10/14 Volnovaska Str., 03124, Kyiv, Ukraine
Tel.:+380 44 594 80 18; training@issp.com
www.issp.training

I-ISMS | Впровадження СУІБ за стандартами ДСТУ ISO / IEC 27001:2022, 27002:2022

Авторський курс від ISSP

3-денний курс про впровадження Систем Управління Інформаційною Безпекою (СУІБ).

Для кого:

- Керівники підрозділів безпеки на підприємствах
- Співробітники підрозділів безпеки, які займаються впровадженням, підтримкою і вдосконаленням систем інформаційної безпеки
- Аудитори інформаційної безпеки

Цей курс дає можливість:

- Впорядкувати знання про те, які елементи системи інформаційної безпеки потрібно впроваджувати і як робити це без помилок.
- Доповнити існуючі знання і скласти їх в органічну систему, зручну для використання в довгостроковому плануванні та щоденній роботі.
- Навчитися впроваджувати комплексну систему управління інформаційною безпекою на підприємстві.
- Обговорити практичні кейси і проаналізувати можливі помилки та нюанси які можуть відігравати вирішальну роль.
- Будувати і розвивати стосунки з професіоналами які щодня захищають IT системи різних підприємств від нових загроз, обмінюватися інформацією про нові загрози і методи боротьби з ними.

Програма курсу:

1. Особливості стандарту ДСТУ ISO / IEC 27001, 27002

2. Що таке інформаційна безпека?
- Цілі і вимоги ІБ
- Необхідні умови впровадження СУІБ
- Використання ризикового підходу при плануванні ІБ

3. Сфера застосування СУІБ

4. Оцінка і обробка ризиків

5. Нормативна документація СУІБ
- Порядок розробки і впровадження нормативної документації

- Адміністративні документи СУІБ
- Політики ІБ
- Бізнес процеси і їх опис
- Інструкції і технологічні карти, процедури, методики
- Протоколи інформаційних систем, аудиторські сліди

6. Стандарт 27001

- Область впровадження
- Нормативні посилання
- Терміни, визначення та абревіатури
- Контекст організації
- Лідерство
- Планування
- Підтримка
- Операційна діяльність
- Оцінка ефективності
- Покращення
- Додаток А

7. Стандарт 27002

- Область впровадження
- Нормативні посилання
- Терміни, визначення та абревіатури
- Структура документу
- Організаційні контролі
- Людські контролі
- Фізичні контролі
- Технологічні контролі
- Додатки

8. Основи методик управління ризиками ІБ

9. Відповіді на питання

*Стандарт 2022 року не входить в навчальний комплект ні в друкованоми вигляді, ні в PDF форматі

Формат навчання:
3 дні, з 10:00 до 17:30, з перервами на обід та кава-паузи.

Мова викладання:
Українська.

10/14 Volnovaska Str., 03124, Kyiv, Ukraine
Tel.:+380 44 594 80 18; training@issp.com
www.issp.training

Тренер курсу

Руслан Соловйов - експерт з інформаційної безпеки та сертифікований Lead Auditor ISO 27001.

Ключові компетенції:

- Розробка, впровадження, управління та аудит систем і процесів забезпечення інформаційної безпеки підприємств на базі вимог стандартів ISO 27000 та PCIDSS v2.0.
- Використання методології COBIT при проведенні аудитів інформаційної безпеки.
- Впровадження та адміністрування антивірусних, DLP, SIEM систем.
- Організація роботи та управління діяльністю інформаційно-технічної служби підприємства.
- Аналіз бізнес-процесів підприємства та розробка програмно-апаратних комплексів для їх оптимізації.