**МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я**

**НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА УПРАВЛІННЯ ЯКІСТЮ**

**Дисципліна: Інтегровані системи управління**

# *Система управління інформаційною безпекою*

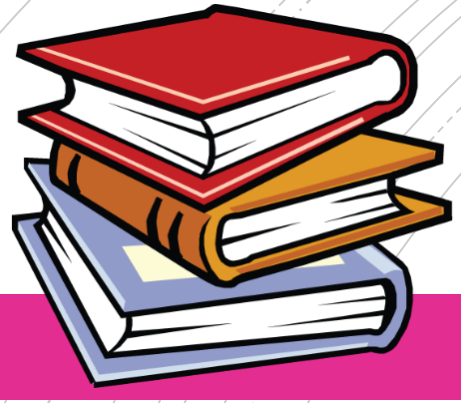
**Лектор: канд. фармац. наук, доцент Зборовська Тетяна Володимирівна**


# План лекції

- Історія виникнення та розвиток поняття інформаційної безпеки.
- Законодавча та нормативно-правова база з питань управління інформаційною безпекою України.
- Огляд структури, аналіз сфери і умов застосування стандарту ДСТУ **ISO/IEC 27001:2015**.
- Заходи забезпечення інформаційної безпеки на рівні організації.

# Питання для самостійної роботи

- Огляд стандартів серії 27000 – 27001, 27000, 27006, 27003, 27004, 27007, ISO/IEC 17799, ISO/IEC 15408, BS 7799 і нормативно-правової бази.
- Основоположні принципи забезпечення інформаційної безпеки відповідно до вимог стандарту ISO 27001.
- Основні напрями розвитку системи управління інформаційною безпекою в Україні та закордоном.

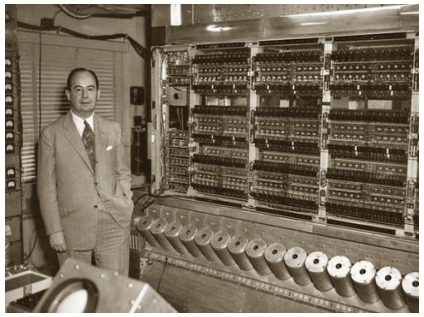


# Література

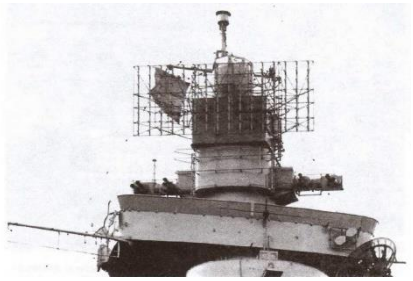

- ДСТУ ISO/IEC 27000:2015 “Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник”
- ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги”
- ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”, які прийняті наказом Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 18 грудня 2015 року № 193
- Закону України Про інформацію
- Закону України Про захист інформації в інформаційно-телекомунікаційних системах
- Закону України Про електронний цифровий підпис
- Закону України Про захист персональних даних

# Історія виникнення та розвиток поняття інформаційної безпеки

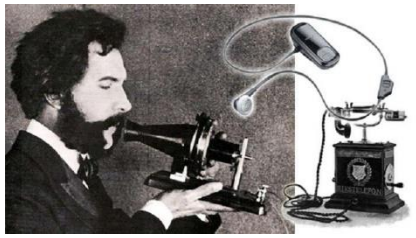
**з 1946 року**



**з 1935 року**



**з 1816 року**



**до 1816 року**

# Історія виникнення та розвиток поняття інформаційної безпеки

**З 1985 року**


**з 1973 року**

**з 1965 року**

# Інтереси держави в інформаційній сфері

- для гармонійного розвитку державної інформаційної інфраструктури
- для реалізації конституційних прав і свобод людини та громадянина
- в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва

# Державної служби спеціального зв'язку та захисту інформації України

Указом Президента України від 07.11.2005 № 1556/2005 «Про додержання прав людини під час проведення оперативно-технічних заходів»

Основні завдання Центрального органу виконавчої влади зі спеціальним статусом:

- реалізація державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних,
- забезпечення функціонування Державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, криптографічного та технічного захисту інформації.
- Держспецзв’язку створено на виконання прийнятого 23 лютого 2006 року Закону України «Про Державну службу спеціального зв’язку та захисту інформації України» на базі ліквідованого Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

# Законодавча та нормативно-правова база з питань управління інформаційною безпекою України

**Закони України:**

- Закон України «Про інформацію» від 02.10.1992 № 2657-XII
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
- Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
- Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

**Постанова КМУ:**

- Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373

# Законодавча та нормативно-правова база з питань управління інформаційною безпекою України

**Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ**

- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96 та
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу та ін.

