

Уважаемый руководитель,
приглашаем Вас и специалистов Вашего предприятия на учебный семинар:

«Специалист по Системам менеджмента информационной безопасности (ISO/IEC 27001:2005)»

Дата проведения: 06 – 10 сентября 2010 г. (5 дней)

Место проведения: г. Донецк (учебный класс ТЮФ Норд Украина)

Целевая аудитория: первый руководитель, служба физической и экономической безопасности, служба информационной безопасности, служба ИТ, руководители подразделений

В настоящее время невозможно представить современный бизнес и процесс управления бизнесом без информации. Информационные активы обладают основными свойствами финансовых и материальных активов предприятия: стоимость, ценность для организации, возможность накопления, возможность трансформации в другие активы. Газетные страницы пестрят заголовками о разглашении закрытых данных, предприятия останавливают работу из-за потери или временной недоступности информации. При этом пострадавшие предприятия тратят на информационную безопасность немало средств. Информационная безопасность имеет более широкий смысл, чем защита конфиденциальных данных. Это сохранение конфиденциальности, целостности и доступности информации. Лучшей мировой практикой в области управления информационной безопасностью признан международный стандарт на системы менеджмента информационной безопасности ISO/IEC 27001:2005.

Курс «Специалист по Системам менеджмента информационной безопасности» подготовит специалиста по информационной безопасности в соответствии с международными стандартами. Курс предназначен для тех, кто занимается или планирует заниматься внедрением, поддержкой, контролем функционирования системы менеджмента информационной безопасности в соответствии с международными стандартами.

Программа семинара, сроки и стоимость:

Программа семинара	Даты / Время	Стоимость с НДС, грн
Курс «Специалист по Системам менеджмента информационной безопасности (ISO/IEC 27001:2005)» состоит из следующих модулей:	06-10.09	5000,00
Модуль SMS 1 Введение в Системы менеджмента информационной безопасности по требованиям ISO/IEC 27001:2005.	06.09 09:30-16:00	
Модуль SMS 2 Разработка и внедрение Системы менеджмента информационной безопасности по требованиям ISO/IEC 27001:2005.	07-09.09 09:00- 16:00	
Модуль SMS 3 Внутренний аудит Системы менеджмента информационной безопасности по требованиям ISO/IEC 27001:2005.	10.09 09:00-15:30	

Курс предусматривает получение знаний о структуре и требованиях стандарта, о информационных активах и их свойствах, о направлениях информационной безопасности, о внедрении и поддержке системы управления рисками, об анализе рисков, о предупреждающих и корректирующих мероприятиях по обеспечению информационной безопасности, о бизнес-процессах поддержания и совершенствования информационной безопасности. Участники курса получают практические навыки по разработке документации и реализации направлений менеджмента информационной безопасности на предприятии, а также теорию и практику внутреннего аудита процессов обеспечения информационной безопасности.

Лектором выступает опытный аудитор по системам менеджмента информационной безопасности, эксперт по стандарту ISO/IEC 27001. На счету лектора более 40 проведенных корпоративных и открытых учебных курсов. Лектор обладает сертификатами Lead auditor ISO/IEC 27001, Lead auditor BS 25999.

Подробная программа семинара, описание стандарта ISO/IEC 27001:2005, информация об учебном центре «ТЮФ Норд Академия - Украина», заявка на обучение - находятся в приложениях.

В стоимость участия входит:

- участие в семинаре
- консультации лектора
- комплект раздаточных материалов на бумаге
- компакт-диск с дополнительными материалами
- стандарты ISO/IEC 27001 и ISO 19011
- питание обедами в дни занятий
- НДС

Проезд к месту проведения семинара в указанную стоимость не входит.

Обращаем Ваше внимание на то, что расходы на участие в семинаре включаются в состав валовых расходов в соответствии со ст. 5 Закона «О налогообложении прибыли предприятий» №283/97-ВР.

Для участия в семинаре необходимо подать заявку по факсу (044) 461-90-69 или (062) 34-34-065, или по электронной почте mvoloskovets@tuev-nord.com.ua, yponomareva@tuev-nord.com.ua, Контактный телефон - (044) 583-53-68, (062) 34-34-097.

Дополнительная информация на нашем сайте www.tuev-nord.com.ua

С уважением,
Генеральный Директор ТЮФ Норд Украина



Шпак-Левенберг Г.Н.

Программа курса:

Модуль SMS 1 (1 день) Введение в Системы менеджмента информационной безопасности по требованиям ISO/IEC 27001:2005.

