«СОГЛАСОВАНО»
Педагогическим Советом ЧОУ ДПО «УМЦ «РЕГКОН»
Протокол № 11 от 26 октября 2020 г.

«УТВЕРЖДЕНО»
Директором ЧОУ ДПО «УМЦ «РЕГКОН»
Распоряжение № 23Р от 18 декабря 2020 г

Учебная программа к образовательной программе повышения квалификации «Разработка, внедрение и внутренний аудит системы менеджмента информационной безопасности»

1 ЦЕЛЬ ОБУЧЕНИЯ

1.1 Предоставление обучающимся знаний и практических навыков, необходимых для разработки и внедрения системы менеджмента информационной безопасности (СМИБ) в соответствии с требованиями ISO/IEC 27001:2013.

1.2 Предоставление обучающимся знаний и навыков, необходимых для проведения внутренних аудитов СМИБ, с учетом руководящих указаний стандарта ISO 19011:2018, а также при оформлении отчетности по результатам внутреннего аудита и действиям после аудита.

2 ЦЕЛЕВАЯ АУДИТОРИЯ

2.1 Программа рассчитана на специалистов в области информационной безопасности (далее – ИБ) и ответственные за разработку, внедрение, сопровождение и проведение внутренних аудитов СМИБ.

3 КРАТКИЙ ОБЗОР ПРОГРАММЫ

3.1 Методологической базой являются стандарты ISO/IEC 27000, ISO/IEC 27001, ISO 19011:2018.

3.2 В рамках программы предлагается изучение требований ISO/IEC 27001:2013, терминологии процесса внутреннего аудита, методологии и практики проведения внутреннего аудита.

3.3 Учебной программой предусмотрено выполнение практических занятий, тестов по итогам каждого учебного дня и итогового теста.

4 ВХОДНЫЕ ТРЕБОВАНИЯ К ОБУЧАЮЩИМСЯ

4.1. Программа рассчитана на обучающихся, имеющих образование не ниже среднего (полного) общего.

4.2. Обучающиеся должны иметь начальные знания о требованиях, предъявляемых в Организации к сотрудникам по информационной безопасности и представление о руководящих указаниях по аудиту согласно ISO 19011:2018.

5 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОГРАММЫ

№	Наименование параметра	Описание
1	Общая продолжительность, академических часов	40
2	Общая продолжительность лекционных занятий, академических часов	18,9
3	Общая продолжительность практических занятий (в том числе тестов и анализ тестов), академических часов	21,1
4	Количество лекционных занятий	28

5	Количество практических занятий	19
6	Количество промежуточных тестов	4
7	Количество итоговых тестов	1
8	Максимальное количество обучающихся в группе	20
9	Время проведения аудиторных занятий	10:00-17:30

6 КРИТЕРИИ УСПЕШНОГО ОСВОЕНИЯ ПРОГРАММЫ

6.1. посещение всех занятий в ходе проведения семинара (отсутствие на занятиях менее 5% от общего времени семинара);
6.2. результативное выполнение практических работ;
6.3. успешная сдача промежуточных тестов (не менее 70%);
6.4. успешная сдача итогового теста (не менее 70%)

7 ВЫХОДНЫЕ ДАННЫЕ

7.1 По завершению программы обучающиеся должны:
- терминология и понятия ISO/IEC 27001:2013;
- основные требования ISO/IEC 27001:2013;
- содержание этапов и последовательность реализации процесса разработки и внедрения СМИБ в соответствии с ISO/IEC 27001:2013;
- общие принципы организации и проведения внутренних аудитов СМИБ;
- этапы и процедуру проведения внутреннего аудита;
- навыки анализа несоответствий, составления актов по несоответствиям, выявленным в ходе аудита, разработки корректирующих действий и умения оценивать их результативность;
- действия после аудита и умение оформлять отчетность по результатам аудитов.

