Настройка обнаружения файлов и сетевых вредоносных программ	0,7	0,7	0,0	
5.6.	Управление трафиком SSL с помощью Cisco FireSIGHT	0,8	0,8	0,0	Групповой опрос
5.7.	Описание политики IPS	0,6	0,6	0,0	
5.8.	Описание политики сетевого анализа	0,7	0,7	0,0	
5.9.	Создание отчетов	0,7	0,7	0,0	
5.10.	Описание правил и политик корреляции	0,6	0,6	0,0	
5.11.	Синтаксис и использование Snort-правил	0,7	0,7	0,0	
5.12.	Лабораторная работа 8: Настройка интерфейсов и создание объектов	1,2	0,0	1,2	
5.13.	Лабораторная работа 9: Создание правил для политики контроля доступа	1,5	0,0	1,5	
5.14.	Лабораторная работа 10: Настройка политики сетевого обнаружения объектов	1,1	0,0	1,1	
5.15.	Лабораторная работа 11: Создание файловой политики	1,2	0,0	1,2	

5.16.	Лабораторная работа 12: Создание политики IPS	1,4	0,0	1,4	
5.17.	Лабораторная работа 13: Создание политики сетевого анализа	1,2	0,0	1,2	
5.18.	Лабораторная работа 14: Отчетность	1,4	0,0	1,4	
5.19.	Лабораторная работа 15: Настройка механизмов корреляции	0,8	0,0	0,8	
6.	Модуль обслуживания Cisco ASA FirePOWER	0,6	0,6	0,0	Групповой опрос
6.1.	Установка модуля обслуживания Cisco FireWare (SFR) Cisco ASA 5500-X	0,6	0,6	0,0	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут).
Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации
«Развертывание решений Cisco по контролю за угрозами в сети (SITCS)».
Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,5	0,5	0,0	Групповой опрос

2. Платформа Cisco Web Security Appliance

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Платформа Cisco Web Security Appliance				
2.1	Описание решений Cisco Web Security Appliance	0,8	0,8	0,0	
2.2	Интеграция Cisco Web Security Appliance	0,7	0,7	0,0	
2.3	Настройка идентификаторов устройств Cisco Web Security и средств проверки подлинности пользователя	0,7	0,7	0,0	
2.4	Настройка элементов Anti-Malware для Cisco Web Security	0,6	0,6	0,0	
2.5	Дешифрование трафика	0,7	0,7	0,0	
2.6	Настройка элементов безопасности Cisco Web Security Appliance	0,7	0,7	0,0	
2.7	Описание решений Cisco Web Security Appliance	0,7	0,7	0,0	
2.8	Лабораторная работа 1: Настройка Explicit Proxy и пользовательской аутентификации на WSA	1,2	0,0	1,2	
	ИТОГО	6,1	4,9	1,2	Групповой опрос

3. Cisco Email Security Appliance

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Cisco Email Security Appliance				
3.1	Описание решений Cisco для защиты электронной почты	0,8	0,8	0,0	
3.2	Описание компонентов и базовой настройки Cisco Email Security Appliance	0,4	0,4	0,0	
3.3	Настройка политики для входящих и исходящих почтовых сообщений	0,6	0,6	0,0	
3.4	Лабораторная работа 2: Настройка базовых политик на ESA	1,4	0,0	1,4	
	ИТОГО	3,2	1,8	1,4	Групповой опрос

4. Расширенная защита от вредоносных программ для конечных точек

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Расширенная защита от вредоносных программ для конечных точек				

4.1	Обзор AMP для конечных точек	0,7	0,7	0,0	
4.2	Настройка обнаружения и политики AMP	0,6	0,6	0,0	
4.3	IOC и IOC Scanning	0,7	0,7	0,0	
4.4	Внедрение AMP Connectors в сети	0,8	0,8	0,0	
4.5	Инструменты анализа	0,7	0,7	0,0	
4.6	Лабораторная работа 3: Консоль AMP Public Cloud	1,3	0,0	1,3	
4.7	Лабораторная работа 4: Настройка политики AMP	1,1	0,0	1,1	
4.8	Лабораторная работа 5: IOC и IOC Scanning	1,4	0,0	1,4	
4.9	Лабораторная работа 6: Внедрение AMP Connectors	1,4	0,0	1,4	
4.10	Лабораторная работа 7: Расширенные механизмы анализа AMP	1,4	0,0	1,4	
	ИТОГО	10,1	3,5	6,6	Групповой опрос

5. IPS Cisco FirePOWER следующего поколения

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	IPS Cisco FirePOWER следующего поколения				
5.1	Описание системы Cisco FireSIGHT	0,7	0,7	0,0	
5.2	Настройка и управление устройствами Cisco FirePOWER	0,7	0,7	0,0	
5.3	Внедрение политики контроля доступа	0,7	0,7	0,0	
5.4	Понимание технологии обнаружения устройств и объектов в сети	0,8	0,8	0,0	
5.5	Настройка обнаружения файлов и сетевых вредоносных программ	0,7	0,7	0,0	
5.6	Управление трафиком SSL с помощью Cisco FireSIGHT	0,8	0,8	0,0	Групповой опрос
5.7	Описание политики IPS	0,6	0,6	0,0	
5.8	Описание политики сетевого анализа	0,7	0,7	0,0	
5.9	Создание отчетов	0,7	0,7	0,0	
5.10	Описание правил и политик корреляции	0,6	0,6	0,0	
5.11	Синтаксис и использование Snort-правил	0,7	0,7	0,0	
5.12	Лабораторная работа 8: Настройка интерфейсов и создание объектов	1,2	0,0	1,2	
5.13	Лабораторная работа 9: Создание правил для политики контроля	1,5	0,0	1,5	

	доступа				
5.14	Лабораторная работа 10: Настройка политики сетевого обнаружения объектов	1,1	0,0	1,1	
5.15	Лабораторная работа 11: Создание файловой политики	1,2	0,0	1,2	
5.16	Лабораторная работа 12: Создание политики IPS	1,4	0,0	1,4	
5.17	Лабораторная работа 13: Создание политики сетевого анализа	1,2	0,0	1,2	
5.18	Лабораторная работа 14: Отчетность	1,4	0,0	1,4	
5.19	Лабораторная работа 15: Настройка механизмов корреляции	0,8	0,0	0,8	
	ИТОГО	17,5	7,7	9,8	Групповой опрос

6. Модуль обслуживания Cisco ASA FirePOWER

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Модуль обслуживания Cisco ASA FirePOWER				
6.1	Установка модуля обслуживания Cisco FireWare (SFR) Cisco ASA 5500-X	0,6	0,6	0,0	
	ВСЕГО	0,6	0,6	0,0	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомолов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Управление безопасностью предприятия с помощью
Cisco Security Manager (CSM) (CI-SSECMGT)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	4
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	8
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	12
3.1 Требования к педагогам	12
3.2 Материально-техническое оснащение программы	12
3.3 Учебно-методическое оснащение программы	12
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	12
V. СОСТАВИТЕЛИ ПРОГРАММЫ	13

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Управление безопасностью предприятия с помощью Cisco Security Manager (CSM) (CI-SSECMGT)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 05.10.2015 N 686н "Об утверждении профессионального стандарта "Специалист по администрированию сетевых устройств информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 30.10.2015 N 39568), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Управление безопасностью предприятия с помощью Cisco Security Manager (CSM) (CI-SSECMGT)» - дать слушателям необходимые знания для внедрения и настройки Cisco Security Manager. В ходе обучения рассматриваются различные технологии, применяемые

в области сетевой безопасности, сопровождаемые разбором кейсов (case study), где наглядно демонстрируются некоторые сценарии внедрения.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Управление безопасностью предприятия с помощью Cisco Security Manager (CSM) (CI-SSECMGT)».