**Галузеві стандарти**

# Інформаційна безпека Information security

- інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді
- захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї

# Основні принципи організації технічного захисту інформації (ТЗІ)

- *принцип легітимності захисту* – ґрунтуватися на положеннях і вимогах чинних в Україні нормативно-правових актів і нормативних документів щодо технічного захисту інформації;
- *принцип комплексності захисту* – захист повинен забезпечуватися комплексом взаємопов'язаних нормативних, організаційних заходів і програмно-технічних засобів;
- *принцип безперервності захисту* – захист повинен забезпечуватися на всіх технологічних етапах та режимах її функціонування і надання послуг, зокрема при проведенні ремонтних і регламентних робіт;
- *принцип мінімальної достатності захисту* – захист повинен забезпечувати необхідний рівень захищеності при мінімальних витратах ресурсів;

# Основні принципи організації технічного захисту інформації (ТЗІ)

- *програмно-технічні засоби захисту* не повинні істотно погіршувати основні характеристики (пропускну спроможність, надійність, можливість зміни конфігурації і т. ін.);
- *оцінка ефективності засобів захисту* є невід'ємною частиною робіт з ТЗІ, що здійснюється згідно з методиками, які враховують всю сукупність технічних характеристик оцінюваного об'єкта, включаючи технічні рішення і практичну реалізацію засобів захисту;
- *впровадження систем управління комплексами засобів захисту* повинні забезпечувати та здійснювати безперервний контроль ефективності засобів захисту, підтримку необхідного рівня захищеності інформаційних ресурсів.


## Система управління інформаційною безпекою – СУІБ information security management system, ISMS

- частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

# Тенденції в сфері менеджменту

| Top 10 countries for ISO/IEC 27001 certificates - 2017 | | |
|---|---|---|
| 1 | Japan | 9 161 |
| 2 | China | 5 069 |
| 3 | United Kingdom | 4 503 |
| 4 | India | 3 272 |
| 5 | United States of America | 1 517 |
| 6 | Germany | 1 339 |
| 7 | Italy | 1 220 |
| 8 | Taiwan, Province of China | 994 |
| 9 | Netherlands | 913 |
| 10 | Spain | 803 |

Україна: 47 організацій

# Тенденції в сфері менеджменту

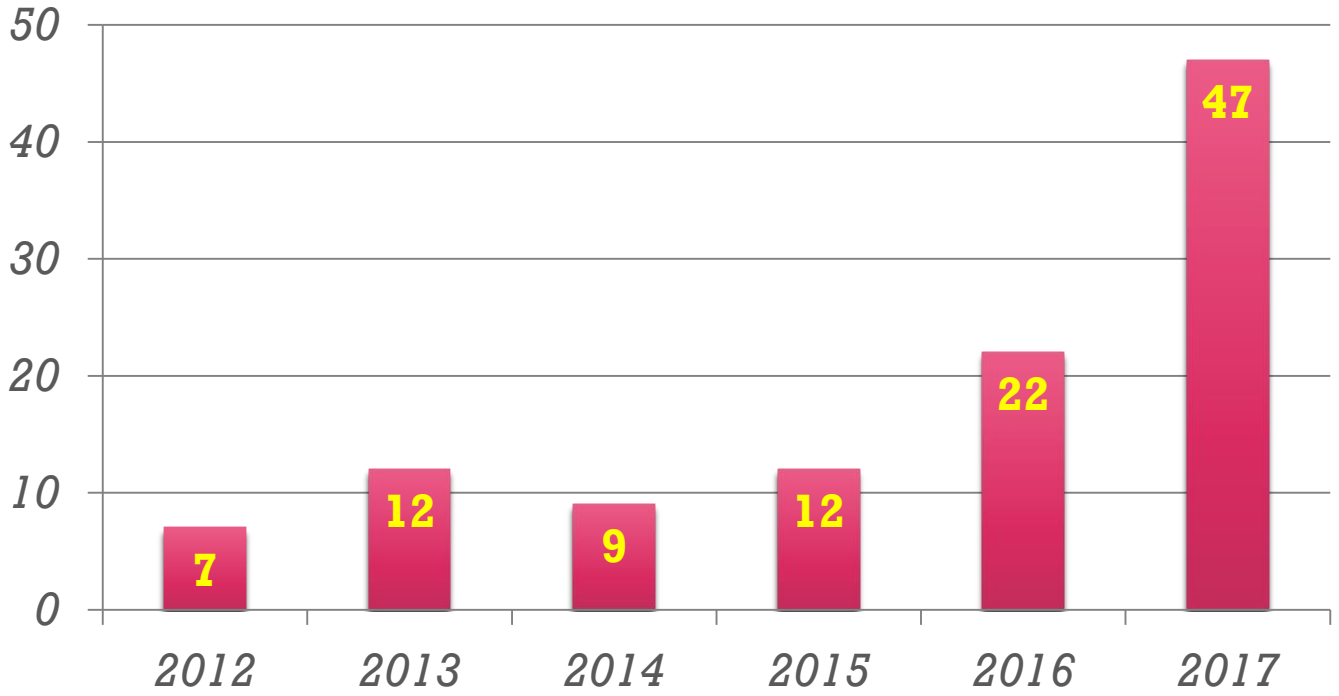
Переважні галузі (всього 39) за кількістю сертифікованих організацій на відповідність вимогам ISO / IEC 27001 в світі:

| Top 5 Industrial Sectors for ISO ISO/IEC 27001 certificates - 2017 | | |
|---|---|---|
| 1 | Информационные технологии | 7 478 |
| 2 | Другие услуги | 1 369 |
| 3 | Транспорт, связь и коммуникации | 930 |
| 4 | Финансовая, кредитная и страховая деятельность, жилищное хозяйство | 344 |
| 5 | Электротехника, точная механика, оптика | 316 |
| … | ….. | … |
| 28 | Фармацевтическая промышленность | 9 |

# Тенденції в сфері менеджменту

Динаміка сертифікації на відповідність вимогам ISO/IEC 27001 в Україні:

Інформаційні технології




Фінансова, кредитна і страхова діяльність, житлове господарство

27001

# Огляд стандарту ДСТУ ISO 27001

- визначає інформаційну безпеку як: «збереження конфіденційності, цілісності та доступності інформації»
- являє собою перелік вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації
- визначає процеси, що представляють можливість бізнесу встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки;
- встановлює вимоги до розробки, впровадження, функціонуванню, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації


# Зміст стандарту ДСТУ ISO 27001

1 Сфера застосування

2 Нормативні посилання

3 Терміни та визначення понять

4 Обставини організації

5 Керівництво

6 Планування

7 Підтримка

8 Функціонування

9 Оцінювання результативності

10 Вдосконалення

# Сфера застосування

- визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення СУІБ з урахуванням обставин організації.
- містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов’язаних з потребами організації.
- вимоги є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи

# Переваги застосування системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO

- Підвищити довіри до організації з боку контрагентів
- Спростити процедуру виходу на зовнішні ринки
- Систематизувати процеси забезпечення інформаційної безпеки
- Своєчасно виявляти і управляти ризиками, пов'язаними з зовнішніми та внутрішніми загрозами
- Оптимізувати процеси управління

# Сценарій управління інформаційною безпекою підприємства

Виявлення та ранжування загроз інформаційних ресурсів

Неформальна модель порушника

Аналіз структури і функцій інформаційної складової підприємства

Розробка пропозицій і рекомендацій з впровадження нових і підвищення ефективності існуючих механізмів ЗІБ

Аналіз і оцінка ризиків

# Види загроз інформаційної безпеки

- ***Загроза розкриття інформаційних ресурсів*** полягає у тому, що дані, інформація і знання стають відомими тим, кому не слід цього знати (несанкціонований доступ до ресурсів системи).
- ***Загроза порушення цілісності інформаційних ресурсів*** полягає в умисному антропогенному впливі (модифікація, видалення, знищення даних).
- ***Загроза порушення доступності до інформаційних ресурсів*** (здійснення дій, які унеможливлюють чи ускладнюють доступ до ресурсів інформаційної системи). Створення таких умов, при яких доступ до послуги або інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.


