Комплексні системи захисту інформації та системи управління інформаційною безпекою (практичні питання створення та впровадження)

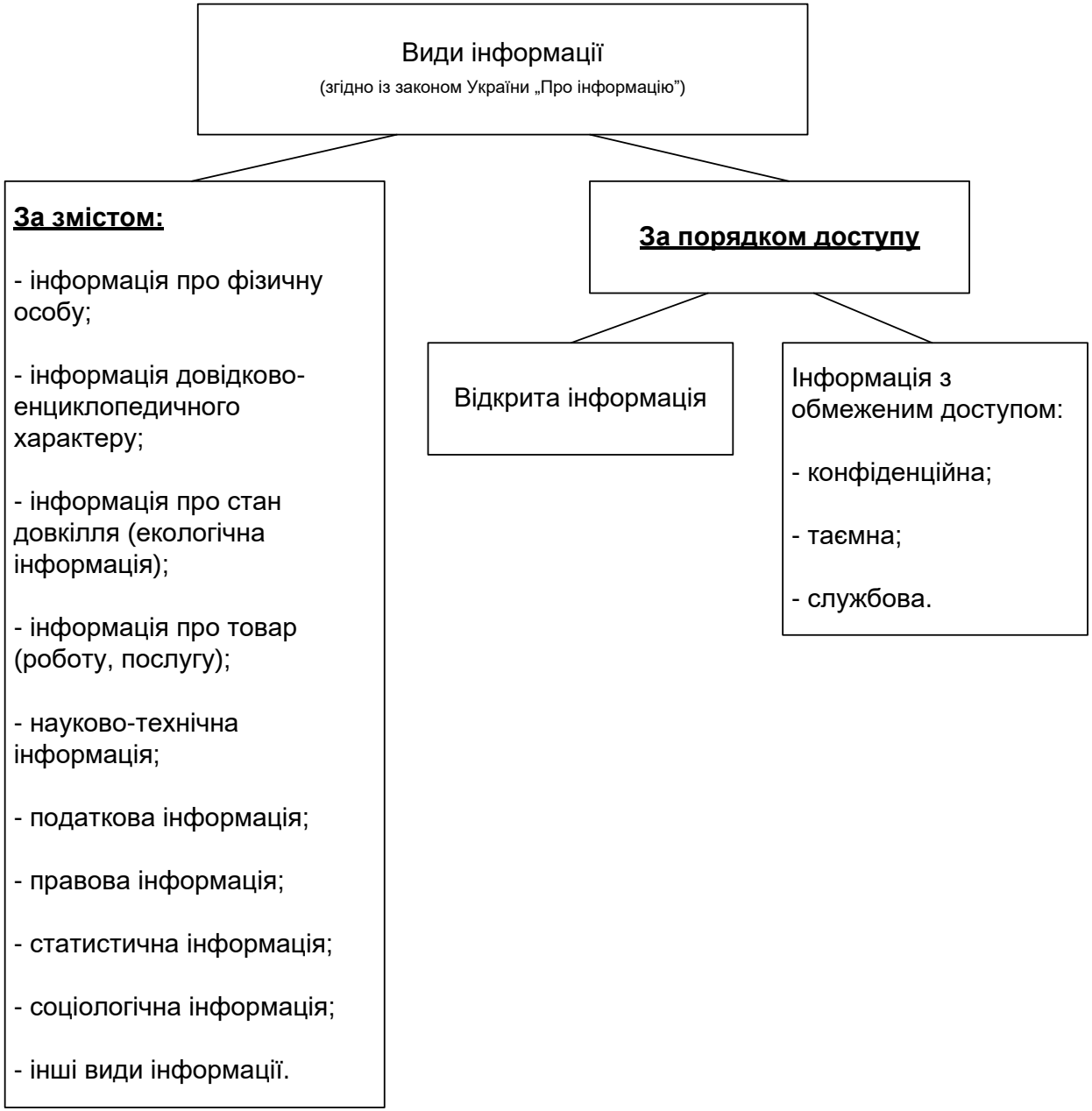
Комаров М.Ю.