7.2 Обучающиеся, выполнившие требования, по постоянной оценке, знаний, навыков и успешно сдавшие итоговый тест, получают удостоверение о повышении квалификации по программе «Разработка, внедрение и внутренний аудит системы менеджмента информационной безопасности».

7.3 Свидетельства о прослушивании программы «Разработка, внедрение и внутренний аудит системы менеджмента информационной безопасности» выдаются обучающимся при условии выполнения требований по посещаемости, но не сдавшим итоговый тест.

8 ПРОИЗВОДСТВЕННЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБУЧЕНИЯ

8.1 Производственные условия должны обеспечивать слушателям:
Помещения для проведения семинаров должно иметь:
- площадь не менее 2 кв. метров на одного слушателя;
- оснащение системами отопления и/или кондиционирования воздуха, обеспечивающими поддержание комфортной температуры;
- оборудование - мультимедийный проектор, компьютер, экран, доска для письма фломастерами или флип-чарт. Если используется доска для письма фломастерами, должны быть подготовлены листы бумаги формата А1 в количестве, необходимом для проведения практических занятий. На доске должны быть предусмотрены крепления для листов бумаги.

8.2. Производственные условия должны обеспечивать обучающимся:
- возможность проведения практических занятий с разбивкой группы обучающихся на подгруппы;
- достаточное освещение и вентиляцию, чтобы максимально уменьшить утомляемость обучающихся в процессе обучения;

– наличие рабочего места (стол и стул) для размещения учебных материалов и ведения записей.

8.3. Обучающимся и преподавателям курса должен быть предоставлен гардероб для верхней одежды, возможность беспрепятственно пользоваться санитарно-техническими помещениями.

9 РАЗДАТОЧНЫЕ МАТЕРИАЛЫ

– Учебный график
– Текст стандарта ISO/IEC 27001:2013 (для использования на семинарах ЧОУ ДПО «УМЦ «РЕГКОН» в учебных целях);
– Текст стандарта ISO/IEC 27000:2018 (для использования на семинарах ЧОУ ДПО «УМЦ «РЕГКОН» в учебных целях);
– Текст стандарта «Руководящие указания по аудиту систем менеджмента. Международный стандарт ISO 19011:2018» (для использования на семинарах ЧОУ ДПО «УМЦ «РЕГКОН» в учебных целях);
– Формы для выполнения практических занятий, тестов;
– Блокнот, ручка.

10 УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование разделов и дисциплин	Всего часов (минут)	В том числе		
			Лекции	практические, лабораторные, семинарские занятия	Форма контроля
1	**Введение.** «Необходимость информационной безопасности». «Требования к ИБ»	15	15		
2	**Лекция № 1.** «Требования к информационной безопасности. Предпосылки внедрения СМИБ»	30	30		
3	**Лекция № 2.** «Обзор стандартов серии ISO/IEC 27000». «Обзор национальных нормативных документов по ИБ».	30	30		
4	**Лекция № 3.** «Термины и определения информационной безопасности».	30	30		
5	**Практическое занятие № 1.** «Термины и определения информационной безопасности».	15		15	
6	**Лекция № 4.** «Структура ISO/IEC 27001:2013».	45	45		
7	**Лекция № 5.** «Требования ISO/IEC 27001:2013 к разработке и внедрению СМИБ»	30	30		
8	**Практическое занятие № 2.** «Создание Системы Менеджмента Информационной Безопасности».	30		30	
9	**Лекция № 6.** «Требования ISO/IEC 27001:2013. Ответственность руководства. Организация ИБ»	45	45		

