МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

_____	_____
На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
«___»_____20__ р.	«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

ПІДХОДИ ДО СТАНДАРТИЗАЦІЇ У СФЕРІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

СТУДЕНТ: Лебединець Марія Віталіївна _____
(підпис)

КЕРІВНИК: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЬ: к.т.н., с.н.с. Рабчун Дмитро Ігорович _____
(підпис)

Київ – 2021

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
«___» _____ 20__ р.

ЗАВДАННЯ

НА ДИПЛОМНУ РОБОТУ

студенту Лебединець Марії Віталіївні

1. Тема роботи «Підходи до стандартизації у сфері управління інформаційною безпекою», затверджена наказом по університету № 230 від «13» жовтня 2020 р.

2. Термін здачі студентом оформленої роботи «___» _____ 20___ р.

3. Об'єкт дослідження: стандартизація у сфері управління інформаційною безпекою.

4. Предмет дослідження: підходи до стандартизації у сфері управління інформаційною безпекою.

5. Мета дослідження полягає у дослідженні підходів до стандартизації у сфері управління інформаційною безпекою.

6. Перелік питань, які мають бути розроблені:

1. Дослідити нормативно-правове й інституційне забезпечення стандартизації в Україні.

2. Проаналізувати міжнародні стандарти ISO з управління інформаційною безпекою.

3. Вивчити стандартизовані вимоги до управління безпекою IT інших експертних організацій (COBIT, SP 800 NIST, ITIL).

4. Розглянути особливості вітчизняної практики стандартизації з управління інформаційною безпекою.

7. Дата видачі завдання «16» вересня 2020 р.

Науковий керівник Т.М. Мужанова
(підпис)

Завдання прийнято до виконання М.В. Лебединець
(підпис)

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи
студентом Лебединець Марією Віталієвною

Дата видачі завдання: «16» вересня 2020 р.

№ з/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	16.09.2020	
2.	Збір та аналіз літератури.	28.09.2020	
3.	Дослідження нормативно-правового й інституційного забезпечення стандартизації в Україні.	12.10.2020	
4.	Аналіз міжнародних стандартів ISO з управління інформаційною безпекою	22.10.2020	
5.	Вивчення стандартизованих вимог до управління безпекою ІТ інших експерт-них організацій (COBIT, NIST, ITIL)	02.11.2020	
6.	Розгляд особливостей вітчизняної практики стандартизації з управління інформаційною безпекою.	16.11.2020	
7.	Формулювання висновків за результатами проведеного дослідження.	23.11.2020	
8.	Оформлення роботи.	07.12.2020	
9.	Оформлення презентації.	14.12.2020	
10.	Отримання рецензії на роботу.	25.12.2020	
11.	Захист в ДЕК.	__.01.2021	

Студент _____ М.В. Лебединець
(підпис)

Науковий керівник _____ Т.М. Мужанова
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню підходів до стандартизації у сфері управління інформаційною безпекою. Робота складається зі вступу, чотирьох розділів, що містять 8 рисунків, висновків та списку використаних джерел з 39 найменувань. Загальний обсяг роботи становить 82 аркуши, з яких 4 аркуши займає список використаних джерел.

Об'єктом дослідження є стандартизація у сфері управління інформаційною безпекою.

Метою роботи є дослідження підходів до стандартизації у сфері управління інформаційною безпекою.

Для цього у роботі використані методи аналізу, зокрема нормативно-правової бази, синтезу, класифікацій та порівняння, системний та процесний підходи, теорії управління та стандартизації у сфері інформаційної безпеки.

Як результат у дипломній роботі досліджено нормативно-правове й інституційне забезпечення стандартизації в Україні; проаналізовано міжнародні стандарти ISO з управління інформаційною безпекою; вивчено стандартизовані вимоги до управління безпекою ІТ інших експертних організацій (COBIT, SP 800 NIST, ITIL); розглянуто особливості вітчизняної практики стандартизації з управління інформаційною безпекою.

Галузь застосування. Зазначені наукові напрацювання можуть бути використані при організації та впровадженні системи управління інформаційною безпекою організації на основі міжнародних стандартизованих підходів і кращих практик, що сприятиме підвищенню рівня ефективності управління інформаційною безпекою.