Аспірант науково-навчального центру кіберфізичних систем, НАНУ

Засадничі нормативно-правові документи із технічного захисту інформації в Україні

- Закон України «Про інформацію»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закон України «Про захист персональних даних»;
- Закон України «Про доступ до публічної інформації»;
- Постанова Кабінету Міністрів України від 29.03.2006 №373 «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;
- Положення про технічний захист інформації в Україні (введено в дію Указом Президента України №1229/99 від 27.09.99);

- Положення про державну експертизу в сфері ТЗІ (затверджено наказом Адміністрації Держспецзв’язку № 93 від 16.05.2007 у редакції наказу № 565 від 13.10.17);
- ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- 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;
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;
- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;
- НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.


Види інформації
(згідно із законом України „Про інформацію”)
За змістом:
- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- інші види інформації.
За порядком доступу
Відкрита інформація
Інформація з обмеженим доступом:
- конфіденційна;
- таємна;
- службова.

Комплексна система захисту інформації

- НД ТЗІ 1.1-003-99

Комплексна система захисту інформації — сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС

Необхідність створення КСЗІ

- Закон України *«Про захист інформації в інформаційно-телекомунікаційних системах»*

Стаття 8. Умови обробки інформації в системі

Інформація, що є власністю держави, або ***інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом,*** повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

