Негосударственное образовательное учреждение
дополнительного профессионального образования
«Институт информационных технологий «АйТи»

У Т В Е Р Ж Д А Ю
Ректор НОУДПО «Институт «АйТи»
_____ И.О. Морозов
«1» сентября 2015 г.

Образовательная программа
дополнительного профессионального образования

(повышения квалификации)
по направлению

ИФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Москва, 2015 г.

Образовательная программа дополнительного профессионального образования повышения квалификации (далее Программа) разработана на основании Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказа Минобрнауки России от 01 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», приказа Минобрнауки России от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности» и приказа Минобрнауки России от 09 января 2014 г. № 2 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

Информационные технологии никогда не стояли на месте. В последнее время наблюдается их особенно стремительное развитие, проявляющееся в регулярном появлении новых и модернизации старых программных и аппаратных средств. Такой бурный рост сопряжён с появлением новых уязвимостей в продуктах информационных технологий и новых угроз информационной безопасности. Параллельно идёт процесс постоянного совершенствования нормативно-правовой и нормативно-методической базы в области обеспечения информационной безопасности и защиты информации. Отмеченные факторы обуславливают необходимость наличия в штате организаций различных форм собственности грамотных, обученных специалистов в области защиты информации, а также необходимость повышения уровня осведомлённости рядовых сотрудников в вопросах информационной безопасности.

Образовательная программа направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалиста в области защиты информации.

Содержание образовательной программы учитывает профессиональные стандарты, квалификационные требования, указанные в квалификационных справочниках по соответствующим должностям, профессиям и специальностям, или квалификационные требования к профессиональным знаниям и навыкам, необходимым для исполнения должностных обязанностей по вопросам информационной безопасности, которые устанавливаются в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации о государственной службе.

При создании Программы реализован модульный принцип построения программ. Каждый модуль представляет собой дидактически самостоятельный курс. Все отклонения от данной Программы при ее реализации в полном или частичном объеме (изучение образовательных модулей (курсов)) согласовываются до начала обучения и отражаются в рабочей образовательной программе (дополнительной профессиональной программе), индивидуальном плане обучения и договоре об образовании.

Цель образовательной Программы - совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалиста в области защиты информации. В рабочей образовательной программе каждого образовательного модуля (курса) настоящая цель конкретизируется.

Планируемые результаты обучения представлены в виде общих для Программы компетенций, качественное изменение которых осуществляется в результате обучения по учебным курсам (дисциплинам), входящим в учебный план Программы. Также дополнительно для каждого учебного курса (дисциплины) результат обучения представлен в виде знаний умений и навыков, которые позволят специалистам решать профессиональные задачи в рамках сформированной компетенции.

Форма организации образовательного процесса:

- очная,
- очно-заочная,
- заочная,

Все формы обучения могут реализовываться с применением электронного обучения и дистанционных образовательных технологий.

Учебный план Программы представляет собой перечень модулей - учебных курсов (дисциплин), каждый из которых имеет свой учебный план, который определяет перечень, трудоемкость, последовательность и формы контроля. Допускается формирование индивидуального учебного плана как для группы слушателей, так и для отдельного слушателя в пределах осваиваемой Программы. Содержание индивидуального учебного плана определяется НОУДПО «Институт «АйТи» с учетом потребностей лица, организации, по инициативе которых осуществляется дополнительное профессиональное образование по настоящей Программе.

Календарный учебный график определяет основные параметры учебного процесса при организации занятий по каждому образовательному модулю (курсу) при освоении настоящей Программы и зависит от трудоёмкости Программы. Календарный период для освоения каждого образовательного модуля (курса) определяется по согласованию с заказчиком

В каждом образовательном модуле (курсе) Программы представлено также тематическое содержание в соответствии с учебным планом, календарным учебным графиком, описание организационно - педагогических условий реализации Программы, описание форм аттестации и оценочных материалов.

Тематическое содержание программы раскрывает тематику и проблематику разделов и тем, которые представлены в виде перечисления дидактических единиц теоретического материала и практических заданий.

Организационно-педагогические условия реализации Программы определяются в соответствии со спецификой образовательного модуля (курса) Программы и подробно расписываются в рабочей образовательной программе.

Обучение проводится в соответствии с учебной программой на лекционных и практических занятиях.

Язык преподавания – русский или английский.

Слушатели обеспечиваются учебно-методическими, информационными и справочными материалами.

Учебный год представляет собой круглогодичное обучение с 1 сентября по 31 августа.

Количество учебных дней в неделю при очном обучении составляет 5 дней.

Академический час равен 45 минутам. Режим проведения занятий: 2 занятия по 45 минут, 15 минут перерыв, перерыв на обед 1 час.

Список программных продуктов, используемых в процессе обучения:

- Microsoft Windows 7
- Microsoft Word 2010
- Microsoft Excel 2010
- Microsoft PowerPoint 2010
- Internet Explorer 9.0

Формы аттестации представляют собой п*ромежуточную аттестацию* и *итоговую аттестацию*. Промежуточный контроль знаний осуществляется через экспертную оценку преподавателем курса успеваемости слушателей в процессе выполнения практических, лабораторных работ и других видов работ по разделам программы.