Ключові слова: СТАНДАРТИЗАЦІЯ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СТАНДАРТИ ISO/IEC 27к, COBIT, ITIL, SP 800 NIST.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ДСТУ – Державний стандарт України

ЗУ – Закон України

ІКСМ – інформаційно-комунікаційні системи і мережі

ІТКС – інформаційно-телекомунікаційна система

НД ТЗІ – нормативний документ технічного захисту інформації

НОС – національна організація стандартизації

СУІБ – система управління інформаційною безпекою

ТК – Технічний комітет

УІБ – управління інформаційною безпекою

ВСТУП

Актуальність теми. Стандартизація відіграє важливу роль у створенні вимог, які забезпечують національне виробництво конкурентоспроможної продукції, і, таким чином, спрямована на забезпечення якісного розвитку економіки України. На сучасному етапі основним завданням цього напрямку є створення ефективної, адекватної, визнаної на міжнародному рівні національної системи стандартів, вимоги якої гармонізовано з вимогами міжнародних та європейських організацій зі стандартизації.

Особливо актуальним є це завдання для динамічної галузі інформаційної безпеки. Вивчення міжнародної та вітчизняної практики з управління інформаційною безпекою дозволить сформувати в Україні передову нормативну базу у цій сфері. Саме успішний процес стандартизації є запорукою того, що в кінцевому результаті буде отримано якісний продукт – створено ефективні системи управління інформаційною безпекою на вітчизняних підприємствах.

З огляду на зазначене тема дипломної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки бізнес-суб'єктів.

Отже, дослідження підходів до стандартизації у сфері управління інформаційною безпекою є актуальним науковим завданням.

Мета і завдання дослідження. **Мета роботи** полягає у дослідженні підходів до стандартизації у сфері управління інформаційною безпекою.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Дослідити нормативно-правове й інституційне забезпечення стандартизації в Україні.
2. Проаналізувати міжнародні стандарти ISO з управління інформаційною безпекою.
3. Вивчити стандартизовані вимоги до управління безпекою IT інших експертних організацій (COBIT, SP 800 NIST, ITIL).
4. Проаналізувати особливості вітчизняної практики стандартизації з управління інформаційною безпекою.

Об’єкт дослідження - стандартизація у сфері управління інформаційною безпекою.

Предмет дослідження – підходи до стандартизації у сфері управління інформаційною безпекою.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, зокрема нормативно-правової бази, синтезу, класифікацій та порівняння, системний та процесний підходи, теорії управління та стандартизації у сфері інформаційної безпеки.

Наукова новизна одержаних результатів. У роботі розглянуто різні стандартизовані підходи до управління інформаційною безпекою, проаналізовано особливості сучасного стану стандартизації з управління інформаційною безпекою в Україні, окреслено основні проблеми та напрями вдосконалення вітчизняної нормативно-правової бази з інформаційної безпеки.

Практичне значення одержаних результатів. Застосування результатів дослідження доцільне при плануванні й реалізації системи управління інформаційною безпекою підприємства на основі міжнародних стандартів.

РОЗДІЛ 1.
НОРМАТИВНО-ПРАВОВЕ Й ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СТАНДАРТИЗАЦІЇ В УКРАЇНІ

1.1 Основи державної політики стандартизації в Україні

Жодне суспільство не існує без технічної бази та нормативних документів, що регламентують правила, процеси, методи виготовлення і контролю продукції, а також гарантують безпеку життя, здоров'я і майна людей і навколишнього середовища.

Стандартизація вважається одиним із діючих засобів прискорення технічного прогресу, впровадження найбільш раціональної організації виробництва, поліпшення якості продукції, економії трудових витрат і матеріальних ресурсів.

Метою стандартизації в Україні є підтримання безпеки для життя і здоров'я людини, флори, фауни, а також володінь і збереження навколишнього світу, також забезпечення умов для оптимального використання всіх різновидів державний ресурсів і відповідності об'єктів стандартизації своєму призначенню, сприяння усуненню технічних бар'єрів у торгівлі.

Після того, як Україна прийняла незалежність в 1991 році Постановою Кабінету Міністрів України №293 від 23.09.91 р. було створено державну систему стандартизації на базі Українського республіканського управління Держстандарту СРСР.

У травні 1993 р. наша країна побачила Декрет Кабінету Міністрів України «Про стандартизацію і сертифікацію». У червні Держстандарт України затвердив і ввів у дію перші 5 державних основоположних стандартів, що заклали фундамент державної системи стандартизації України:

1. ДСТУ 1.0:2003 Державна система стандартизація України. Основні положення.