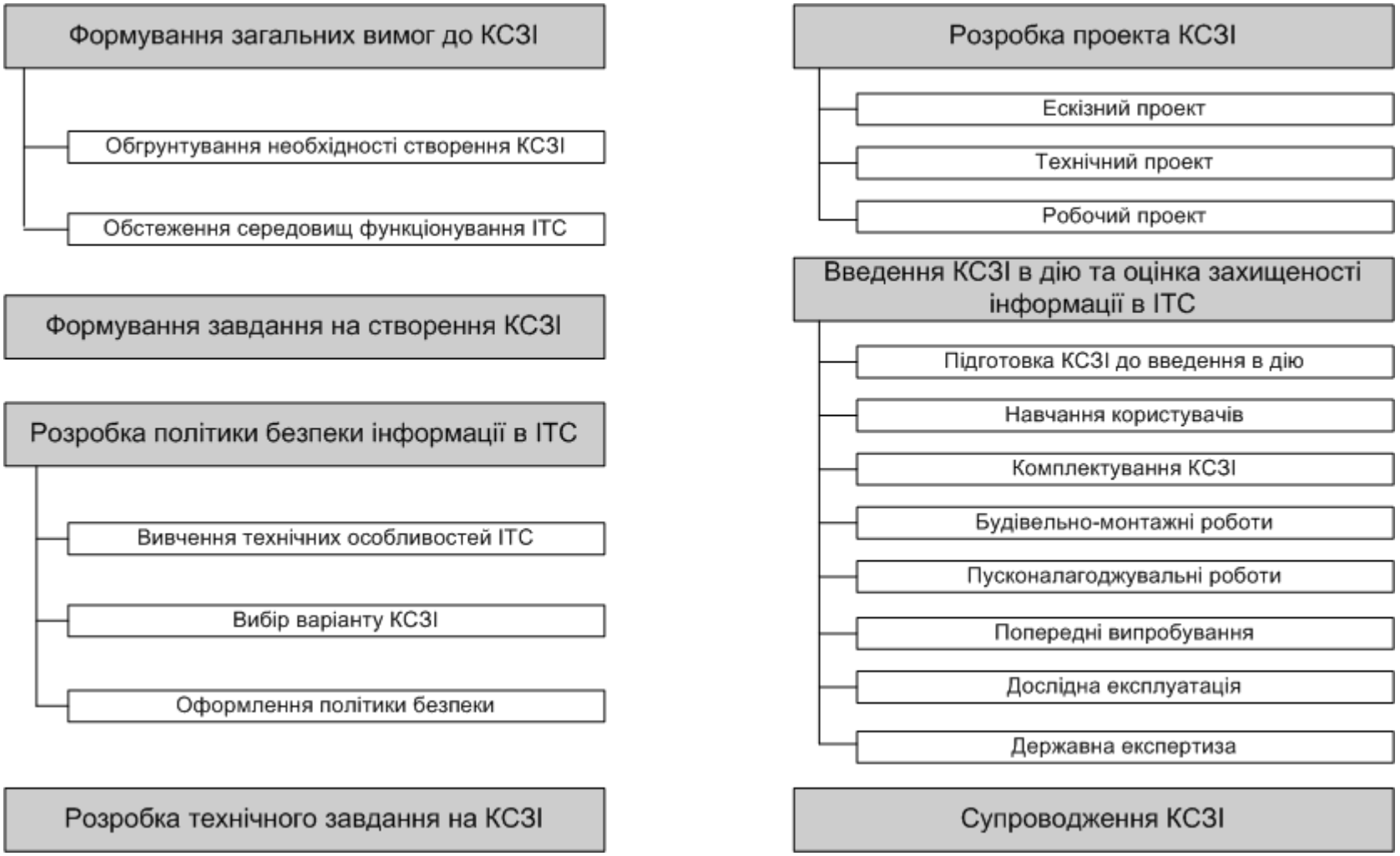
Необхідність створення КСЗІ

- *Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах* (ПКМУ № 373 від 29.03.2006)

4. Захисту в системі підлягає:

- Відкрита інформація, яка відноситься до ***державних інформаційних ресурсів***, а також ***інформація*** про діяльність суб'єктів владних повноважень, воєнних формувань, яка ***оприлюднюється в інтернеті***, інших глобальних інформаційних мережах та системах або передається телекомунікаційними мережами;
- ***Конфіденційна інформація***, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації»;
- ***Службова інформація*** (з грифом «Для службового користування»);
- інформація, що становить ***державну*** або іншу передбачену законом ***таємницю***;
- ***інформація***, ***вимога із захисту*** якої ***встановлена законом***.

Етапи створення КСЗІ



Система управління інформаційною безпекою

Система управління інформаційною безпекою (СУІБ) - це «та частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки».

(ISO 27001)

ОГЛЯД НОРМАТИВНОЇ БАЗИ

- **ISO27000** (ISO/IEC 27000:2009) «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Визначення та основні принципи».
- **ISO27001** (ISO/IEC 27001:2013) «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційної безпеки – Вимоги».
- **ISO27002** (ISO/IEC 27002:2013) «Інформаційні технології – Методи забезпечення безпеки – Практичні правила управління інформаційною безпекою».
- **ISO27003** (ISO/IEC 27003:2010) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з впровадження системи управління інформаційною безпекою».
- **ISO27004** (ISO/IEC 27004:2009) «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки - Вимірювання».

ОГЛЯД НОРМАТИВНОЇ БАЗИ

- **ISO27005** (ISO/IEC 27005:2011) «Інформаційні технології – Методи забезпечення безпеки – Управління ризиками інформаційної безпеки».
- **ISO27006** (ISO/IEC 27006:2007) «Інформаційні технології. Методи забезпечення безпеки – Вимоги до органів аудиту та сертифікації систем управління інформаційною безпекою».
- **ISO27007** (ISO/IEC 27007:2011) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з аудиту Систем управління інформаційної безпеки».
- **ISO27008** (ISO/IEC TR 27008:2011) «Інформаційні технології – Методи забезпечення безпеки – Керівництво для аудиторів з механізмів контролю Систем менеджменту інформаційної безпеки».
- **ISO27010** (ISO/IEC 27010:2012) «Інформаційні технології – Методи забезпечення безпеки – Управління інформаційною безпекою при комунікаціях між секторами».

