Автономная некоммерческая организация
дополнительного профессионального образования
«Учебный центр «Эшелон»

УТВЕРЖДАЮ
Директор АНО ДПО
«Учебный центр «Эшелон»

_____ / Фортфель Н.В
(подпись)

«1» декабря 2015 г.

М.П.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«Внутренний аудит СУИБ на соответствие требованиям международного стандарта ISO/IEC 27001:2013»

Москва
2015

СОДЕРЖАНИЕ

1. УЧЕБНЫЙ ПЛАН

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля
			Внеаудиторная (самостоятельная работа)	Аудиторная работа (семинарские занятия)	
1	Внутренний аудит системы менеджмента информационной безопасности	17	2	15	
2	Итоговая аттестация	1		1	Тестирование
	ИТОГО	**18**	**2**	**16**	

2. УЧЕБНО – ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля
			Внеаудиторная (самостоятельная работа)	Аудиторная работа (семинарские занятия)	
1	**Внутренний аудит системы менеджмента информационной безопасности**	**17**	**2**	**15**	
1.1	Принципы аудита	1		2	
1.2	Разработка плана аудита	2		2	
1.3	Процессы аудита	4	1	3	
1.4	Подготовка к аудиту	2		3	
1.5	Отчетность по аудиту	1	1	2	
1.6	Контроль выполнения	1		1	
1.7	Проведение аудита последующих действий	1		2	
3	**Итоговая аттестация**	**1**		**1**	**Тестирование**
	ИТОГО	**18**	**2**	**16**	

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Недели обучения		**1**
Внутренний аудит системы менеджмента информационной безопасности	Аудиторная нагрузка	15
	Самостоятельное обучение	2

4. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая программа представляет собой совокупность требований, обязательных при реализации программы дополнительного профессионального образования по теме «Внутренний аудит СУИБ на соответствие требованиям международного стандарта ISO/IEC 27001:2013», разработанная на основании федеральных требований к программам повышения квалификации специалистов.

Право на реализацию дополнительной образовательной программы Повышение квалификации «Внутренний аудит СУИБ на соответствие требованиям международного стандарта ISO/IEC 27001:2013» имеет образовательный центр при наличии соответствующей лицензии.

Целью реализации программы повышения квалификации является совершенствование компетенций, необходимых руководителям, работающим в области информационной безопасности (далее – обучающиеся), для осуществления профессиональной деятельности в области менеджмента информационной безопасности.

Категория слушателей: лица, имеющие ВПО/СПО (в т.ч. получающие высшее /среднее профессиональное образование)

- руководители организаций,
- руководители служб информационной безопасности,
- руководители служб информационных технологий,
- специалисты по информационной безопасности;
- ИТ-аудиторы;
- аудиторы информационной безопасности.

Организационно-педагогические условия:

Образовательный процесс осуществляется на основании учебного плана и регламентируется расписанием занятий для каждой учебной группы.

Срок обучения: 18/2/1 (час., дни., недели.)

Режим занятии: 2 часа самостоятельного обучения, 16 часов аудиторной работы.

Форма обучения – очная

Для реализации программы задействован следующий кадровый потенциал:

- Преподаватели учебных дисциплин – Обеспечивается необходимый уровень компетенции преподавательского состава, включающий высшее образование в области соответствующей дисциплины программы или высшее образование в иной области и стаж преподавания по изучаемой тематике не менее трех лет; использование при изучении программы эффективных методик преподавания, предполагающих решение слушателями задач, контрольных вопросов.
- Административный персонал – обеспечивает условия для эффективной работы педагогического коллектива, осуществляет контроль и текущую организационную работу
- Информационно-технологический персонал - обеспечивает функционирование информационной структуры (включая ремонт техники, оборудования, макетов иного технического обеспечения образовательного процесса, поддержание сайта

Содержание программы повышения квалификации определяется учебным планом и календарным учебным графиком программы дисциплин (модулей), требованиями к итоговой аттестации и требованиями к уровню подготовки лиц, успешно освоивших Программу.

Текущий контроль знаний, полученных обучающимися посредством самостоятельного обучения (освоения части образовательной программы) проводится в виде проверки устного опроса по основным понятиям предыдущего занятия

Итоговая аттестация по программе проводится в форме тестирования и должна выявить теоретическую и практическую подготовку специалиста в области аудита системы менеджмента информационной безопасности.