Слушатель должен уметь:

- применять CSM для управления устройствами, политиками и объектами;
- управлять сервисами межсетевого экрана.

Слушатель должен знать:

- принципы управления VPN;
- процесс интеграции между CSM и Cisco ACS.

Слушатель должен владеть:

- навыками использования инструментов: мониторинга, поиска и устранения неисправностей в сети, диагностики.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 40 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Управление безопасностью предприятия с помощью Cisco Security Manager
(CSM) (CI-SSECMGT)»

Срок обучения: 40 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,8	0,8	0,0	Групповой опрос
2.	Обзор CSM	7,4	3,4	4,0	Групповой опрос
2.1.	Применение CSM	0,7	0,7	0,0	
2.2.	Управление устройствами	0,8	0,8	0,0	
2.3.	Управление политиками	0,9	0,9	0,0	
2.4.	Управление объектами	0,4	0,4	0,0	
2.5.	Использование Map View	0,6	0,6	0,0	
2.6.	Лабораторная работа 1: Настройка загрузочных процессов устройств, проверка доступности	0,9	0,0	0,9	
2.7.	Лабораторная работа 2: Импорт устройств	1,1	0,0	1,1	
2.8.	Лабораторная работа 3: Определение ролей интерфейсов	1,1	0,0	1,1	
2.9.	Лабораторная работа 4: Создание объектов для политик	0,9	0,0	0,9	
3.	Управление политиками межсетевого экрана	5,6	2,2	3,4	Групповой опрос
3.1.	Управление сервисами межсетевого экрана	0,8	0,8	0,0	
3.2.	Управление межсетевыми экранами	0,8	0,8	0,0	
3.3.	Мониторинг событий и корреляция правил для межсетевых экранов	0,6	0,6	0,0	
3.4.	Лабораторная работа 5: Управление политиками для МСЭ	1,1	0,0	1,1	
3.5.	Лабораторная работа 6: Настройка NAT	1,3	0,0	1,3	
3.6.	Лабораторная работа 7: Настройка мониторинга событий для МСЭ, корреляция	1,0	0,0	1,0	
4.	Управление политиками VPN	14,0	6,1	7,9	Групповой опрос
4.1.	Управление VPN	0,7	0,7	0,0	

4.2.	Управление удаленным доступом IPsec VPN	0,6	0,6	0,0	
4.3.	Конфигурирование Client-Based SSL VPN	0,6	0,6	0,0	
4.4.	Конфигурирование Clientless SSL VPN	0,7	0,7	0,0	
4.5.	Настройка расширенных функций VPN	0,8	0,8	0,0	
4.6.	Лабораторная работа 8: Управление VPN инфраструктурой с использованием Cisco AnyConnect	1,3	0,0	1,3	
4.7.	Лабораторная работа 9: Управление Clientless SSL VPN	1,2	0,0	1,2	
4.8.	Лабораторная работа 10: Управление инфраструктурой DMVPN	1,1	0,0	1,1	
4.9.	Лабораторная работа 11: Управление инфраструктурой GET VPN	1,0	0,0	1,0	
4.10.	Управление системами Cisco IPS	0,9	0,9	0,0	
4.11.	Управление сервисами Cisco IPS	0,5	0,5	0,0	
4.12.	Управление устройствами Cisco IPS	0,5	0,5	0,0	
4.13.	Управление событиями Cisco IPS	0,8	0,8	0,0	
4.14.	Лабораторная работа 12: Настройка Cisco IOS IPS	1,1	0,0	1,1	
4.15.	Лабораторная работа 13: Настройка модулей IPS	1,1	0,0	1,1	
4.16.	Лабораторная работа 14: Настройка мониторинга событий для IPS, корреляция	1,1	0,0	1,1	
5.	Работа с устройствами Cisco IOS	3,6	1,4	2,2	Групповой опрос
5.1.	Управление роутерами	0,9	0,9	0,0	
5.2.	Использование Device Manager для коммутатора Cisco Catalyst 6500 Series и маршрутизатора Cisco 7600 Series Router	0,5	0,5	0,0	
5.3.	Лабораторная работа 15: Настройка маршрутизаторов с ОС Cisco IOS	1,1	0,0	1,1	
5.4.	Лабораторная работа 16: Управление DHCP-устройствами с помощью CiscoWorks Auto Update Server	1,1	0,0	1,1	
6.	Обзор VPN-компонентов для Cisco ASA	2,3	2,3	0,0	Групповой опрос
6.1.	Обзор технологий VPN	0,8	0,8	0,0	
6.2.	Реализация профилей, групповых политик и пользовательских политик	0,8	0,8	0,0	
6.3.	Внедрение сервисов PKI	0,7	0,7	0,0	
7.	Анализ сервиса FlexConfigs в CSM	4,3	2,8	1,5	Групповой опрос

7.1.	Управление FlexConfigs	0,7	0,7	0,0	
7.2.	Управление активностями и процессами внедрения	0,7	0,7	0,0	
7.3.	Процесс интеграции между CSM и Cisco ACS	0,7	0,7	0,0	
7.4.	Сохранение резервных копий и восстановление баз данных CSM	0,6	0,6	0,0	
7.5.	Использование инструментов: мониторинга, поиска и устранения неисправностей в сети, диагностики	0,1	0,1	0,0	
7.6.	Лабораторная работа 17: Настройка FlexConfigs	1,0	0,0	1,0	
7.7.	Лабораторная работа 18: Интеграция ACS и CSM	0,5	0,0	0,5	
	Всего:	38	19	19	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	40	19	19	

2.2 Календарный учебный график

Занятия проводятся 5 раз в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1				
	дни	1	1	1	1	1
Вид занятий		А	А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Управление безопасностью предприятия с помощью Cisco Security Manager (CSM) (CI-SSECMGT)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,8	0,8	0,0	Групповой опрос

2. Обзор CSM

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Обзор CSM				
2.1.	Применение CSM	0,7	0,7	0,0	
2.2.	Управление устройствами	0,8	0,8	0,0	
2.3.	Управление политиками	0,9	0,9	0,0	
2.4.	Управление объектами	0,4	0,4	0,0	
2.5.	Использование Map View	0,6	0,6	0,0	
2.6.	Лабораторная работа 1: Настройка загрузочных процессов устройств, проверка доступности	0,9	0,0	0,9	
2.7.	Лабораторная работа 2: Импорт устройств	1,1	0,0	1,1	
2.8	Лабораторная работа 3: Определение ролей интерфейсов	1,1	0,0	1,1	
2.9	Лабораторная работа 4: Создание объектов для политик	0,9	0,0	0,9	
	ИТОГО	7,4	3,4	4,0	Групповой опрос

3. Управление политиками межсетевого экрана

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Управление политиками межсетевого экрана				
3.1.	Управление сервисами межсетевого экрана	0,8	0,8	0,0	
3.2.	Управление межсетевыми экранами	0,8	0,8	0,0	
3.3.	Мониторинг событий и корреляция правил для межсетевых экранов	0,6	0,6	0,0	
3.4.	Лабораторная работа 5: Управление политиками для МСЭ	1,1	0,0	1,1	
3.5.	Лабораторная работа 6: Настройка NAT	1,3	0,0	1,3	
3.6.	Лабораторная работа 7: Настройка мониторинга событий для МСЭ, корреляция	1,0	0,0	1,0	
	ИТОГО	5,6	2,2	3,4	Групповой опрос