Итоговая аттестация слушателей состоит из одного аттестационного испытания. Обучение по каждому образовательному модулю (курсу) Программы завершается сдачей экзамена (в форме тестирования) или зачета (в форме выполнения практической работы, лабораторной работы, проекта, составления отчета о выполненных практических работах).

В случае успешного прохождения итоговой аттестации по образовательному модулю (курсу) Программы, слушатель получает удостоверение о повышении квалификации Слушателю, не прошедшему итоговую аттестацию или получившему на итоговой аттестации неудовлетворительную оценку, выдается справка об обучении.

Оценочные материалы могут быть представлены либо в форме списка вопросов, либо в форме теста, либо в форме лабораторной работы. Если итоговая лабораторная работа является виртуальной или включена в рабочую тетрадь, то текст лабораторной работы в Программу не включается. В этом случае в данном разделе указывается форма лабораторной работы (виртуальная или на бумажном носителе).

Рабочие образовательные программы модулей (курсов) – базируются на данной типовой Программе и дополняются и уточняются с учетом пожеланий заказчика обучения. Рабочая образовательная программа (дополнительная профессиональная программа повышения квалификации) разрабатывается при заказе образовательного модуля (курса), утверждается Ректором НОУДПО «Институт «АйТи» не позднее чем за 1 день, до начала занятий.

Описание образовательной Программы размещается на сайте по адресу http://www.academy.it.ru

Учебный план

	Название образовательного модуля (курса)	всего часов	в том числе		формы контроля
			Лекции	практические и семинарские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	2830_ Разработка безопасности для сетей Microsoft.	24	6	18	выполнение лабораторной работы
2.	CEH1_ Сертифицированный этичный хакер.	40	11	29	экзамен
3.	CEH2_ CHFI. Выявление и расследование инцидентов информационной безопасности.	40	12	28	экзамен
4.	CEH3_ ECSA_LPT. Сертифицированный аналитик по вопросам безопасности информационных систем.	40	12	28	экзамен
5.	FIREWALL_ Внедрение межсетевых экранов Cisco ASA (версия 2.0) (FIREWALL).	40	12	28	выполнение лабораторной работы
6.	IINS _ Безопасность в сетях Cisco.	40	11	29	выполнение лабораторной работы
7.	IPS _ Внедрение системы предотвращения вторжений Cisco.	40	12	28	выполнение лабораторной работы
8.	SECURE_Обеспечение безопасности сетей с помощью маршрутизаторов и коммутаторов Cisco (SECURE.	40	10	30	выполнение лабораторной работы
9.	SENSS _ Развертывание решений Cisco по обеспечению безопасности границ сети.	40	10	30	выполнение лабораторной работы
10.	SIMOS _ Внедрение решений Cisco для безопасной мобильности.	40	10	30	выполнение лабораторной работы
11.	SISAS _ Внедрение решений Cisco для безопасного доступа.	40	10	30	выполнение лабораторной работы
12.	SITCS _ Развертывание решений Cisco по контролю за угрозами.	40	10	30	выполнение лабораторной работы
13.	SN010_ Многофакторная аутентификация на основе продуктов компании SafeNet.	24	8	16	экзамен в форме тестирования
14.	SN011_ Аутентификация с использованием цифровых сертификатов на основе продуктов компании SafeNet.	16	4	12	экзамен в форме тестирования

15.	SN012_ Аутентификация с использованием одноразовых паролей на основе продуктов компании SafeNet.	16	5	11	экзамен в форме тестирования
16.	SN020_ Сертифицированный специалист по продукту eSafe SmartSuite 8.5.	16	5	11	экзамен пробный
17.	VPN_ Внедрение виртуальных частных сетей средствами Cisco ASA (VPN).	40	10	30	выполнение лабораторной работы
18.	ИБ001_ Правовые и нормативно-методические основы обеспечения информационной безопасности.	24	8	16	экзамен в форме тестирования
19.	ИБ002_ Безопасность компьютерных систем и сетей.	40	10	30	экзамен в форме тестирования
20.	ИБ010_ Информационная безопасность в деятельности.	72	21	51	экзамен в форме тестирования
21.	ИБ011_ Информационная безопасность_ Комплексное обеспечение информационной безопасности автоматизированных систем.	104	25	79	экзамен в форме тестирования
22.	ИБ020_ Обеспечение комплексной защиты.	72	20	52	экзамен в форме тестирования
23.	ИБ021_ Организация конфиденциального делопроизводства.	24	7	17	экзамен в форме тестирования
24.	ИБ022_Организация процесса обработки и регулирование отношений при осуществлении проверок операторов персональных данных.	24	6	16	экзамен в форме тестирования
25.	ИБ023_ Установление и реализация режима коммерческой тайны.	16	4	12	экзамен в форме тестирования
26.	ИБ024_ Организация обработки персональных данных в компаниях и организациях (предприятиях) различных форм собственности.	24	6	18	экзамен в форме тестирования
27.	ИБ030_ Управление информационной безопасностью организации.	40	12	28	экзамен в форме тестирования
28.	ИБ032_ Управление рисками информационной безопасности.	24	7	17	экзамен в форме тестирования
29.	ИБ033_ Управление непрерывностью бизнеса.	24	6	18	экзамен в форме тестирования
30.	ИБ034_ Аудит информационной безопасности.	24	8	16	экзамен в форме тестирования