Слушатель допускается к итоговой аттестации после самостоятельного изучения дисциплин программы в объеме, предусмотренном для обязательных занятий.

Лица, освоившие программу и успешно прошедшие итоговую аттестацию, получают **удостоверение о повышении квалификации установленного образца.**

Оценочными материалами по программе являются блоки контрольных вопросов по дисциплинам, формируемые образовательной организацией и используемые при текущем контроле знаний и итоговой аттестации.

Методическими материалами к программе являются методические пособия, нормативные правовые акты, положения которых изучаются при освоении дисциплин программы. Перечень методических материалов приводится в рабочей программе.

Характеристика профессиональной деятельности слушателей

Область профессиональной деятельности слушателей:

- менеджмент информационной безопасности;
- аудит информационной безопасности;
- техническая защита конфиденциальной информации.

Объектами профессиональной деятельности слушателей являются:

- объекты информатизации, включающие автоматизированные (информационные) системы различного уровня и назначения, средства и системы обработки информации и средства их обеспечения, а также помещения, предназначенные для ведения конфиденциальных переговоров (защищаемые помещения);
- система нормативных правовых актов, методических документов, национальных и международных стандартов в области информационной безопасности;
- способы и средства, используемые для обеспечения информационной безопасности.

Специалист по информационной безопасности готовится к следующим видам деятельности:

- определение угроз информационной безопасности на объектах информатизации и угроз безопасности информации в автоматизированных (информационных) системах;

- контроль эффективности принятых мер информационной безопасности.

Требования к результатам освоения дополнительной профессиональной образовательной программы

Специалист должен обладать общими компетенциями (ОК), включающими в себя способность:

Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес.

Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий.

Специалист должен обладать профессиональными компетенциями (ОК), соответствующими основным видам профессиональной деятельности:

- Разработка политик, процедур и стандартов организации по информационной безопасности;
- Оценка рисков информационной безопасности;
- Выбор мер информационной безопасности;
- Аудит информационной безопасности.

Рабочая программа Учебной дисциплины «Внутренний аудит системы менеджмента информационной безопасности»

Цель: совершенствование профессиональных навыков по внутреннему аудиту системы менеджмента информационной безопасности.

Задачи:

Знать требования международного стандарта ISO 27001 к системе менеджмента информационной безопасности и ее документированию.

Планировать и проводить аудит системы менеджмента информационной безопасности.

Место дисциплины в структуре программы.

Дисциплина позволяет слушателям изучить подходы к аудиту системы менеджмента информационной безопасности.

Перечень методических материалов

- методическое пособие;
- нормативные правовые акты

Требования к результатам освоения дисциплины.

В результате обучения дисциплине слушатели должны:

Знать: требования к процессу системы менеджмента информационной безопасности.

Уметь: разрабатывать план и программу аудита системы менеджмента информационной безопасности.

Владеть навыками профессионально и эффективно применять на практике приобретенные в процессе обучения знания и умения.

Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 18 часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) - 2 часа, семинарские занятия – 16 ак. часов).

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля
			Внеаудиторная (самостоятельная работа)	Аудиторная работа (семинарские занятия)	
1	**Внутренний аудит системы менеджмента информационной безопасности**	**17**	**2**	**15**	
1.1	Принципы аудита	1		2	
1.2	Разработка плана аудита	2		2	
1.3	Процессы аудита	4	1	3	
1.4	Подготовка к аудиту	2		3	
1.5	Отчетность по аудиту	1	1	2	
1.6	Контроль выполнения	1		1	
1.7	Проведение аудита последующих действий	1		2	
3	**Итоговая аттестация**	**1**		**1**	**Тестирование**
	ИТОГО	**18**	**2**	**16**	

Тема 1. Принципы аудита

- основные термины и определения в области аудита информационной безопасности;
- честность;

- беспристрастность;
- профессиональная осмотрительность;
- конфиденциальность;
- независимость;
- подход, основанный на свидетельстве.

Тема 2. Разработка плана аудита

- составление плана аудита;
- границы аудита;
- распределение работы среди членов команды.

Тема 3. Процессы аудита

- методы аудита;
- интервью;
- разовый проход по процессу;
- выборочное тестирование.

.

Тема 4. Подготовка к аудиту

- разработка проверочных листов;

Тема 5. Отчетность по аудиту

- сбор свидетельств аудита;
- документирование в ходе аудита;
- формулировка обнаружения недостатка;
- аудиторское заключение;
- подготовка результирующего отчета;

Тема 6. Контроль выполнения

- контроль качества аудита;

Тема 7. Проведение аудита последующих действий

- контроль исправления выявленных недостатков.