- I. Введение
 - **Информация, Виды и Роль информации, Свойства информации, Свойство «безопасности»**
 - **Проблемы безопасности, Аспекты безопасности**
- II. Безопасность информации – проблема менеджмента?
 - **Технические средства, Недостатки технических средств**
 - **Менеджмент ИБ**
- III. Система менеджмента
 - **Цикл PDCA, Место СМИБ в общей СМ, Принципы системы менеджмента**
 - **Стандарт 9001 – рекомендуемая база**
 - **ИСО/МЭК 27001 – Требования к лучшей практике менеджмента ИБ**
- IV. История 27001
- V. Выгоды внедрения стандарта
- VI. Активы – основные объекты стандарта
 - **идентификация активов, реестр активов, интегрированные активы**
- VII. Структура стандарта
 - **Вводная часть**
 - **Основная часть стандарта – требования к СМИБ**
 - **Приложения**

Модуль SMS 2 (3 дня) Разработка и внедрение Системы менеджмента информационной безопасности по требованиям ISO/IEC 27001:2005.

- I. Требования стандарта
- II. Система управление рисками по требованию стандарта ISO 27001:2005
 - **алгоритм определения рисков**
 - **реестр рисков**
 - **управление рисками**
- III. Реализация Требований стандарта и Приложения А (Обязательное к применению)
 - **Основа менеджмента ИБ - Требования 4-8**
 - **A5. ПОЛИТИКА В ОБЛАСТИ БЕЗОПАСНОСТИ.**
 - **A6. ОРГАНИЗАЦИЯ СИСТЕМЫ БЕЗОПАСНОСТИ.**
 - **A7. КЛАССИФИКАЦИЯ АКТИВОВ И УПРАВЛЕНИЕ.**
 - **A8. БЕЗОПАСНОСТЬ И ПЕРСОНАЛ.**
 - **A9. ФИЗИЧЕСКАЯ И ВНЕШНЯЯ БЕЗОПАСНОСТЬ.**
 - **A10. МЕНЕДЖМЕНТ КОМПЬЮТЕРОВ И СЕТЕЙ.**
 - **A11. УПРАВЛЕНИЕ ДОСТУПОМ К СИСТЕМЕ.**
 - **A12. ПРИОБРЕТЕНИЕ, РАЗРАБОТКА И ОБСЛУЖИВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ.**
 - **A13. МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**
 - **A14. ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ БИЗНЕСА.**
 - **A15. СООТВЕТСТВИЕ ЗАКОНОДАТЕЛЬСТВУ.**
- IV. Методика внедрения системы менеджмента информационной безопасности
 - **ИТ-грундшутц – германская экспресс-методика внедрения СМИБ, Каталоги ИТ-Грундшутц**
- V. Документация СМИБ
- VI. Алгоритм внедрения системы менеджмента информационной безопасности
- VII. Интеграция СМИБ по требованиям ISO/IEC 27001:2005 и системы менеджмента качества по требованиям ISO 9001:2000
- VIII. Сертификация СМИБ

Модуль SMS 3 (1 день) Внутренний аудит Системы менеджмента информационной безопасности по требованиям ISO/IEC 27001:2005.

- I. Требования стандарта ISO 19011:2002 к проведению аудитов.
 - **Виды аудитов.**
 - **Терминология аудита.**
- II. Этапы внутреннего аудита СМИБ.
- III. Планирование внутренних аудитов СМИБ.
 - **Область аудита.**
 - **Годовой план проверки.**
- IV. Аудит процессов и функциональных подразделений.
- V. Подготовка к проведению аудита.
- VI. Алгоритм сбора объективных свидетельств в процессе аудита.
 - **Ведение заметок в процессе аудита, Регистрация отклонений, Разработка отчета об аудите.**
- VII. Проведение корректирующих и предупреждающих действий.
 - **Проверка выполнения.**
- VIII. Требования к аудиторам.
 - **Этика аудита, Рекомендации аудиторам.**

Дополнительная информация

- Учебный курс содержит практические работы, ориентированные на понимание требований стандарта ISO/IEC 27001:2005 и умение проверить выполнение данных требований на практике.
- Учебный курс предусматривает обязательное тестирование участников, по результатам тестирования выдается:
 - сертификат «Внутреннего аудитора систем менеджмента информационной безопасности» (срок действия 3 года) и
 - сертификат «Специалиста по Системам менеджмента информационной безопасности» (без ограничения срока действия) или
 - свидетельство участника семинара «Специалист по Системам менеджмента информационной безопасности».

ISO/IEC 27001:2005

Международный стандарт ISO/IEC 27001:2005 «Системы менеджмента информационной безопасности. Требования».

Устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы.

Выгоды внедрения стандарта

Система управления информационной безопасностью на основе стандарта ISO 27001 позволит:

- Сделать большинство информационных активов наиболее понятными для менеджмента компании
- Выявлять основные угрозы безопасности для существующих бизнес-процессов
- Рассчитывать риски и принимать решения на основе бизнес-целей компании
- Обеспечить эффективное управление системой в критических ситуациях
- Проводить процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности)
- Четко определить личную ответственность Достигнуть снижения и оптимизации стоимости поддержки системы безопасности
- Облегчить интеграцию подсистемы безопасности в бизнес-процессы и интеграцию с ISO 9001:2000
- Продемонстрировать клиентам, партнерам, владельцам бизнеса свою приверженность к информационной безопасности
- Получить международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках
- Подчеркнуть прозрачность и чистоту бизнеса перед законом благодаря соответствию стандарту

О стандарте ISO/IEC 27001:2005

Основа стандарта ИСО 27001 – система управление рисками, связанными с информацией.

Система управления рисками позволяет получать ответы на следующие вопросы:

- На каком направлении информационной безопасности требуется сосредоточить внимание?
- Сколько времени и средств можно потратить на данное техническое решение для защиты информации?

Данный Стандарт определяет информационную безопасность как: «сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность».

Основной задачей информационной безопасности является защита информационных ресурсов компании от внутренних и внешних умышленных и неумышленных угроз (подделка, вандализм, кража, пожар, системный сбой и др.).

Целью информационной безопасности является обеспечение непрерывности бизнеса компании и минимизация бизнес-рисков путем предупреждения инцидентов безопасности и уменьшения размеров потенциального ущерба.

Наряду с элементами управления для компьютеров и компьютерных сетей, стандарт уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на работу, обучение, увольнение с работы), обеспечению непрерывности производственного процесса, юридическим требованиям.

ПОЛИТИКА НАШЕЙ РАБОТЫ

- Мы предоставляем широкий спектр учебных курсов в области менеджмента, позволяющий обучать менеджеров и специалистов работающих в различных направлениях менеджмента на предприятии.
- Мы работаем на рынке учебных услуг с 1999 года, в рамках нашего учебного центра прошли обучение более 3 000 специалистов по различным направлениям менеджмента.
- Наши лекторы являются действующими аудиторами. Поэтому наши курсы сопровождаются практическими невыдуманными примерами. Лекторы делают акценты на темах курса, которые вызывают сложности на предприятиях.
- Среди наших партнеров крупные высшие учебные заведения, консультационные компании, узконаправленные специализированные учебные центры, известные лекторы и консультанты.
- Наши клиенты работают с нами на протяжении многих лет, постоянно проявляют интерес к новым курсам и направлениям.

Среди наших клиентов АЗОЦМ, ДМЗ, Днепротяжмаш, Запорожсталь, МЗТМ, ММК им. Ильича, НКМЗ, НЗНТ, НТК, ЛАЗ, Норд, АСКА, В.А.Т.–Прилуки, Силур, Квазар-Микро, Нацбанк Казахстана, ДнепрАЗОТ, Запорожогнеупор, Веркон, Одескабель, РАЭС, Артемовский завод шампанских вин, Славутич и др. Всего более 250 крупных, средних и малых предприятий Украины, России и Казахстана.

Заявка на участие в семинаре

Наименование семинара:	Дата семинара:
Предприятие:	

Сотрудник(-и), участвующий(-ие) в семинаре:

1.	Фамилия	
	Имя	
	Отчество	
	Должность	
	Телефон:	
	Факс	
	e-mail:	
2.	Фамилия	
	Имя	
	Отчество	
	Должность	
	Телефон:	
	Факс	
	e-mail:	

Данные для подготовки договора

Точное и полное наименование предприятия	
Должность руководителя, подписывающего договор	
<ul style="list-style-type: none">• Ф.И.О. полностью	
<ul style="list-style-type: none">• Действующего на основании (Устава, доверенности №)	
Реквизиты: <ul style="list-style-type: none">• Адрес• Телефон• Факс• E-mail• МФО• Наименование банка• Р/с• ОКПО• Свидетельство №• Индивидуальный №	

Для участия в семинаре необходимо подать заявку по факсу (044) 461-90-69 или (062) 34-34-065, или по электронной почте mvoloskovets@tuev-nord.com.ua, yponomareva@tuev-nord.com.ua.
Контактный телефон - (044) 583-53-68, (062) 34-34-097
Дополнительная информация на нашем сайте www.tuev-nord.com.ua