ОГЛЯД НОРМАТИВНОЇ БАЗИ

- **ISO27011** (ISO/IEC 27011:2008) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з управління інформаційною безпекою для телекомунікацій».
- **ISO27013** (ISO/IEC 27013:2012) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з інтегрованого впровадження ISO/IEC 20000-1 та ISO/IEC 27001».
- **ISO27014** (ISO/IEC 27014:2013) «Інформаційні технології – Методи забезпечення безпеки – Базова структура управління інформаційною безпекою».
- **ISO27031 (**ISO/IEC 27031:2011**) «**Інформаційні технології – Методи забезпечення безпеки – Керівництво із забезпечення готовності інформаційних та комунікаційних технологій та їх використання для управління безперервністю бізнесу**».**
- **ISO27032 (**ISO/IEC 27032:2012**) «**Інформаційні технології – Методи забезпечення безпеки – Керівництво із забезпечення кібербезпеки**».**

ОГЛЯД НОРМАТИВНОЇ БАЗИ

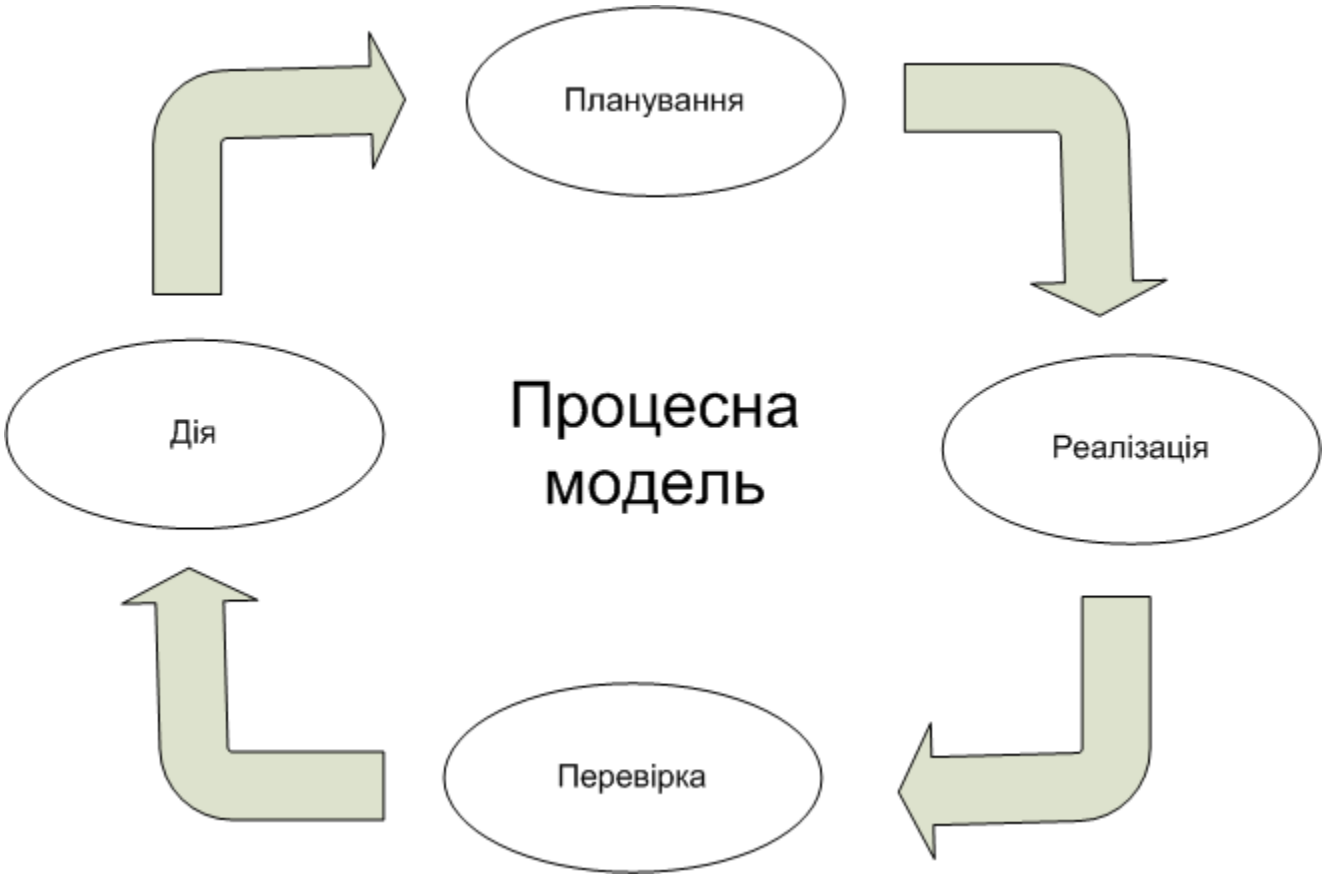
- **ISO27033 (**ISO/IEC 27033-1:2009**) «**Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Основні концепції управління мережевою безпекою**».**
- **ISO27033** (ISO/IEC 27033-2:2012) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Керівництво з проектування та впровадження системи забезпечення мережевої безпеки».
- **ISO27033** (ISO/IEC 27033-3:2010) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Базові мережеві сценарії – загрози, методи проектування та механізми контролю».
- **ISO27033** (ISO/IEC 27033-4:2014) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Забезпечення безпеки міжмережевих взаємодій за допомогою шлюзів безпеки - загрози, методи проектування та механізми контролю».
- **ISO27033** (ISO/IEC 27033-5) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Забезпечення безпеки Віртуальних Приватних Мереж - загрози, методи проектування та механізми контролю».