10	**Практическое занятие № 3.** «Ответственность руководства».	30		30	
11	**Лекция № 7.** «Требования ISO/IEC 27001:2013. Внутренний аудит».	30	30		
12	**Подведение итогов первого дня. Ответы на вопросы слушателей.**	15		15	
13	**Тест по итогам 1 дня** и обзор результатов теста	30		15	15
14	**Практическое занятие № 4.** «Внутренние аудиты Системы Менеджмента Информационной Безопасности».	30		30	
15	**Лекция № 8.** «Анализ и улучшение СМИБ».	30	30		
16	**Практическое занятие № 5.** «Улучшение Системы Менеджмента Информационной Безопасности».	30		30	
17	**Лекция № 9.** «Контроль и управление рисками»	30	30		
18	**Практическое занятие № 6.** «Реестр Активов».	30		30	
19	**Лекция № 10.** «Требования ISO/IEC 27001:2013 к оценке риска»	30	30		
20	**Практическое занятие № 7.** «Оценка риска»	30		30	
21	**Лекция № 11.** «Требования ISO/IEC 27001:2013. Вопросы безопасности, связанные с персоналом».	30	30		
22	**Лекция № 12.** «Требования ISO/IEC 27001:2013. Контроль и управление рисками».	30	30		
23	**Практическое занятие № 8.** «Меры контроля и управления рисками».	45		45	
24	**Подведение итогов второго дня. Ответы на вопросы слушателей.**	15		15	
25	**Тест по итогам 2 дня** и обзор результатов	30		15	15
26	**Лекция № 13.** «Требования ISO/IEC 27001:2013. Физическая безопасность и защита от воздействия окружающей среды».	15	15		
27	**Лекция № 14.** «Требования ISO/IEC 27001:2013. Менеджмент систем связи и эксплуатации».	30	30		

28	**Практическое занятие № 9.** «Требования ISO/IEC 27001:2013. Менеджмент систем связи и эксплуатации».	30		30	
29	**Лекция № 15.** «Требования ISO/IEC 27001:2013. Контроль доступа».	30	30		
30	**Практическое занятие № 10.** «Требования ISO/IEC 27001:2013. Контроль доступа».	30		30	
31	**Лекция № 16.** «Требования ISO/IEC 27001:2013. Менеджмент инцидентов информационной безопасности».	45	45		
32	**Практическое занятие № 11.** «Требования ISO/IEC 27001:2013. Менеджмент инцидентов информационной безопасности».	45		45	
33	**Лекция № 17.** «Требования ISO/IEC 27001:2013. Управление непрерывностью бизнеса».	30	30		
34	**Лекция № 18.** «Требования ISO/IEC 27001:2013. Соответствие требованиям законодательства».	30	30		
35	**Лекция № 19** «Требования ISO/IEC 27001:2013. Отношения с поставщиками».	30	30		
36	**Подведение итогов третьего дня. Ответы на вопросы слушателей.**	15		15	
37	**Тест по итогам 3 дня и обзор результатов**	30		15	15
38	**Практическое занятие № 12.** «Оценка и управление рисками»	60		60	
39	**Лекция № 20** «Международные стандарты менеджмента».	15	15		
40	**Лекция № 21.** «Системы менеджмента современного бизнеса».	30	30		
41	**Лекция № 22.** «Внутренний аудит (Международные стандарты, Термины и определения)».	30	30		
42	**Практическое занятие № 13.** «Термины и определения».	15		15	
43	**Лекция №23.** «Менеджмент аудита»	90	90		
44	**Практическое занятие № 14.** «Планирование внутреннего аудита».	45		45	
45	**Практическое занятие № 15.** «Документация СМИБ»	30		30	

46	**Подведение итогов четвертого дня. Ответы на вопросы слушателей.**	15		15	
47	**Тест по итогам 4 дня и обзор результатов**	30		15	15
48	**Практическое занятие № 16.** «Анализ Политики СМИБ Организации».	60		60	
49	**Лекция № 24.** «Этапы аудита».	15	15		
50	**Практическое занятие № 17.** «Формирование акта о несоответствии».	50		50	
51	**Лекция № 25.** «Компетентность».	10	10		
52	**Лекция № 26.** «Действия после аудита».	15	15		
53	**Лекция № 27.** «Советы аудиторам».	30	30		
54	**Практическое занятие № 18.** «Подготовка опросного листа (чек-листа)».	45		45	
55	**Практическое занятие № 19.** «Проведение внутреннего аудита – «Ролевая игра»	30		30	
56	**Подведение итогов. Ответы на вопросы слушателей**	30		30	
57	**Итоговый тест.**	60			60
	ИТОГО	**1800**	**850**	**830**	**120**
		40	**18,9**	**18,4**	**2,7**