31.	ИБ038_ Построение автоматизированной системы управления информационной безопасностью с использованием продукта Security Vision.	16	5	11	экзамен в форме тестирования
32.	ИБ040_ Расследование компьютерных инцидентов.	40	12	28	экзамен в форме тестирования
33.	НСД001_ Эксплуатация средств защиты от НСД семейства Аккорд.	24	2	22	экзамен в форме тестирования
34.	НСД002_ Оценка эффективности системы защиты от несанкционированного доступа.	24	8	16	экзамен в форме тестирования
35.	НСД003_Token Management System 2.0 Возможности и эксплуатация системы.	16	5	11	экзамен в форме тестирования
36.	НСД004_ Token Management System 2.0 Установка и настройка системы.	8	1	7	тестирование
37.	НСД005_ Построение подсистемы аутентификации в информационных системах на основе продуктов eToken и Token Management System.	8	2	6	тестирование
38.	НСД006_ Построение подсистемы аутентификации в информационных системах на основе продуктов eToken и SafeNet Authentication Manager.	8	2	6	тестирование
39.	НСД007_ SafeNet Authentication Manager Возможности, установка, настройка и эксплуатация.	8	1	7	тестирование
40.	НСД008_ Применение системы защиты Secret Net 7. Базовый курс.	24	8	16	экзамен в форме тестирования
41.	НСД009_ Применение системы защиты Secret Net 7. Расширенный курс.	16	4	12	экзамен в форме тестирования
42.	СЗП001_ Организация защиты периметра корпоративной сети.	24	8	16	экзамен в форме тестирования
43.	СЗП002_ Обнаружение вторжений в корпоративные сети.	24	6	18	экзамен в форме тестирования
44.	СЗП003_ Безопасность беспроводных сетей.	24	7	17	экзамен в форме тестирования
45.	СЗП005_ Анализ защищенности сетей.	24	8	16	экзамен в форме тестирования
46.	СКЗИ001_Теория и практика использования средства криптографической защиты информации «КриптоПро CSP.	16	5	11	экзамен в форме тестирования

47.	СКЗИ002_ Построение системы юридически значимой электронной цифровой подписи в сети организации с использованием продуктов ООО «КриптоПро».	40	12	28	экзамен в форме тестирования
48.	СКЗИ003_ Правовое регулирование и нормативно-методическое обеспечение деятельности удостоверяющего центра и использования электронной подписи в информационных системах.	16	5	11	экзамен в форме тестирования
49.	СКЗИ007_ Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием продуктов ООО «КРИПТО-ПРО».	72	19	53	экзамен в форме тестирования
50.	СКЗИ013_ Системы защиты конфиденциальной информации Secret Disk.	16	5	11	экзамен в форме тестирования
51.	СКЗИ014_ Построение инфраструктуры аутентификации в информационных системах на основе продуктов eToken и Token Management System.	16	5	11	экзамен в форме тестирования
52.	СКЗИ023_ Использование «КриптоПро IPsec»» для обеспечения безопасности информации при передаче по каналам связи.	16	5	11	экзамен в форме тестирования
53.	СКЗИ024_ Теория и практика использования программного продукта «КриптоАРМ.	8	3	5	тестирование
54.	СКЗИ041_Теория и практика использования средства криптографической защиты информации «Верба-OW.	16	4	12	экзамен в форме тестирования
55.	СКЗИ042_ Построение системы юридически значимой электронной подписи с использованием аппаратно-программного комплекса «Верба-Сертификат МВ.	32	8	24	экзамен в форме тестирования
56.	СКЗИ043_ Администрирование АПКШ «Континент» Версия 3.7. Базовый курс.	24	8	16	экзамен в форме тестирования
57.	СКЗИ044_ Администрирование АПКШ «Континент» Версия 3.7. Расширенный курс.	16	2	14	экзамен в форме тестирования
58.	СПО201_ Администрирование ОС Linux.	40	8	32	экзамен в форме тестирования
59.	СПО202_ Безопасность ОС Linux.	32	6	26	экзамен в форме тестирования

60.	ТЗКИ001_ Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.	72	20	52	экзамен в форме тестирования
61.	ТЗКИ002_ Подготовка объектов информатизации к аттестации по требованиям безопасности информации.	24	7	17	экзамен в форме тестирования
62.	ТЗКИ009_Защита информации от утечки по техническим каналам. Защита информации от несанкционированного доступа (НСД).	72	24	48	экзамен в форме тестирования
	Итого	1904	525	1379	