ОГЛЯД НОРМАТИВНОЇ БАЗИ

- **ISO27033** (ISO/IEC 27033-6) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Конвергенція в IP-мережах».
- **ISO27033** (ISO/IEC 27033-7) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Керівництво із забезпечення безпеки бездротових мереж – Ризики, методи проектування та механізми контролю».
- **ISO27034** (ISO/IEC 27034-1:2011) «Інформаційні технології – Методи забезпечення безпеки – Огляд та основні концепції в області забезпечення безпеки додатків».
- **ISO27035** (ISO/IEC 27035:2011) «Інформаційні технології – Методи забезпечення безпеки – Управління інцидентами безпеки».
- **ISO27036** (ISO/IEC 27036-1:2014) «Інформаційні технології – Методи забезпечення безпеки – Інформаційна безпека при взаємодії з постачальниками – Частина 1: Огляд та концепції».

ОГЛЯД НОРМАТИВНОЇ БАЗИ

- **ISO27036** (ISO/IEC 27036-2:2014) «Інформаційні технології – Методи забезпечення безпеки – Керівництво із взаємодії з постачальниками – Частина 2: Вимоги».
- **ISO27036** (ISO/IEC 27036-3:2013) «Інформаційні технології – Методи забезпечення безпеки – Інформаційна безпека при взаємодії із постачальниками – Частина 3: Керівні вказівки із захисту ланцюгів поставки інформаційних та комунікаційних технологій».
- **ISO27040** (ISO/IEC 27040:2015) «Інформаційні технології – Методи забезпечення безпеки – Безпека зберігання даних».
- **ISO27041** (ISO/IEC 27041:2015) **«**Інформаційні технології – Методи забезпечення безпеки – Керівництво з надання гарантій придатності та адекватності методу розслідування інциденту**».**


Планування
Реалізація
Перевірка
Дія
Процесна модель

ЕТАПИ СТВОРЕННЯ СУІБ

- вибір процесів (сфери діяльності), які передбачається сертифікувати;
- формування робочого колективу (команди);
- проведення внутрішнього аудиту з метою визначення поточного стану інформаційної безпеки в підприємстві;
- проведення ідентифікації ресурсів, що входять до обраної сфери діяльності;
- визначення цінності ресурсів;
- визначення ризиків;
- розробка пакету документів (політики, стандарти, положення, процедури, інструкції тощо);
- проведення внутрішнього аудиту та оцінку створеної СУІБ з урахуванням здійсненої роботи із впровадження організаційних та технічних заходів;
- подання заявки на проведення сертифікаційного аудиту;
- сертифікаційний аудит.

Дякую за увагу!