## Сценарій розрахунку ризиків складається з наступних базових складових

- визначення методології оцінювання ризику для інформаційної системи;
- розроблення критеріїв ухвалення ризиків та визначення прийнятого рівня ризику;
- визначення активів;
- виявлення небезпеки для активів;
- виявлення вразливих місць в системі захисту;
- виявлення дій, які порушують конфіденційність, цілісність та доступність активів та інформаційної системи;


## Сценарій розрахунку ризиків складається з наступних базових складових

- визначення ймовірності провалу системи безпеки за наявності переважних небезпек та вразливостей;
- оцінювання рівнів ризику;
- визначення прийнятності ризику або проведення процедури скорочення, використовуючи встановлені критерії допустимості та прийнятності ризику;
- вибір завдань та засобів управління для скорочення ризиків з умов забезпечення ефективності захисту.

# Етапи впровадження СУІБ

Етап 1. Діагностичний аудит

- Розробка документації СУІБ
- Навчання співробітників

Етап 2. Впровадження СУІБ

- Процес управління ризиками інформаційної безпеки
- Інвентаризація та класифікація інформаційних активів
- Оцінка та обробка ризиків
- Створення плану заходів з обробки ризиків

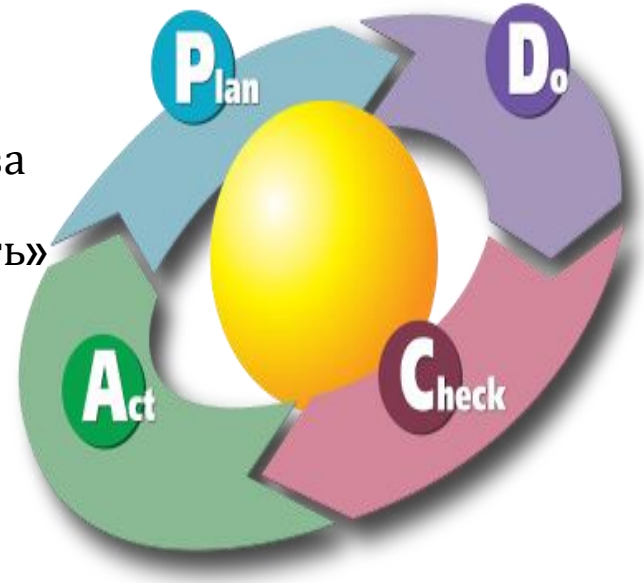
Етап 3. Сертифікація СУІБ на відповідність вимогам стандарту ISO 27001

## Організація СУІБ

- Визначення об’єму та меж СУІБ
- Визначення підходу до оцінки ризиків
- Ідентифікація та оцінка ризиків
- Оцінити підхід до обробки ризиків
- Вибір контролів (Додаток **А**)
- Отримання затвердження від керівництва
- Підготовка «Положення про застосовність»

## Підтримка та вдосконалення СУІБ

- Впровадження визначених вдосконалень
- Впровадження корегувальних та запобіжних заходів
- Інформування щодо визначених вдосконалень та заходів




## Впровадження та функціонування СУІБ

- Формулювання і впровадження Плану обробки ризиків
- Впровадження обраних контролів
- Проведення навчання співробітників
- Управління функціонуванням СУІБ
- Надання необхідних ресурсів СУІБ

## Моніторинг і аудит СУІБ

- Виконання процедур моніторингу
- Перегляд і оцінка ефективності СУІБ
- Проведення внутрішніх аудитів СУІБ
- Оновлення плану заходів по вдосконаленню СУІБ
- Збереження записів про інциденти інформаційної безпеки

# Обов'язкові документи СУІБ.

1. Записи ключових управлінських рішень стосовно СУІБ;
2. Набір політик інформаційної безпеки, у тому числі політика СУІБ і політика ІБ;
3. Опис сфери впливу СУІБ;
4. Опис заходів ІБ;
5. Документація контролів (засобів захисту, які охоплюють політику, заходи, настанови, втілення або організаційні структури);
6. Методи оцінки ризиків;
7. Звіти оцінки ризиків;
8. Інструкції щодо дій відносно ризиків;
9. Оперативні заходи СУІБ;
10. Оцінки ІБ;

# Обов'язкові документи СУІБ.

11. Звіт відповідності;

12. Заходи з контролю документів;

13. Заходи з контролю записів;

14. Записи ознайомлення з умовами безпеки, навчальні матеріали, а також матеріали ознайомлення з інформаційною безпекою, звіти з оцінками навчання та відгуками;

15. Плани та заходи внутрішнього аудиту СУІБ, а також звіти з аудиту СУІБ, погоджені плани дій і звіти з планових заходів, перевірок, припинення;

16. Заходи з виправлення невідповідностей;

17. Заходи із запобігання невідповідностям.

# ДЯКУЮ ЗА УВАГУ!!!