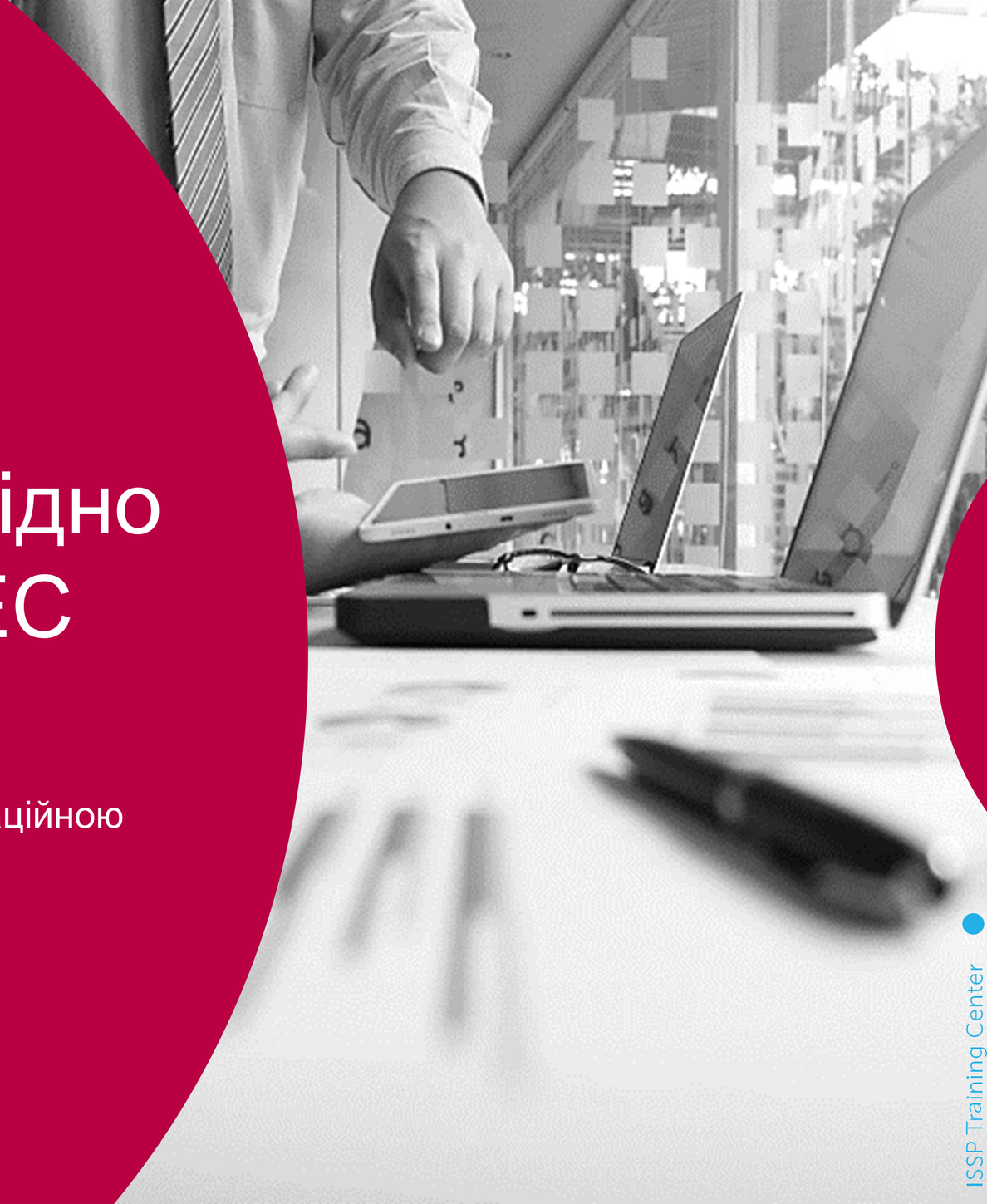
ISSP

I-ISMS

Впровадження СУІБ відповідно до стандарту ДСТУ ISO / IEC 27001, 27002

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



ISSP Training Center

Для кого:

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

ISSP

ISSP Training Center

Даний курс допоможе:

- 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:

Особливості стандарту ДСТУ ISO / IEC 27001, 27002

Що таке інформаційна безпека?

- Цілі і вимоги ІБ
- Необхідні умови впровадження СУІБ
- Використання ризикового підходу при плануванні ІБ

Сфера застосування СУІБ

Оцінка і обробка ризиків

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

Організація ІБ

- Внутрішня організація ІБ
- Мобільне обладнання та віддалена робота

Безпека людських ресурсів (до, під час і після закінчення роботи)

Управління ресурсами СУІБ

- Відповідальність за ресурси СУІБ
- Класифікація, маркування і правила обробки інформації
- Поводження з носіями

Програма курсу:

Контроль доступу

- Бізнес-вимоги до контролю доступу
- Управління правами доступу користувача
- Відповідальність користувача
- Контроль доступу до систем та прикладних програм

Криптографія

- Криптографічні засоби захисту

Фізична безпека та безпека інфраструктури

- Безпека приміщень, зони безпеки
- Безпека обладнання

Безпека експлуатації

- Процедури експлуатації та відповідальності
- Захист від зловмисного коду
- Резервне копіювання
- Ведення журналів аудиту та моніторинг
- Контроль програмного забезпечення, що перебуває в експлуатації
- Управління технічною вразливістю
- Розгляд аудиту інформаційних систем

Безпека комунікацій

- Управління безпекою мережі
- Обмін інформацією

Програма курсу:

Придбання, розробка та підтримка інформаційних систем
- Вимоги щодо безпеки для інформаційних систем
- Безпека в процесах розробки та підтримки
- Дані для тестування систем

Взаємовідносини з постачальниками
- Інформаційна безпека у взаємовідносинах з постачальниками
- Управління наданням послуг постачальником

Управління інцидентами ІБ
- Управління інцидентами інформаційної безпеки та вдосконаленням

Аспекти інформаційної безпеки управління безперервністю бізнесу
- Безперервність інформаційної безпеки
- Резервне обладнання

Відповідність
- Відповідність правовим та контрактним вимогам
- Перевірки інформаційної безпеки
- Відповідність вимогам стандартів безпеки

Основи методик управління ризиками ІБ

Відповіді на питання

Руслан Соловйов

Експерт з кібербезпеки
Сертифікований Senior 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.

Особливості та деталі

До навчального пакету входить:

- робота тренера
- навчальні матеріали (в електронному вигляді)
- сертифікат про проходження курсу від ISSP Training Center
- кава-брейки

Тривалість навчання:
3 дні

Мова навчання:
російська

Дати проведення:
3-5 листопада 2021

Місце проведення:
ISSP Training Center, вул. Радищева 10/14

ISSP Training Center

Контакти:

03680 м. Київ
вул. Радищева 10/14
+380 44 594 8018
https://goo.gl/maps/YV1qqDGUK4aHAhVX8

Кирило Кулаковський
Learning manager
Моб: +380 95 010 17 45
e-mail: kkulakovskyi@issp.com
https://www.issp.training/