

## ПРИГЛАШЕНИЕ НА УЧЕБНЫЙ ВЕБИНАР

«Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности на соответствие ГОСТ Р ИСО /МЭК 27001-2021: лидерство, контекст организации, SWOT анализ, риск-ориентированный подход. Внутренний аудит, в соответствии ГОСТ Р ИСО 190011-2018».

### Место и время проведения

- ✓ 26-28 октября 2022г.
- ✓ Санкт-Петербург, ул. Парковая, д. 4, литер Д, ауд.227- очно/онлайн

### О курсе

**Новая версия!!!** Стандарт ГОСТ Р ИСО/МЭК 27001 – источник лучших практик при проектировании систем управления, применим практически к любой организации, независимо от формы собственности, вида деятельности, размера и внешних условий. Он нейтрален в технологическом плане и всегда оставляет возможность выбора технологий. Система менеджмента информационной безопасности (СМИБ) – часть общей системы управления, основанной на подходе деловых рисков, с целью создать, внедрить, эксплуатировать, постоянно контролировать, анализировать, поддерживать в рабочем состоянии и улучшать защиту информации. Является системным подходом по управлению конфиденциальной информацией. В данную систему входит персонал, производимые процессы и ИТ-системы, объединенные путем внедрения процессов риск-менеджмента. С целью формирования комплексных требований к безопасности информации стандарт определяет три основных показателя:

- оценка рисков, с которыми сталкивается организация (определение угрозы для ресурсов, их уязвимость и вероятность возникновения угроз, а также возможный ущерб);
- соблюдение законодательных, нормативных и договорных требований, которые должны выполняться самой организацией, ее партнерами по бизнесу, подрядчиками и поставщиками услуг;
- формирование комплекса принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности.

*Цель нашего вебинара- оказать методическую помощь большим и малым предприятиям различных отраслей промышленности*

### Курс позволит

- ❖ Повысить свою квалификацию в области системы менеджмента безопасности информации
- ❖ Развитие карьеры и профессионального роста;
- ❖ Возможность увеличить свои доходы.

### Курс содержит

- 1) Обзор стандарта:
  - ISO 27001:2021
  - ISO 27002:2021

## Документы по окончанию:

I. Удостоверение о прохождении курса

## Стоимость участия:

- Стоимость участия 1 человека – 25 000 рублей
- \* Скидки при участии от 2-х человек (500руб/с чел.)

## Контакты для связи

По вопросам содержания программы семинара и для оформления заявки обращаться:

Науман Светлана Сергеевна - эксперт СМ, E-mail: cert\_gociss@mail  
Тел.: (812) 387-13-09, +7-953-170-4057

## Программа семинара по теме:

«Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности на соответствие ГОСТ Р ИСО /МЭК 27001-2021: лидерство, контекст организации, SWOT анализ, риск-ориентированный подход».

1 День	
10.00-10.20	<b>Новые критерии Росаккредитации. Требования к сертификации систем менеджмента.</b>
10.20-16.00	<ul style="list-style-type: none"><li>• Контекст деятельности организации</li><li>• Потребности и ожидания заинтересованных сторон</li><li>• Область применения СМИБ</li><li>• Руководство. Лидерство. Ориентация на потребителей. Политика</li><li>• Действия по рассмотрению рисков и возможностей</li><li>• Ресурсы, Квалификация. Осведомленность</li><li>• Документированная информация</li><li>• Функционирование</li><li>• Мониторинг, оценка защищенности, анализ и оценивание</li><li>• Внутренний аудит</li><li>• Проверка со стороны руководства</li><li>• Постоянное улучшение</li></ul>
12.00-13.00	<b>Обеденный перерыв</b>
14.20-14.40	<b>Кофе пауза</b>
2 день	
10.00-15.00	<ul style="list-style-type: none"><li>• Категории мер обеспечения информационной безопасности</li><li>• Пересмотр Политик информационной безопасности</li><li>• Роли и обязанности по обеспечению ИБ</li><li>• Мобильные устройства и дистанционная работа</li><li>• Безопасность связанная с персоналом</li><li>• Менеджмент активов</li><li>• Управление доступом</li><li>• Криптография</li><li>• Физическая безопасность при эксплуатации. Контроль программного обеспечения</li><li>• Менеджмент информационной безопасности сетей</li><li>• Взаимоотношения с поставщиками</li><li>• Соответствие</li></ul>

