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

УТВЕРЖДАЮ
Директор АНО ДПО
«Учебный центр «Эшелон»

_____ / Дорофеев А.В.
(подпись)

«__1__» _декабря_ 2015 г.

М.П.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«Внедрение системы управления информационной безопасностью»

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	Документирование системы менеджмента информационной безопасности	10	1	8	
2	Планирование процесса внедрения системы менеджмента информационной безопасности	9	1	7	
3	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	**Документирование системы менеджмента информационной безопасности**	**10**	**1**	**8**	
1.1	История возникновения стандарта ISO/IEC 27001	1		1	
1.2	Определение Области и Политики СМИБ	2		2	
1.3	Разработка политик	4	1	2	
1.4	Документирование СМИБ	2		2	
1.5	Соответствие требованиям СУИБ в части документированных процедур	1		1	
2	**Планирование процесса внедрения системы менеджмента информационной безопасности**	**9**	**1**	**7**	
2.1	Идентификация информационных активов	1		1	
2.2	Определение ценности информационных активов	1		1	
2.3	Определение рисков и потерь	2	1	1	
2.4	Установление целей и выбор контрмер	3		2	
2.5	Подготовка плана внедрения СМИБ	1		1	
2.6	Процесс сертификации	1		1	
3	**Итоговая аттестация**	**1**		**1**	**Тестирование**
	ИТОГО	**18**	**2**	**16**	

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Недели обучения		**1**
Документирование системы менеджмента информационной безопасности	Аудиторная нагрузка	8
	Самостоятельное обучение	1
Планирование процесса внедрения системы менеджмента информационной безопасности	Аудиторная нагрузка	8
	Самостоятельное обучение	1

4. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая программа представляет собой совокупность требований, обязательных при реализации программы дополнительного профессионального образования по теме «Внедрение системы управления информационной безопасностью», разработанная на основании федеральных требований к программам повышения квалификации специалистов.

Право на реализацию дополнительной образовательной программы Повышение квалификации «Внедрение системы управления информационной безопасностью» 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.

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 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;
- 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:

- планирование деятельности по обеспечению информационной безопасности (разработка документов, регламентирующих в организации политики (правила, процедуры) по обеспечению информационной безопасности);
- организация внедрения и применения политик (правил, процедур) по обеспечению информационной безопасности в организации;
- проведение контроля (мониторинга) и анализа применения политик (правил, процедур) по обеспечению информационной безопасности в организации;

- поддержка и совершенствование деятельности по обеспечению информационной безопасности в организации;
- определение угроз информационной безопасности на объектах информатизации и угроз безопасности информации в автоматизированных (информационных) системах;
- внедрение способов и средств для обеспечения информационной безопасности на объектах информатизации (внедрение системы защиты информации объекта информатизации).

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;
- Планирование внедрения системы менеджмента информационной безопасности.

Рабочая программа Учебной дисциплины «Документирование системы менеджмента информационной безопасности»

Цель: совершенствование профессиональных навыков по разработке документов системы менеджмента информационной безопасности.

Задачи:

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

Разрабатывать организационно-распорядительные документы по информационной безопасности: политики, процедуры, стандарты, регламенты.

Место дисциплины в структуре программы.

Дисциплина позволяет слушателям изучить требования к документированию системы менеджмента информационной безопасности и практики разработки необходимой организационно-распорядительной документации по информационной безопасности.

Перечень методических материалов

- методическое пособие;
- нормативные правовые акты

Требования к результатам освоения дисциплины.

В результате обучения дисциплине слушатели должны:

Знать: требования к документированию системы менеджмента информационной безопасности.

Уметь: разрабатывать организационно-распорядительную документацию.

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

Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 9 часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) - 1 час, семинарские занятия – 8 ак. часов).

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля
			Внеаудиторная (самостоятел	Аудиторная работа (семинарские	

			ьная работа)	занятия)	
1	**Документирование системы менеджмента информационной безопасности**	**9**	**1**	**8**	
1.1	История возникновения стандарта ISO/IEC 27001	1		1	
1.2	Определение Области и Политики СМИБ	2		2	
1.3	Разработка политик	4	1	2	
1.4	Документирование СМИБ	2		2	
1.5	Соответствие требованиям СУИБ в части документированных процедур	1		1	

Тема 1. История возникновения стандарта ISO/IEC 27001

- основные термины и определения в области информационной безопасности;
- структура стандарта ISO/IEC 27001;
- история возникновения стандарта ISO/IEC 27001.

Тема 2. Определение Области и Политики СМИБ

- понятие контекста организации;
- заинтересованные стороны;
- область действия СМИБ;
- варианты документирования области действия СМИБ.

Тема 3. Разработка политик

- политика, процедура, руководство;
- типовые структуры документов;
- правила разработки эффективных организационно-распорядительных документов.

Тема 4. Документирование СМИБ

- определение степени детализации документов СМИБ;
- руководство по СМИБ: что это и нужно ли это?
- положение о применимости контрмер;
- методика оценки рисков информационной безопасности.