11. УЧЕБНЫЙ ПЛАН-ГРАФИК

Время	Темы занятий
	День 1
09.45 – 10.00	Регистрация слушателей.
10.00 – 10.15	Введение. «Необходимость информационной безопасности». Требования к ИБ»
10.15 – 10.45	Лекция № 1. «Требования к информационной безопасности. Предпосылки внедрения СМИБ».
10.45 – 11.15	Лекция № 2. «Обзор стандартов серии ISO/IEC 27000». «Обзор национальных нормативных документов по ИБ».
11.15 – 11.30	Перерыв
11.30 – 12.00	Лекция № 3. «Термины и определения информационной безопасности».
12.00 – 12.15	Практическое занятие № 1. «Термины и определения информационной безопасности».

Время	Темы занятий
12.15 – 13.00	Лекция № 4. «Структура ISO/IEC 27001:2013».
13.00 – 14.00	Обед
14.00 – 14.30	Лекция № 5. «Требования ISO/IEC 27001:2013 к разработке и внедрению СМИБ».
14.30 – 15.00	Практическое занятие № 2. «Создание Системы Менеджмента Информационной Безопасности».
15.00 – 15.45	Лекция № 6. «Требования ISO/IEC 27001:2013. Ответственность руководства. Организация ИБ».
15.45 – 16.00	Перерыв.
16.00 – 16.30	Практическое занятие № 3. «Ответственность руководства».
16.30 – 17.00	Лекция № 7. «Требования ISO/IEC 27001:2013. Внутренний аудит».
17.00 – 17.15	Подведение итогов первого дня. Ответы на вопросы слушателей.
17.15 – 17.30	Промежуточный тест первого дня
17.30	Конец занятий первого дня
День 2	
10.00 – 10.15	Анализ и обсуждение результатов теста первого дня
10.15 – 10.45	Практическое занятие № 4. «Внутренние аудиты Системы Менеджмента Информационной Безопасности».
10.45 – 11.15	Лекция № 8. «Анализ и улучшение СМИБ».
11.15 – 11.30	Перерыв.
11.30 – 12.00	Практическое занятие № 5. «Улучшение Системы Менеджмента Информационной Безопасности».
12.00 – 12.30	Лекция № 9. «Контроль и управление рисками.
12.30 – 13.00	Практическое занятие № 6. «Реестр Активов».
13.00 – 14.00	Обед
14.00 – 14.30	Лекция № 10. «Требования ISO/IEC 27001:2013 к оценке риска».
14.30 – 15.00	Практическое занятие № 7. «Оценка риска».
15.00 – 15.30	Лекция № 11. «Требования ISO/IEC 27001:2013. Вопросы безопасности, связанные с персоналом».
15.30 – 15.45	Перерыв.
15.45 – 16.15	Лекция № 12. «Требования ISO/IEC 27001:2013. Контроль и управление рисками».
16.15 – 17.00	Практическое занятие № 8. «Меры контроля и управления рисками».
17.00 – 17.15	Подведение итогов второго дня. Ответы на вопросы слушателей.