4. Управление политиками VPN

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические	

				занятия	
4.	Управление политиками VPN				
4.1.	Управление VPN	0,7	0,7	0,0	
4.2.	Управление удаленным доступом IPsec VPN	0,6	0,6	0,0	
4.3.	Конфигурирование Client-Based SSL VPN	0,6	0,6	0,0	
4.4.	Конфигурирование Clientless SSL VPN	0,7	0,7	0,0	
4.5.	Настройка расширенных функций VPN	0,8	0,8	0,0	
4.6.	Лабораторная работа 8: Управление VPN инфраструктурой с использованием Cisco AnyConnect	1,3	0,0	1,3	
4.7.	Лабораторная работа 9: Управление Clientless SSL VPN	1,2	0,0	1,2	
4.8.	Лабораторная работа 10: Управление инфраструктурой DMVPN	1,1	0,0	1,1	
4.9.	Лабораторная работа 11: Управление инфраструктурой GET VPN	1,0	0,0	1,0	
4.10.	Управление системами Cisco IPS	0,9	0,9	0,0	
4.11.	Управление сервисами Cisco IPS	0,5	0,5	0,0	
4.12.	Управление устройствами Cisco IPS	0,5	0,5	0,0	
4.13.	Управление событиями Cisco IPS	0,8	0,8	0,0	
4.14.	Лабораторная работа 12: Настройка Cisco IOS IPS	1,1	0,0	1,1	
4.15.	Лабораторная работа 13: Настройка модулей IPS	1,1	0,0	1,1	
4.16.	Лабораторная работа 14: Настройка мониторинга событий для IPS, корреляция	1,1	0,0	1,1	
	ИТОГО	14,0	6,1	7,9	Групповой опрос

5. Работа с устройствами Cisco IOS

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Работа с устройствами Cisco IOS				
5.1.	Управление роутерами	0,9	0,9	0,0	
5.2.	Использование Device Manager для коммутатора Cisco Catalyst 6500 Series и маршрутизатора Cisco 7600 Series Router	0,5	0,5	0,0	
5.3.	Лабораторная работа 15: Настройка маршрутизаторов с ОС Cisco IOS	1,1	0,0	1,1	

5.4.	Лабораторная работа 16: Управление DHCP-устройствами с помощью CiscoWorks Auto Update Server	1,1	0,0	1,1	
	ИТОГО	3,6	1,4	2,2	Групповой опрос

6. Обзор VPN-компонентов для Cisco ASA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Обзор VPN-компонентов для Cisco ASA				
6.1.	Обзор технологий VPN	0,8	0,8	0,0	
6.2.	Реализация профилей, групповых политик и пользовательских политик	0,8	0,8	0,0	
6.3.	Внедрение сервисов PKI	0,7	0,7	0,0	
	ИТОГО	2,3	2,3	0,0	Групповой опрос

7. Анализ сервиса FlexConfigs в CSM

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
7.	Анализ сервиса FlexConfigs в CSM				
7.1.	Управление FlexConfigs	0,7	0,7	0,0	
7.2.	Управление активностями и процессами внедрения	0,7	0,7	0,0	
7.3.	Процесс интеграции между CSM и Cisco ACS	0,7	0,7	0,0	
7.4.	Сохранение резервных копий и восстановление баз данных CSM	0,6	0,6	0,0	
7.5.	Использование инструментов: мониторинга, поиска и устранения неисправностей в сети, диагностики	0,1	0,1	0,0	
7.6.	Лабораторная работа 17: Настройка FlexConfigs	1,0	0,0	1,0	
7.7	Лабораторная работа 18: Интеграция ACS и CSM	0,5	0,0	0,5	
	ИТОГО	4,3	2,8	1,5	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Защита от вредоносного ПО с помощью Cisco AMP
для конечных точек (SSFAMP)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	3
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	4
1.5 Трудоемкость обучения	4
1.6 Форма аттестации	4
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	8
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	12
3.1 Требования к педагогам	12
3.2 Материально-техническое оснащение программы	12
3.3 Учебно-методическое оснащение программы	12
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	12
V. СОСТАВИТЕЛИ ПРОГРАММЫ	13

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Защита от вредоносного ПО с помощью Cisco AMP для конечных точек (SSFAMP)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 05.10.2015 N 686н "Об утверждении профессионального стандарта "Специалист по администрированию сетевых устройств информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 30.10.2015 N 39568), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Защита от вредоносного ПО с помощью Cisco AMP для конечных точек (SSFAMP)» - предоставить слушателям знания о защите от современных методов атак, вредоносных программ, эксплойтов и бот-сетей. В ходе обучения слушатели познакомятся с решением Cisco Advanced Malware Protection для конечных точек.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Защита от вредоносного ПО с помощью Cisco AMP для конечных точек (SSFAMP)».

Слушатель должен уметь:

- обнаруживать вредоносные программы;
- настраивать политики для конечных точек, защищенных AMP.

Слушатель должен знать:

- индивидуальные функции безопасности операционных систем;
- векторы современных атак и тренды.

Слушатель должен владеть:

- навыками предотвращения распространения вредоносного ПО.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 24 часа, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Защита от вредоносного ПО с помощью Cisco AMP для конечных точек
(SSFAMP)»

Срок обучения: 24 часа.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,3	0,3	0,0	Групповой опрос
2.	Современное вредоносное ПО	0,4	0,4	0,0	Групповой опрос
2.1.	Что такое Malware?	0,4	0,4	0,0	
3.	Особенности операционных систем	0,8	0,8	0,0	Групповой опрос
3.1.	Индивидуальные функции безопасности операционных систем	0,5	0,5	0,0	
3.2.	Распространенные уязвимости	0,3	0,3	0,0	
4.	Эксплойты и бот-сети	0,8	0,8	0,0	Групповой опрос
4.1.	Exploits	0,4	0,4	0,0	
4.2.	Изучение бот-сетей	0,4	0,4	0,0	
5.	Векторы современных атак и тренды	2,4	0,9	1,5	Групповой опрос
5.1.	Векторы атак	0,4	0,4	0,0	
5.2.	Тренды	0,5	0,5	0,0	
5.3.	Лабораторная работа 1: Типичное поведение вредоносного ПО	1,5	0,0	1,5	
6.	Обзор и архитектура системы AMP for Endpoints	1,0	1,0	0,0	Групповой опрос
6.1.	Исследование механизма AMP для конечных точек	0,5	0,5	0,0	
6.2.	Исследование AMP Cloud	0,3	0,3	0,0	
6.3.	Обзор приватного облака для работы сервиса AMP	0,2	0,2	0,0	
7.	Консольный интерфейс и навигация	2,2	0,9	1,3	Групповой опрос
7.1.	Первоначальные настройки	0,3	0,3	0,0	
7.2.	Статистика и функции мониторинга	0,6	0,6	0,0	
7.3.	Лабораторная работа 2: Доступ к AMP для оконечных устройств	1,3	0,0	1,3	