Список литературы

1. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements
2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования
3. ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента

Оценочные материалы
ТЕСТОВЫЕ ВОПРОСЫ

1. В ходе процесса оценки рисков должны быть..
   A. Определены критерии принятия рисков ИБ
   B. Проанализированы риски ИБ
   C. Обеспечены сопоставимые и воспроизводимые результаты
   D. Всё вышеперечисленное
2. Какое из утверждений, связанных с внедрением контролей безопасности из Приложения А, верное?
   A. Все они должны быть отражены в SoA с обоснованием
   B. Все контроли должны быть внедрены
   C. За каждым контролем должен быть закреплен его владелец
   D. Неприменимые контроли не должны входить в SoA

3. Что должна сделать организация в подтверждении соответствия требованиям ISO 27001?
   A. Внедрить лучшие практики из ISO 27002
   B. Внедрить все контроли Приложения А
   C. Внедрить достаточное количество контролей
   D. Внедрить контроли для выбранных способов обработки рисков

4. В ходе процесса анализа и оценки рисков организация должна:
   A. Оценить возможный ущерб для бизнеса
   B. Оценить вероятность возникновения угроз
   C. Определить уровни рисков
   D. Все вышеперечисленное

5. Что из перечисленного требуется для демонстрации руководящей роли менеджмента?
   A. Утверждение политики СМИБ
   B. Обеспечение проведения внутренних аудитов СМИБ
   C. Все перечисленное
   D. Назначение ролей и ответственностей за обеспечение ИБ

6. Возможные способы обработки рисков включают в себя:
   A. Исключение рисков из карты рисков
   B. Принятие риска для его дальнейшего отслеживания
   C. Инструкции менеджмента руководствоваться здравым смыслом
   D. Все вышеперечисленное

7. Что не является составляющей шага Check цикла PDCA в ISO 27001?
   A. Контроль со стороны руководства
   B. Операционный контроль
   C. Внутренний аудит
   D. Проверка системы менеджмента качества со стороны партнера

8. Что нельзя отнести к методам аудита информационной безопасности:

   A. Интервью

B. Разовый проход по процессу (walkthrough)
C. Выборочное тестирование
D. Стресс-интервью

9. Шаги по устранению причин несоответствия называются:

A. Коррекция
B. Корректирующее действие
C. Превентивное действие
D. Ничего из указанного

10. Документальное свидетельство прошедшего события называется:

A. Документ
B. Документированная процедура
C. Запись
D. Ничего из вышеуказанного

11. Что не является шагом в цикле Деминга

A. Plan
B. Act
C. Do
D. Co-Ordinate

12. Аудиторский чеклист НЕ должен:

A. Содержать закрытые вопросы
B. Содержать открытые вопросы
C. Идентифицировать, что аудитор запросит в качестве свидетельства
D. Не выходить за область аудита

13. Аудит – это

A. Систематический, независимый и документируемый процесс для получения свидетельств аудита и объективной оценки для определения области, в рамках которой критерии аудита выполнены
B. Систематический, независимый и документируемый процесс для получения заключений аудита
C. Действие, направленное на устранение причины выявленного несоответствия или иной нежелательной ситуации
D. Описание действий и мероприятий (мер)

14. Сертификационный аудит со стороны BSI это:

A. Аудит 1-ой стороны
B. Аудит 2-ой стороны
C. Аудит 3-ей стороны

15. Внутренний аудит это:

A. Аудит 1-ой стороны
B. Аудит 2-ой стороны

C. Аудит 3-ей стороны

16. Аудит аутсорсера:
A. Аудит 1-ой стороны
B. Аудит 2-ой стороны
C. Аудит 3-ей стороны

17. Находки аудита (Audit Findings):
A. Набор политик, процедур, или требований
B. Записи, изложение факта или иная информация, являющиеся важными для критериев аудита и проверяемые
C. Описание действий и мероприятий (мер)
D. Результаты оценки собранных в ходе аудита свидетельств соответствия критериям аудита

18. Риск –
A. Причина нежелательного инцидента
B. Комбинация вероятности реализации угрозы и последствий
C. Брешь в защите, позволяющая угрозе реализоваться
D. Мера определенности при достижении цели