<b>12.00-13.00</b>	<b>Обеденный перерыв</b>
<b>3 день</b>	
<b>10.00-13.00</b>	<b>Внутренний/внешний аудит. ГОСТ Р ИСО 19011-2018</b> <ul style="list-style-type: none"> <li>• Принципы аудита</li> <li>• Управление программой аудита</li> <li>• Определение целей программы аудита</li> <li>• Определение и оценка рисков и возможностей, связанных с программой аудита</li> <li>• Разработка программы аудита</li> <li>• Компетентность лица, управляющего программой аудита</li> <li>• Определение объема программы аудита</li> <li>• Выполнение программы аудита</li> <li>• Выбор и определение методов аудита</li> <li>• Выбор членов группы по аудиту. Руководитель группы</li> <li>• Управление результатами выполнения программы аудита</li> <li>• Управление записями по программе аудита</li> <li>• Мониторинг. Пересмотр и улучшение программы аудита.</li> <li>• Проведение аудита</li> <li>• Инициирование аудита</li> <li>• Установление контакта с проверяемой организацией</li> <li>• Определение возможности проведения аудита</li> <li>• Подготовка к проведению аудита. Анализ документированной информации</li> <li>• Планирование аудита. Риск-ориентированный подход при планировании</li> <li>• Проведение аудита. Назначение ролей и обязанностей сопровождающих и наблюдателей</li> <li>• Проведение открывающего совещания</li> <li>• Обмен информацией в ходе аудита</li> <li>• Места получения информации для аудита и доступ к ней</li> <li>• Анализ документированной информации в ходе аудита</li> <li>• Сбор и проверка информации</li> <li>• Формирование выводов</li> <li>• Подготовка заключений аудита</li> <li>• Проведение заключительного совещания</li> <li>• Подготовка и рассылка отчета об аудите</li> </ul>
<b>Обед 13.00-14.00</b>	
<b>14.00-15.00</b>	<b>Разбор несоответствий</b>
<b>15.00-16.00</b>	<b>Практическая работа: определение несоответствий, заполнение бланков несоответствий</b>

**ТЕМА СЕМИНАРА:**

«Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности на соответствие ГОСТ Р ИСО /МЭК 27001-2021: лидерство, контекст организации, SWOT анализ, риск-ориентированный подход. Внутренний аудит, в соответствии ГОСТ Р ИСО 190011-2018»

указать тему семинара

**ДАТА ПРОВЕДЕНИЯ:**

указать дату семинара

### Заявка на участие в семинаре (курсе повышения квалификации)

#### Данные заказчика

Организация (полное и краткое юридическое наименование)	
ФИО и должность руководителя, на основании чего действует	
Юридический адрес	
Почтовый адрес	
ИНН / КПП	
Банковские реквизиты	
Контактное лицо (фамилия, имя, отчество, телефон, E-mail)	

#### Информация об участниках семинара:

№	ФИО	Должность	Контакты (телефон/E-mail)
1.			
2.			
3.			

#### Информация для бронирования:

Название гостиницы	Удаленность от места	Стоимость руб. в сутки	Контакты
ВЕЛЕС мини-отель	15 мин. пешком	от 2000	<a href="http://www.veles-hotel.ru">www.veles-hotel.ru</a>
Мини-отель Моисеев	15 мин. пешком	от 2400	<a href="http://www.moiseevhotel.ru">www.moiseevhotel.ru</a>
Невский Отель Гранд	4 ст. метро и 20 мин пешком	от 4 650	<a href="http://www.hon.ru">www.hon.ru</a>

Руководитель предприятия \_\_\_\_\_

(подпись)

(ФИО)

Заполненные заявки просим направлять на электронную почту: [cert\\_gociss@mail.ru](mailto:cert_gociss@mail.ru)



АТТЕСТАТ АККРЕДИТАЦИИ  
ОРГАНА ПО СЕРТИФИКАЦИИ  
РА.RU. 13СМ43