8.	Предотвращение распространения вредоносного ПО	2,0	0,7	1,3	Групповой опрос
8.1.	Обнаружение вредоносных программ	0,5	0,5	0,0	
8.2.	Настройка индикаторов компрометации	0,2	0,2	0,0	
8.3.	Лабораторная работа 3: Предотвращение распространения вредоносного ПО	1,3	0,0	1,3	
9.	Политики управления оконечными устройствами	2,0	0,6	1,4	Групповой опрос
9.1.	Обзор политики для конечных точек	0,6	0,6	0,0	
9.2.	Лабораторная работа 4: Настройка политик для конечных точек, защищенных AMP	1,4	0,0	1,4	
10.	Группы и их внедрение	3,8	2,5	1,3	Групповой опрос
10.1.	Создание групп	0,4	0,4	0,0	
10.2.	Настройка исключений	0,6	0,6	0,0	
10.3.	Подготовка к внедрению	0,4	0,4	0,0	
10.4.	Внедрение Windows Connectors	0,3	0,3	0,0	
10.5.	Интерфейс Windows Connector	0,4	0,4	0,0	
10.6.	Поиск и устранение неполадок в работе	0,4	0,4	0,0	
10.7.	Лабораторная работа 5: Группы и их внедрение	1,3	0,0	1,3	
11.	Анализ угроз	4,3	1,5	2,8	Групповой опрос
11.1.	Анализ событий	0,4	0,4	0,0	
11.2.	Анализ файлов	0,5	0,5	0,0	
11.3.	Траектория файлов	0,3	0,3	0,0	
11.4.	Дополнительные функции	0,3	0,3	0,0	
11.5.	Лабораторная работа 6: Анализ угроз	1,5	0,0	1,5	
11.6.	Лабораторная работа 7: Zbot анализ	1,3	0,0	1,3	
12.	Примеры анализа угроз	0,6	0,6	0,0	Групповой опрос
12.1.	Обнаружение вредоносного ПО	0,3	0,3	0,0	
12.2.	ZeroAccess	0,3	0,3	0,0	
13.	Учетные записи пользователей	2,4	0,5	1,9	Групповой опрос
13.1.	Управление пользователями	0,3	0,3	0,0	
13.2.	Дополнительные функции	0,2	0,2	0,0	
13.3.	Лабораторная работа 8: Учетные записи пользователей	1,9	0,0	1,9	
	Всего:	23	11,5	11,5	
	Итоговый контроль знаний	1	0	0	Электронное тестирование

	Итого:	24	11,5	11,5	
--	---------------	-----------	-------------	-------------	--

2.2 Календарный учебный график

Занятия проводятся 3 раза в неделю по 8 академических часов (1 ак. час - 45 минут).
Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1		
	дни	1	1	1
Вид занятий		А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Защита от вредоносного ПО с помощью Cisco AMP для конечных точек (SSFAMP)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,3	0,3	0,0	Групповой опрос

2. Современное вредоносное ПО

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Современное вредоносное ПО				
2.1.	Что такое Malware?	0,4	0,4	0,0	
	ИТОГО	0,4	0,4	0,0	Групповой опрос

3. Особенности операционных систем

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Особенности операционных систем				
3.1.	Индивидуальные функции	0,5	0,5	0,0	

	безопасности операционных систем				
3.2.	Распространенные уязвимости	0,3	0,3	0,0	
	ИТОГО	0,8	0,8	0,0	Групповой опрос

4. Эксплойты и бот-сети

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Эксплойты и бот-сети				
4.1.	Exploits	0,4	0,4	0,0	
4.2.	Изучение бот-сетей	0,4	0,4	0,0	
	ИТОГО	0,8	0,8	0,0	Групповой опрос

5. Векторы современных атак и тренды

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Векторы современных атак и тренды				
5.1.	Векторы атак	0,4	0,4	0,0	
5.2.	Тренды	0,5	0,5	0,0	
5.3.	Лабораторная работа 1: Типичное поведение вредоносного ПО	1,5	0,0	1,5	
	ИТОГО	2,4	0,9	1,5	Групповой опрос

6. Обзор и архитектура системы AMP for Endpoints

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Обзор и архитектура системы AMP for Endpoints				
6.1.	Исследование механизма AMP для конечных точек	0,5	0,5	0,0	
6.2.	Исследование AMP Cloud	0,3	0,3	0,0	
6.3.	Обзор приватного облака для работы сервиса AMP	0,2	0,2	0,0	
	ИТОГО	1,0	1,0	0,0	Групповой опрос

7. Консольный интерфейс и навигация

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
7.	Консольный интерфейс и навигация				
7.1.	Первоначальные настройки	0,3	0,3	0,0	

7.2.	Статистика и функции мониторинга	0,6	0,6	0,0	
7.3.	Лабораторная работа 2: Доступ к АМР для конечных устройств	1,3	0,0	1,3	
	ИТОГО	2,2	0,9	1,3	Групповой опрос

8. Предотвращение распространения вредоносного ПО

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
8.	Предотвращение распространения вредоносного ПО				
8.1.	Обнаружение вредоносных программ	0,5	0,5	0,0	
8.2.	Настройка индикаторов компрометации	0,2	0,2	0,0	
8.3.	Лабораторная работа 3: Предотвращение распространения вредоносного ПО	1,3	0,0	1,3	
	ИТОГО	2,0	0,7	1,3	Групповой опрос

9. Политики управления конечными устройствами

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
9.	Политики управления оконечными устройствами				
9.1.	Обзор политики для конечных точек	0,6	0,6	0,0	
9.2.	Лабораторная работа 4: Настройка политик для конечных точек, защищенных AMP	1,4	0,0	1,4	
	ИТОГО	2,0	0,6	1,4	Групповой опрос

10. Группы и их внедрение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
10.	Группы и их внедрение				
10.1.	Создание групп	0,4	0,4	0,0	
10.2.	Настройка исключений	0,6	0,6	0,0	
10.3.	Подготовка к внедрению	0,4	0,4	0,0	
10.4.	Внедрение Windows Connectors	0,3	0,3	0,0	
10.5.	Интерфейс Windows Connector	0,4	0,4	0,0	
10.6.	Поиск и устранение неполадок в работе	0,4	0,4	0,0	
10.7.	Лабораторная работа 5: Группы и их внедрение	1,3	0,0	1,3	

	ИТОГО	3,8	2,5	1,3	Групповой опрос
--	--------------	------------	------------	------------	----------------------------

11. Анализ угроз

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
11.	Анализ угроз				
11.1.	Анализ событий	0,4	0,4	0,0	
11.2.	Анализ файлов	0,5	0,5	0,0	
11.3.	Траектория файлов	0,3	0,3	0,0	
11.4.	Дополнительные функции	0,3	0,3	0,0	
11.5.	Лабораторная работа 6: Анализ угроз	1,5	0,0	1,5	
11.6.	Лабораторная работа 7: Zbot анализ	1,3	0,0	1,3	
	ИТОГО	4,3	1,5	2,8	Групповой опрос

12. Примеры анализа угроз

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
12.	Примеры анализа угроз				
12.1.	Обнаружение вредоносного ПО	0,3	0,3	0,0	
12.2.	ZeroAccess	0,3	0,3	0,0	
	ИТОГО	0,6	0,6	0,0	Групповой опрос

13. Учетные записи пользователей

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
13.	Учетные записи пользователей				
13.1.	Управление пользователями	0,3	0,3	0,0	
13.2.	Дополнительные функции	0,2	0,2	0,0	
13.3.	Лабораторная работа 8: Учетные записи пользователей	1,9	0,0	1,9	
	ИТОГО	2,4	0,5	1,9	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г

М.П.