Время	Темы занятий
17.15 – 17.30	Промежуточный тест второго дня семинара.
17.30	Конец занятий второго дня
День 3	
10.00 – 10.15	Анализ и обсуждение результатов теста второго дня.
10.15 – 10.30	Лекция № 13. «Требования ISO/IEC 27001:2013. Физическая безопасность и защита от воздействия окружающей среды».
10.30 – 11.00	Лекция № 14. «Требования ISO/IEC 27001:2013. Менеджмент систем связи и эксплуатации».
11.00 – 11.15	Перерыв.
11.15 – 11.45	Практическое занятие № 9. «Требования ISO/IEC 27001:2013. Менеджмент систем связи и эксплуатации».
11.45 – 12.15	Лекция № 15. «Требования ISO/IEC 27001:2013. Контроль доступа».
12.15 – 12.45	Практическое занятие № 10. «Требования ISO/IEC 27001:2013. Контроль доступа».
12.45 – 13.00	Лекция № 16. «Требования ISO/IEC 27001:2013. Менеджмент инцидентов информационной безопасности».
13.00 – 14.00	Обед
14.00 – 14.30	Лекция № 16 (продолжение) «Требования ISO/IEC 27001:2013. Менеджмент инцидентов информационной безопасности».
14.30 – 15.15	Практическое занятие № 11. «Требования ISO/IEC 27001:2013. Менеджмент инцидентов информационной безопасности».
15.15 – 15.30	Перерыв.
15.30 – 16.00	Лекция № 17. «Требования ISO/IEC 27001:2013. Управление непрерывностью бизнеса».
16.00 – 16.30	Лекция № 18. «Требования ISO/IEC 27001:2013. Соответствие требованиям законодательства».
16.30 – 17.00	Лекция № 19 «Требования ISO/IEC 27001:2013. Отношения с поставщиками».
17.00 – 17.15	Подведение итогов третьего дня. Ответы на вопросы слушателей.
17.15 – 17.30	Промежуточный тест третьего дня
17.30	Конец занятий третьего дня
4 день	
10.00 – 10.15	Анализ и обсуждение результатов теста третьего дня.
10.15 – 11.15	Практическое занятие № 12. «Оценка и управление рисками»
11.15 – 11.30	Перерыв.
11.30 – 11.45	Лекция № 20

Время	Темы занятий
	«Международные стандарты менеджмента».
11.45 – 12.15	Лекция № 21. «Системы менеджмента современного бизнеса».
12.15 – 12.45	Лекция № 22. «Внутренний аудит» (Международные стандарты, Термины и определения).
12.45 – 13.00	Практическое занятие № 13. «Термины и определения».
13.00 – 14.00	Обед
14.00 – 14.15	Лекция №23. «Менеджмент аудита» (часть 1).
14.15 – 15.00	Лекция №23. «Менеджмент аудита» (часть 2)
15.00 – 15.30	Лекция №23. «Менеджмент аудита» (часть 3).
15.30 – 15.45	Перерыв.
15.45 – 16.30	Практическое занятие № 14. «Планирование внутреннего аудита».
16.30 – 17.00	Практическое занятие № 15. «Документация СМИБ»
17.00 – 17.15	Подведение итогов четвертого дня. Ответы на вопросы слушателей.
17.15 – 17.30	Промежуточный тест четвертого дня.
17.30	Конец занятий четвертого дня
5 день	
10.00 – 10.15	Анализ и обсуждение результатов теста второго дня курса.
10.15 – 11.15	Практическое занятие № 16. «Анализ Политики СМИБ Организации».
11.15 –11.30	Перерыв.
11.30 – 11.45	Лекция № 24. «Этапы аудита».
11.45 – 12.35	Практическое занятие № 17. «Формирование акта о несоответствии».
12.35 – 12.45	Лекция № 25. «Компетентность».
12.45 – 13.00	Лекция № 26. «Действия после аудита».
13.00 –14.00	Обед
14.00 – 14.30	Лекция № 27. «Советы аудиторам».
14.30 – 15.15	Практическое занятие № 18. «Подготовка опросного листа (чек-листа)».
15.15 –15.30	Перерыв.
15.30 – 16.00	Практическое занятие № 19.

Время	Темы занятий
	«Проведение внутреннего аудита - «Ролевая игра»
16.00 – 16.30	Подведение итогов. Ответы на вопросы слушателей
16.30 – 17.30	Итоговый тест.
17.30	Закрытие курса.