Тема 5. Соответствие требованиям СМИБ в части документированных процедур

- понятие документированной информации;
- документы, требуемые ISO/IEC 27001;

Рабочая программа Учебной дисциплины «Планирование процесса внедрения системы менеджмента информационной безопасности»

Цель: научить планировать внедрение системы менеджмента информационной безопасности на предприятии.

Задачи:

Освоить проведение оценки рисков информационной безопасности.

Научиться выбирать меры информационной безопасности, подходящие для конкретного предприятия.

Получить навыки разработки плана по внедрению системы менеджмента информационной безопасности.

Место дисциплины в структуре программы.

Дисциплина позволяет оказать слушателям практическую помощь в планировании внедрения системы менеджмента информационной безопасности в соответствии с ISO 27001.

Перечень методических материалов

- методическое пособие;
- нормативные правовые акты

Требования к результатам освоения дисциплины.

В результате обучения дисциплине слушатели должны:

Знать: разделы международного стандарта ISO/IEC 27001, посвященные внедрению системы менеджмента информационной безопасности.

Владеть навыками планирования внедрения системы менеджмента информационной безопасности, профессионально и эффективно применять на практике приобретенные в процессе обучения знания и умения.

Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 8 часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) - 1 час, семинарские занятия – 7 ак. часов)

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля
			Внеаудиторная (самостоятельная работа)	Аудиторная работа (семинарские занятия)	
2	**Планирование процесса внедрения системы менеджмента информационной безопасности**	**8**	**1**	**7**	
2.1	Идентификация	1		1	

	информационных активов				
2.2	Определение ценности информационных активов	1		1	
2.3	Определение рисков и потерь	2	1	1	
2.4	Установление целей и выбор контрмер	3		2	
2.5	Подготовка плана внедрения СМИБ	1		1	
2.6	Процесс сертификации	1		1	

Тема 1. Идентификация информационных активов

- понятие «информационный актив»;
- выявление активов при анализе бизнес-процессов.

Тема 2. Определение ценности информационных активов

- количественные методы определения ценности активов;
- качественные методы определения ценности активов;

Тема 3. Определение рисков и потерь

- понятие «риск»;
- идентификация угроз;
- количественные методы оценки рисков;
- качественные методы оценки рисков;
- критерии оценки рисков;
- матрица вероятность-последствия.

Тема 4. Установление целей и выбор контрмер

- понятие «контрмера»;
- классификация контрмер;
- обзор контрмер из приложения А ISO/IEC 27001.

Тема 5. Подготовка плана внедрения СМИБ

- реализация цикла PDCA при внедрении СМИБ;
- роли и обязанности членов команды внедрения;
- разработка плана внедрения СМИБ.

Тема 6. Процесс сертификации

- процесс сертификации СМИБ в соответствии с ISO/IEC 27001.

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

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. Согласно ISO 27001 внутренние аудиты СУИБ должны быть…
   A. Проведены один раз в год
   B. Проведены в соответствии с принятой программой аудитов
   C. Проведены перед прохождением внешнего аудита
   D. Ничего из вышеперечисленного
3. Что является требованием ISO 27001?
   A. Наличие координатора рисков
   B. Задокументированный процесс обработки рисков
   C. Использование всех контролей приложения А
   D. Проведение ежемесячного анализа со стороны руководства
4. Что из нижеперечисленного является верным утверждением для документированной информации СУИБ в соответствии с ISO 27001 ?
   A. Она должна быть представлена в электронном формате
   B. Она должна храниться в единой системе документооборота
   C. Она может быть представлена в любой форме и на любом типе носителя
   D. Она должна храниться минимум три года
5. 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

6. 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

7. 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

8. Что из перечисленного требуется для демонстрации руководящей роли менеджмента?
   A. Утверждение политики СУИБ
   B. Обеспечение проведения внутренних аудитов СУИБ
   C. Все перечисленное

D. Назначение ролей и ответственностей за обеспечение ИБ

9. 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

10. Раздел 7.2 Компетенция имеет отношение к:
   A. Профессионалам в ИБ, осуществляющим управление СУИБ
   B. Менеджеру СУИБ и его команде
   C. Всему рабочему персоналу, способному оказывать влияние на информационную безопасность
   D. IT – персоналу

11. Шаги по устранению причин несоответствия называются:

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

12. Документальное свидетельство прошедшего события называется:

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

13. Что не является шагом в цикле Деминга

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

14. 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

15. Последовательность конкретных действий по предоставлению доступа к информационной системе описывается в:

   A. Политике
   B. Процедуре
   C. Стандарте
   D. Инструкции

16. Принципы информационной безопасности фиксируются в:

A. Политике
B. Процедуре
C. Стандарте
D. Инструкции

17. Рекомендации по способам формирования паролей пользователями включают в:

A. Политику
B. Процедуру
C. Руководство
D. Инструкцию