**Дополнительная профессиональная программа
повышения квалификации**

**«Защита сетей с помощью платформы Cisco Firepower
Next-Generation IPS (CI-SSFIPS)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность.....	3
1.2 Цель и задачи реализации программы.....	3
1.3 Планируемые результаты обучения.....	4
1.4 Требования к слушателям.....	4
1.5 Трудоемкость обучения.....	5
1.6 Форма аттестации.....	5
1.7 Форма обучения.....	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план.....	6
2.2 Календарный учебный график	8
2.3 Рабочая программа учебных предметов.....	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.....	14
3.1 Требования к педагогам.....	14
3.2 Материально-техническое оснащение программы.....	14
3.3. Учебно-методическое оснащение программы.....	14
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	14
V. СОСТАВИТЕЛИ ПРОГРАММЫ	15

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Защита сетей с помощью платформы Cisco Firepower Next-Generation IPS (CI-SSFIPS)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 19 мая 2014 года N 316н "Об утверждении профессионального стандарта "Инженер-проектировщик в области связи (телекоммуникаций) " (Зарегистрировано в Минюсте России 10 июля 2014 года, регистрационный N 33047), приказом Минтруда России от 05.10.2015 N 686н "Об утверждении профессионального стандарта "Специалист по администрированию сетевых устройств информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 30.10.2015 N 39568), приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации

«Защита сетей с помощью платформы Cisco Firepower Next-Generation IPS (CI-SSFIPS)» - научить слушателей основным принципам работы систем предотвращения вторжений нового поколения (NGIPS), детально разбирая платформу Cisco Firepower.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Защита сетей с помощью платформы Cisco Firepower Next-Generation IPS (CI-SSFIPS)».

Слушатель должен уметь:

- настраивать политики Network Discovery;
- настраивать политики контроля доступа;
- работать с шифрованным трафиком.

Слушатель должен знать:

- основные принципы работы систем предотвращения вторжений нового поколения;
- основные компоненты системы Firepower.

Слушатель должен владеть:

- навыками внедрения системы Cisco Firepower, оптимальной настройки политик, использования сервисов проверки файлов в сети.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 32 часа, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Защита сетей с помощью платформы Cisco Firepower Next-Generation IPS (CI-
SSFIPS)»

Срок обучения: 32 часа.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,5	0,5	0,0	Групповой опрос
2.	Обзор технологий безопасности	0,5	0,5	0,0	Групповой опрос
2.1.	Сравнение и анализ систем предотвращения вторжений и межсетевых экранов	0,5	0,5	0,0	
3.	Компоненты системы Cisco Firepower, основные функции	2,3	1,0	1,3	Групповой опрос
3.1.	Обзор системы	0,3	0,3	0,0	
3.2.	Основные компоненты системы Firepower	0,4	0,4	0,0	
3.3.	Процесс внедрения Firepower	0,3	0,3	0,0	
3.4.	Лабораторная работа 1: Подключение к лабораторному стенду	1,3	0,0	1,3	
4.	Обзор Cisco Firepower MGMT Center	2,0	0,8	1,2	Групповой опрос
4.1.	Исследование GUI	0,4	0,4	0,0	
4.2.	Введение в политики	0,4	0,4	0,0	
4.3.	Лабораторная работа 2: Изучение функций Cisco Firepower MGMT Center	1,2	0,0	1,2	
5.	Подключение управляемых устройств	2,5	1,3	1,2	Групповой опрос
5.1.	Обзор дизайнов внедрения системы	0,5	0,5	0,0	
5.2.	Управляемые устройства	0,4	0,4	0,0	
5.3.	Система лицензирования	0,4	0,4	0,0	
5.4.	Лабораторная работа 3: Настройка FTD устройств	1,2	0,0	1,2	
6.	NAT для Firepower Threat Defense	1,5	0,2	1,3	Групповой опрос
6.1.	Обзор методов трансляции сетевых адресов в FTD	0,2	0,2	0,0	
6.2.	Лабораторная работа 4: Настройка	1,3	0,0	1,3	

	NAT				
7.	QoS на Firepower	0,4	0,4	0,0	
7.1.	Обзор механизмов QoS	0,4	0,4	0,0	
8.	Механизм анализа сети Firepower Discovery	2,5	1,4	1,1	Групповой опрос
8.1.	Обзор	0,5	0,5	0,0	
8.2.	Анализ профиля хоста	0,5	0,5	0,0	
8.3.	Работа с идентификационной информацией пользователя	0,4	0,4	0,0	
8.4.	Лабораторная работа 5: Настройка политики Network Discovery	1,1	0,0	1,1	
9.	Политика контроля доступа к ресурсам	4,7	2,2	2,5	Групповой опрос
9.1.	Введение	0,4	0,4	0,0	
9.2.	Исследование базы объектов	0,4	0,4	0,0	
9.3.	Анализ списка правил, дефолтное действие	0,3	0,3	0,0	
9.4.	Расширенные функции	0,6	0,6	0,0	
9.5.	Рекомендации для внедрения политики контроля доступа	0,5	0,5	0,0	
9.6.	Лабораторная работа 6: Работа с базой объектов	1,3	0,0	1,3	
9.7.	Лабораторная работа 7: Настройка политики контроля доступа	1,2	0,0	1,2	
10.	Механизм Security Intelligence	2,2	1,1	1,1	Групповой опрос
10.1.	Обзор механизма	0,4	0,4	0,0	
10.2.	Объекты	0,4	0,4	0,0	
10.3.	Настройка Security Intelligence	0,3	0,3	0,0	
10.4.	Лабораторная работа 8: Security Intelligence	1,1	0,0	1,1	
11.	Контроль файлов и расширенная защита от вредоносного ПО	2,2	1,0	1,2	Групповой опрос
11.1.	Анализ файловой политики	0,5	0,5	0,0	
11.2.	Анализ сервиса AMP	0,5	0,5	0,0	
11.3.	Лабораторная работа 9: Файловая политика	1,2	0,0	1,2	
12.	Система предотвращения вторжений	1,6	0,5	1,1	Групповой опрос
12.1.	Введение, Snort-правила	0,3	0,3	0,0	
12.2.	Настройка IPS-политики	0,2	0,2	0,0	
12.3.	Лабораторная работа 10: Политика IPS	1,1	0,0	1,1	
13.	Политика анализа сети	2,1	0,8	1,3	Групповой опрос
13.1.	Исследование работы препроцессора	0,4	0,4	0,0	

13.2.	Обзор политики анализа сети	0,4	0,4	0,0	
13.3.	Лабораторная работа 11: Политика анализа сети	1,3	0,0	1,3	
14.	Firepower Threat Defense VPN	0,4	0,4	0,0	Групповой опрос
14.1.	Обзор возможностей	0,4	0,4	0,0	
15.	Работа с шифрованным трафиком	4,6	2,9	1,7	Групповой опрос
15.1.	Механизмы дешифрования SSL-трафика	0,5	0,5	0,0	
15.2.	Разбор техник детального анализа трафика	0,6	0,6	0,0	
15.3.	Типа событий	0,3	0,3	0,0	
15.4.	Контекстная информация	0,5	0,5	0,0	
15.5.	Механизмы для анализа	0,2	0,2	0,0	
15.6.	Настройки оповещений	0,8	0,8	0,0	
15.7.	Лабораторная работа 12: Политика корреляции	1,2	0,0	1,2	
15.8.	Лабораторная работа 13: Детальный анализ, настройка оповещений	0,5	0,0	0,5	
	Всего:	30	15	15	
	Итоговый контроль знаний	2	0	0	Электронное тестирование
	Итого:	32	15	15	

2.2 Календарный учебный график

Занятия проводятся 4 раза в неделю по 8 академических часов (1 ак. час - 45 минут). Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1			
	дни	1	1	1	1
Вид занятий		А	А	А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации «Защита сетей с помощью платформы Cisco Firepower Next-Generation IPS (CI-SSFIPS)».

Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0,5	0,5	0,0	Групповой опрос

2. Обзор технологий безопасности

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
2.	Обзор технологий безопасности				
2.1	Сравнение и анализ систем предотвращения вторжений и межсетевых экранов	0,5	0,5	0,0	
	ИТОГО	0,5	0,5	0,0	Групповой опрос

3. Компоненты системы Cisco Firepower, основные функции

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Компоненты системы Cisco Firepower, основные функции				
3.1	Обзор системы	0,3	0,3	0,0	
3.2	Основные компоненты системы Firepower	0,4	0,4	0,0	
3.3	Процесс внедрения Firepower	0,3	0,3	0,0	
3.4	Лабораторная работа 1: Подключение к лабораторному стенду	1,3	0,0	1,3	
	ИТОГО	2,3	1,0	1,3	Групповой опрос

4. Обзор Cisco Firepower MGMT Center

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Обзор Cisco Firepower MGMT Center				
4.1	Исследование GUI	0,4	0,4	0,0	
4.2.	Введение в политики	0,4	0,4	0,0	
4.3.	Лабораторная работа 2: Изучение функций Cisco Firepower MGMT Center	1,2	0,0	1,2	
	ИТОГО	2,0	0,8	1,2	Групповой опрос

5. Подключение управляемых устройств

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Подключение управляемых устройств				
5.1	Обзор дизайнов внедрения системы	0,5	0,5	0,0	
5.2.	Управляемые устройства	0,4	0,4	0,0	
5.3	Система лицензирования	0,4	0,4	0,0	
5.4	Лабораторная работа 3: Настройка FTD устройств	1,2	0,0	1,2	
	ИТОГО	2,5	1,3	1,2	Групповой опрос

6. NAT для Firepower Threat Defense

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	NAT для Firepower Threat Defense				
6.1	Обзор методов трансляции сетевых адресов в FTD	0,2	0,2	0,0	
6.2	Лабораторная работа 4: Настройка NAT	1,3	0,0	1,3	
	ВСЕГО	1,5	0,2	1,3	Групповой опрос

7. QoS на Firepower

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
7.	QoS на Firepower				
7.1	Обзор механизмов QoS	0,4	0,4	0,0	
	ИТОГО	0,4	0,4	0,0	Групповой опрос

8. Механизм анализа сети Firepower Discovery

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
8.	Механизм анализа сети Firepower Discovery				
8.1	Обзор	0,5	0,5	0,0	
8.2.	Анализ профиля хоста	0,5	0,5	0,0	
8.3	Работа с идентификационной информацией пользователя	0,4	0,4	0,0	
8.4	Лабораторная работа 5: Настройка политики Network Discovery	1,1	0,0	1,1	
	ИТОГО	2,5	1,4	1,1	Групповой опрос

9. Политика контроля доступа к ресурсам

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
9.	Политика контроля доступа к ресурсам				
9.1	Введение	0,4	0,4	0,0	
9.2.	Исследование базы объектов	0,4	0,4	0,0	
9.3	Анализ списка правил, дефолтное действие	0,3	0,3	0,0	
9.4	Расширенные функции	0,6	0,6	0,0	
9.5	Рекомендации для внедрения политики контроля доступа	0,5	0,5	0,0	
9.6	Лабораторная работа 6: Работа с базой объектов	1,3	0,0	1,3	
9.7	Лабораторная работа 7: Настройка политики контроля доступа	1,2	0,0	1,2	
	ИТОГО	4,7	2,2	2,5	Групповой опрос

10. Механизм Security Intelligence

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
10.	Механизм Security Intelligence				
10.1	Обзор механизма	0,4	0,4	0,0	
10.2.	Объекты	0,4	0,4	0,0	
10.3	Настройка Security Intelligence	0,3	0,3	0,0	
10.4	Лабораторная работа 8: Security Intelligence	1,1	0,0	1,1	
	ИТОГО	2,2	1,1	1,1	Групповой опрос

11. Контроль файлов и расширенная защита от вредоносного ПО

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
11.	Контроль файлов и расширенная защита от вредоносного ПО				
11.1	Анализ файловой политики	0,5	0,5	0,0	
11.2	Анализ сервиса AMP	0,5	0,5	0,0	
11.3	Лабораторная работа 9: Файловая политика	1,2	0,0	1,2	
	ИТОГО	2,2	1,0	1,2	Групповой опрос

12. Система предотвращения вторжений

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
12.	Система предотвращения вторжений				
12.1	Введение, Snort-правила	0,3	0,3	0,0	
12.2.	Настройка IPS-политики	0,2	0,2	0,0	
12.3	Лабораторная работа 10: Политика IPS	1,1	0,0	1,1	
	ИТОГО	1,6	0,5	1,1	Групповой опрос

13. Политика анализа сети

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
13.	Политика анализа сети				
13.1	Исследование работы препроцессора	0,4	0,4	0,0	
13.2.	Обзор политики анализа сети	0,4	0,4	0,0	
13.3.	Лабораторная работа 11: Политика анализа сети	1,3	0,0	1,3	
	ИТОГО	2,1	0,8	1,3	Групповой опрос

14. Firepower Threat Defense VPN

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
14.	Firepower Threat Defense VPN				
14.1	Обзор возможностей	0,4	0,4	0,0	
	ИТОГО	0,4	0,4	0,0	Групповой опрос

15. Работа с шифрованным трафиком

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
15.	Работа с шифрованным трафиком				
15.1	Механизмы дешифрования SSL-трафика	0,5	0,5	0,0	
15.2.	Разбор техник детального анализа трафика	0,6	0,6	0,0	
15.3	Типа событий	0,3	0,3	0,0	
15.4	Контекстная информация	0,5	0,5	0,0	
15.5	Механизмы для анализа	0,2	0,2	0,0	
15.6	Настройки оповещений	0.8	0.8	0.0	

15.7	Лабораторная работа 12: Политика корреляции	1,2	0,0	1,2	
15.8	Лабораторная работа 13: Детальный анализ, настройка оповещений	0,5	0,0	0,5	
	ИТОГО	4,6	2,9	1,7	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».

**Общество с ограниченной ответственностью
«Фаст Лейн Столица»**

УТВЕРЖДАЮ

Генеральный директор
О.А. Богомолов

«09» января 2019г.

МП



**Дополнительная профессиональная программа
повышения квалификации**

**«Организация защиты доступа в интернет с
использованием Cisco Web Security Appliance (v.2.1)
(SWSA)»**

Москва, 2019

ОГЛАВЛЕНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ	3
1.1 Актуальность	3
1.2 Цель и задачи реализации программы	4
1.3 Планируемые результаты обучения	4
1.4 Требования к слушателям	5
1.5 Трудоемкость обучения	5
1.6 Форма аттестации	5
1.7 Форма обучения	5
II. СОДЕРЖАНИЕ ПРОГРАММЫ	6
2.1 Учебный план	6
2.2 Календарный учебный график	8
2.3 Рабочая программа учебных предметов	8
III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	13
3.1 Требования к педагогам	13
3.2 Материально-техническое оснащение программы	13
3.3 Учебно-методическое оснащение программы	13
IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ	13
V. СОСТАВИТЕЛИ ПРОГРАММЫ	14

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Актуальность

Настоящая дополнительная профессиональная программа повышения квалификации «Организация защиты доступа в интернет с использованием Cisco Web Security Appliance (v.2.1) (SWSA)» предназначена для лиц, имеющих среднее профессиональное и (или) высшее образование, либо лиц получающих среднее профессиональное и (или) высшее образование.

Содержание программы направлено на создание условий для знакомства слушателей с современным инновационным теоретическим и практическим опытом в области использования сетевого оборудования Cisco.

Программа разработана в соответствии с ФЗ-№273 «Об образовании в РФ» от 29.12.2012г., приказом Минобрнауки России от 01.07.2013 N 499 (ред. от 15.11.2013) "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", приказом Минтруда России от 03.11.2016 N 608н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 25.11.2016 N 44449), приказом Минтруда России от 15.09.2016 N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 28.09.2016 N 43857), приказом Минтруда России от 19 мая 2014 года N 316н "Об утверждении профессионального стандарта "Инженер-проектировщик в области связи (телекоммуникаций) " (Зарегистрировано в Минюсте России 10 июля 2014 года, регистрационный N 33047), приказом Минтруда России от 05.10.2015 N 688н "Об утверждении профессионального стандарта "Специалист по технической поддержке информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 22.10.2015 N 39412), приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 19.10.2015 N 39361).

Стремительное развитие IT-технологий требует обновления содержания профессиональных программ в связи с изменениями потребностей личности, общества и государства в дополнительном образовании. Вследствие чего формируется социальный заказ в системе повышения квалификации инженеров, выражающийся в требованиях к повышению профессиональной компетентности специалиста, работающего в сфере инфокоммуникаций.

1.2 Цель и задачи реализации программы

Цель дополнительной профессиональной программы повышения квалификации «Организация защиты доступа в интернет с использованием Cisco Web Security Appliance (v.2.1) (SWSA)» - предоставить слушателям информацию о том, как устанавливать, конфигурировать и администрировать устройства Cisco Web Security Appliance. Слушатели получают подробные сведения о наиболее часто используемых функциях и особенностях продукта.

Для реализации цели программы необходимо решить комплекс задач:

- способствовать внедрению в учебный процесс современных эффективных методик проведения лабораторных работ, которые позволяют выполнять сложные задания на различных топологиях сети;
- обеспечить общее понимание слушателями перспектив развития ИТ-отрасли.

1.3 Планируемые результаты обучения

Программа направлена на приобретение знаний, умений и навыков слушателями, необходимых для качественного изменения профессиональных компетенций в рамках имеющейся квалификации.

Вид профессиональной деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

В результате освоения учебной дополнительной профессиональной программы повышения квалификации «Организация защиты доступа в интернет с использованием Cisco Web Security Appliance (v.2.1) (SWSA)».

Слушатель должен уметь:

- настраивать и администрировать устройства Cisco Web Security Appliance;
- производить мониторинг работы Cisco WSA.

Слушатель должен знать:

- модели и архитектуру Cisco WSA.

Слушатель должен владеть:

- навыками обеспечения безопасности данных.

1.4 Требования к слушателям

Данная учебная программа предназначена для инженеров сопровождения и технической поддержки, специалистов технических и инженерных служб, системных администраторов.

1.5 Трудоемкость обучения

Нормативная трудоёмкость обучения по данной программе составляет 16 часов, включает все виды аудиторной работы слушателя, время, отводимое на контроль качества освоения слушателем программы.

1.6 Форма аттестации

Обучение по программе завершается итоговой аттестацией слушателей. Формой аттестации является *тест*.

Лицам, успешно освоившим данную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: удостоверение о повышении квалификации.

Лицам, не освоившим данную программу и не прошедшим итоговую аттестацию, выдается справка о прослушивании курса по данной программе.

1.7 Форма обучения

Обучение предусматривает очную форму обучения (с отрывом от работы).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Дополнительной профессиональной программы повышения квалификации
«Организация защиты доступа в интернет с использованием Cisco Web Security
Appliance (v.2.1) (SWSA)»

Срок обучения: 16 часов.

Режим занятий: 8 часов в день

№	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0.2	0.2	0	Групповой опрос
2.	Обзор Cisco Web Security Appliance	0.5	0.5	0	Групповой опрос
2.1.	Примеры использования	0.2	0.2	0	
2.2.	Модели и архитектура Cisco WSA	0.3	0.3	0	
3.	Установка и проверка работы Cisco WSA	1.8	0.3	1.5	Групповой опрос
3.1.	Обзор Cisco Content SMA	0.1	0.1	0	
3.2.	Установка и настройка физического устройства Cisco WSA	0.1	0.1	0	
3.3.	Установка и настройка виртуального Cisco WSA для VMware	0.1	0.1	0	
3.4.	Лабораторная работа 1: Доступ к удаленному лабораторному стенду Cisco	0.5	0	0.5	
3.5.	Лабораторная работа 2: Установка и проверка Cisco WSA	1	0	1	
4.	Внедрение прокси-сервисов	1.2	0.7	0.5	Групповой опрос
4.1.	Сравнение режимов работы Proxu	0.2	0.2	0	
4.2.	Настройка и управление Proxu сервисом на Cisco WSA	0.3	0.3	0	
4.3.	Native FTP Proxu	0.1	0.1	0	
4.4.	Просмотр журнала доступа и HTTP-заголовков	0.1	0.1	0	
4.5.	Лабораторная работа 3: Внедрение Proxu сервиса	0.5	0	0.5	
5.	Использование сервиса аутентификации	1.5	0.5	1	Групповой опрос
5.1.	NTLM и Proxu аутентификация	0.3	0.3	0	
5.2.	Разрешение проблем подключения к домену и тестирование аутентификации	0.2	0.2	0	

5.3.	Лабораторная работа 4: Настройка аутентификации	1	0	1	
6.	Настройка политик	2	1	1	
6.1.	Настройка политик доступа	0.3	0.3	0	
6.2.	Описание других типов политик	0.2	0.2	0	
6.3.	Настройка исключения для аутентификации	0.2	0.2	0	
6.4.	Обзор журнала доступа и примеров	0.3	0.3	0	
6.5.	Лабораторная работа 5: Настройка политик Cisco WSA	1	0	1	
7.	Основные функции	1.6	1.1	0.5	
7.1.	URL-категории и фильтры	0.2	0.2	0	
7.2.	Распознавание и контроль приложений	0.3	0.3	0	
7.3.	Контроль доступа сервиса SaaS	0.3	0.3	0	
7.4.	Инспектирование HTTPS	0.2	0.2	0	
7.5.	Настройка HTTPS Proxy	0.1	0.1	0	
7.6.	Лабораторная работа 6: Настройка ограничений доступа в Интернет	0.5	0	0.5	
8.	Защита от вредоносного программного обеспечения	1	0.5	0.5	
8.1.	Описание и настройка WBSR	0.2	0.2	0	
8.2.	Сканирование вредоносного программного обеспечения	0.2	0.2	0	
8.3.	ACL метки	0.1	0.1	0	
8.4.	Лабораторная работа 7: Защита от вредоносного программного обеспечения	0.5	0	0.5	
9.	Обеспечение безопасности данных	1.5	0.5	1	
9.1.	Настройка обеспечения безопасности данных	0.2	0.2	0	
9.2.	Предотвращение утечки данных	0.3	0.3	0	
9.3.	Лабораторная работа 8: Настройка обеспечения безопасности данных	1	0	1	
10.	Описание сервиса Cisco Cloud Web Security	0.7	0.7	0	
10.1.	Cisco Cloud Web Security функции и преимущества	0.4	0.4	0	
10.2.	Подключение к Cisco Cloud	0.3	0.3	0	
11.	Использование клиента Cisco AnyConnect Secure Mobility	0.8	0.3	0.5	
11.1.	Интеграция клиента Cisco AnyConnect Secure Mobility с Cisco WSA и Cisco Cloud Web Security	0.3	0.3	0	
11.2.	Лабораторная работа 9: Настройка Cisco Cloud Web Security	0.5	0	0.5	
12.	Администрирование и поиск	2.2	1.2	1	

	неисправностей				
12.1.	Управление отчетами	0.2	0.2	0	
12.2.	Мониторинг работы Cisco WSA	0.3	0.3	0	
12.3.	Инструменты для диагностики проблем	0.5	0.5	0	
12.4.	Журнал логов доступа	0.2	0.2	0	
12.5.	Лабораторная работа 10: Администрирование и разрешение проблем	1	0	1	
	Всего:	15	7.5	7.5	
	Итоговый контроль знаний	1	0	0	Электронное тестирование
	Итого:	16	7.5	7.5	

2.2 Календарный учебный график

Занятия проводятся 2 раза в неделю по 8 академических часов (1 ак. час - 45 минут).
Всего в периоде обучения – одна учебная неделя. Учебная неделя не привязана к началу или окончанию учебного и календарного года. Формирование группы слушателей происходит в течение всего календарного года.

Сроки обучения	недели	1	
	дни	1	1
Вид занятий		А	А/И

А – аудиторные занятия

И – итоговая аттестация

2.3 Рабочая программа учебных предметов

дополнительной профессиональной программы повышения квалификации
«Организация защиты доступа в интернет с использованием Cisco Web Security Appliance (v.2.1) (SWSA)».
Учебно-тематический план

1. Введение

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
1.	Введение	0.2	0.2	0	Групповой опрос

2. Обзор Cisco Web Security Appliance

№ Тема	Наименование разделов и тем	Всего, часов	В том числе		Форма контроля
			лекции	практические занятия	

2.	Обзор Cisco Web Security Appliance				
2.1.	Примеры использования	0.2	0.2	0	
2.2.	Модели и архитектура Cisco WSA	0.3	0.3	0	
	ИТОГО	0.5	0.5	0	Групповой опрос

3. Установка и проверка работы Cisco WSA

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
3.	Установка и проверка работы Cisco WSA				
3.1.	Обзор Cisco Content SMA	0.1	0.1	0	
3.2.	Установка и настройка физического устройства Cisco WSA	0.1	0.1	0	
3.3	Установка и настройка виртуального Cisco WSA для VMware	0.1	0.1	0	
3.4	Лабораторная работа 1: Доступ к удаленному лабораторному стенду Cisco	0.5	0	0.5	
3.5	Лабораторная работа 2: Установка и проверка Cisco WSA	1	0	1	
	ИТОГО	1.8	0.3	1.5	Групповой опрос

4. Внедрение прокси-сервисов

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
4.	Внедрение прокси-сервисов				
4.1.	Сравнение режимов работы Proxu	0.2	0.2	0	
4.2.	Настройка и управление Proxu сервисом на Cisco WSA	0.3	0.3	0	
4.3	Native FTP Proxu	0.1	0.1	0	
4.4	Просмотр журнала доступа и HTTP-заголовков	0.1	0.1	0	
4.5	Лабораторная работа 3: Внедрение Proxu сервиса	0.5	0	0.5	
	ИТОГО	1.2	0.7	0.5	Групповой опрос

5. Использование сервиса аутентификации

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
5.	Использование сервиса аутентификации				
5.1.	NTLM и Proxu аутентификация	0.3	0.3	0	

5.2.	Разрешение проблем подключения к домену и тестирование аутентификации	0.2	0.2	0	
5.3.	Лабораторная работа 4: Настройка аутентификации	1	0	1	
	ИТОГО	1.5	0.5	1	Групповой опрос

6. Настройка политик

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
6.	Настройка политик				
6.1.	Настройка политик доступа	0.3	0.3	0	
6.2.	Описание других типов политик	0.2	0.2	0	
6.3.	Настройка исключения для аутентификации	0.2	0.2	0	
6.4	Обзор журнала доступа и примеров	0.3	0.3	0	
6.5	Лабораторная работа 5: Настройка политик Cisco WSA	1	0	1	
	ИТОГО	2	1	1	Групповой опрос

7. Основные функции

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
7.	Основные функции				
7.1.	URL-категории и фильтры	0.2	0.2	0	
7.2.	Распознавание и контроль приложений	0.3	0.3	0	
7.3.	Контроль доступа сервиса SaaS	0.3	0.3	0	
7.4	Инспектирование HTTPS	0.2	0.2	0	
7.5	Настройка HTTPS Proxy	0.1	0.1	0	
7.6	Лабораторная работа 6: Настройка ограничений доступа в Интернет	0.5	0	0.5	
	ИТОГО	1.6	1.1	0.5	Групповой опрос

8. Защита от вредоносного программного обеспечения

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
8.	Защита от вредоносного программного обеспечения				
8.1.	Описание и настройка WBSR	0.2	0.2	0	
8.2.	Сканирование вредоносного	0.2	0.2	0	

	программного обеспечения				
8.3.	ACL метки	0.1	0.1	0	
8.4	Лабораторная работа 7: Защита от вредоносного программного обеспечения	0.5	0	0.5	
	ИТОГО	1	0.5	0.5	Групповой опрос

9. Обеспечение безопасности данных

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
9.	Обеспечение безопасности данных				
9.1.	Настройка обеспечения безопасности данных	0.2	0.2	0	
9.2.	Предотвращение утечки данных	0.3	0.3	0	
9.3	Лабораторная работа 8: Настройка обеспечения безопасности данных	1	0	1	
	ИТОГО	1.5	0.5	1	Групповой опрос

10. Описание сервиса Cisco Cloud Web Security

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
10.	Описание сервиса Cisco Cloud Web Security				
10.1.	Cisco Cloud Web Security функции и преимущества	0.4	0.4	0	
10.2.	Подключение к Cisco Cloud	0.3	0.3	0	
	ИТОГО	0.7	0.7	0	Групповой опрос

11. Использование клиента Cisco AnyConnect Secure Mobility

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
11.	Использование клиента Cisco AnyConnect Secure Mobility				
11.1.	Интеграция клиента Cisco AnyConnect Secure Mobility с Cisco WSA и Cisco Cloud Web Security	0.3	0.3	0	
11.2.	Лабораторная работа 9: Настройка Cisco Cloud Web Security	0.5	0	0.5	
	ИТОГО	0.8	0.3	0.5	Групповой опрос

12. Администрирование и поиск неисправностей

№ тема	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			лекции	практические занятия	
12.	Администрирование и поиск неисправностей				
12.1.	Управление отчетами	0.2	0.2	0	
12.2.	Мониторинг работы Cisco WSA	0.3	0.3	0	
12.3	Инструменты для диагностик проблем	0.5	0.5	0	
12.4	Журнал логов доступа	0.2	0.2	0	
12.5	Лабораторная работа 10: Администрирование и разрешение проблем	1	0	1	
	ИТОГО	2.2	1.2	1	Групповой опрос

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

3.1 Требования к педагогам

К реализации программы допускаются педагогические работники с соответствующим уровнем профессионального образования, а также с учетом требований, профессионального стандарта, утвержденному Приказом Минтруда России от 08.09.2015 N 608н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 24.09.2015 N 38993).

3.2 Материально-техническое оснащение программы

Для освоения слушателями программы учебная аудитория укомплектована следующим набором оборудования:

- столы
- стулья
- маркерная доска
- проектор
- ПК

Комплект оборудования может пополняться и (или) заменяться по мере необходимости.

3.3. Учебно-методическое оснащение программы

1. Руководство слушателя Student Guide (<http://learningspace.cisco.com>);
2. Инструкции по выполнению лабораторных работ Lab Guide (<http://learningspace.cisco.com>);
3. Презентации.

IV. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Реализация программы предполагает итоговую аттестацию слушателей в форме зачета, который проводится в форме письменного теста.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Богомоллов О.А. – генеральный директор ООО «Фаст Лейн Столица».