2. ДСТУ 1.2:2003 Державна система стандартизація України. Порядок розробки державних стандартів.

3. ДСТУ 1.3:1993 Державна система стандартизація України. Порядок розробки, побудови, викладання та оформлення технічних умов.

4. ДСТУ 1.4:19933 Державна система стандартизація України. Стандарти підприємства. Основні положення.

5. ДСТУ 1.5:2003 Державна система стандартизація України. Загальні вимоги до побудови, викладання, оформлення та змісту стандартів.

В 1998 році Державний стандарт України підготував «Концепція розвитку національних систем стандартизації, сертифікації і акредитації», що підводить підсумки досягнень багаторічного досвіду стандартизації і визначає завдання по актуалізації цілей і методів стандартизації, вибору пріоритетних напрямків стандартизації і міжнародного співробітництва, гармонізації основної термінології з основними документами ISO, IEC, СОТ та ін.

При цьому підкреслюється необхідність практичної реалізації прийнятих у міжнародній практиці економічної, соціальної і комунікативної функцій стандартизації, що є однією з умов приєднання України до СОТ.

Стандартизація – це діяльність, що полягає у встановленні положень для загального і багаторазового застосування щодо наявних і можливих задач з метою досягнення оптимального рівня упорядкованості у визначеній сфері, результатом якої є підвищення рівня відповідності продукції, процесів і послуг їхньому функціональному призначенню, усунення технічних бар'єрів у торгівлі і сприяння науково-технічному співробітництву.

Об'єктами стандартизації є продукція, процеси і послуги, зокрема матеріали, устаткування, системи, їхнє об'єднання, правила, процедури, функції, методи або діяльність.

Державна політика в області стандартизації базується на таких основах:

- участь фізичних і юридичних осіб у розробці стандартів, можливість самостійно обирати види стандартів при виробництві;
- відкритість і прозорість методів розробки і прийняття стандартів, при цьому враховуються інтереси всіх сторін, що зацікавлені;

- підвищення конкурентоздатності продукції українських виробників;
- доступність стандартів для споживачів;
- відповідність стандартів положенням законів України;
- адаптація до нинішніх досягнень в науці і техніці з урахуванням стану державної економіки;
- пріоритетність введення на Україні міжнародних і регіональних стандартів;
- використання інтернаціональних та європейських правил і процедур стандартизації;
- участь у міжнародній (регіональній) стандартизації.

Мету стандартизації також ділять на загальну і більш вузьку, яка стосується забезпечення відповідності.

Загальна мета випливає частіше всього із сенсу поняття. Більша конкретика спільних цілей для державної стандартизації пов'язана з дотриманням тих правил стандартів, що вважаються обов'язковими.

До загальної мети відноситься розробка норм, вимог, засад, що забезпечують: якісну продукцію, роботу, послуги для життя людей, безпеку навколишнього середовища і майна; об'єднаність і взаємозамінність робіт; якість продукції; більш економне ставлення до всіх типів ресурсів; безпеку господарських об'єктів, що пов'язана з можливістю виникнення збоїв і НС різного масштабу; готовність держави до оборони та мобілізації.

Конкретна мета стандартизації відноситься до певної сфери виробництва товарів і послуг, того або іншого виду продукції, підприємства тощо.

Стандартизація може здійснюватися в різних ступенях. *Ступінь стандартизації* визначається з огляду на учасників, що приймають стандарт, і оцінку географічного, економічного, політичного регіону їх розташування. У випадку, якщо участь у стандартизації доступна для належних органів будь-якої країни, то це називається міжнародна стандартизація.

Регіональна стандартизація – сфера діяльності, що доступна лише для

відповідних державних органів певного географічного, політичного або економічного регіону світу. Регіональна і міжнародна стандартизації реалізується спеціалістами держав, представлених у відповідних регіональних і міжнародних організаціях.

Національна стандартизація - стандартизація в одній конкретній державі. Проте ця стандартизація також можлива на таких рівнях: державному, галузевому рівні, в різних секторах економіки, на рівні асоціацій, виробничих фірм, підприємств і установ.

Стандартизацію, яку проводять в адміністративно-територіальній одиниці (провінції, краї і т.д.), прийнято називати адміністративно-територіальною стандартизацією.

У 2014 році Президент України підписав закон України «Про стандартизацію», який установлює правові й організаційні основи стандартизації в Україні [1] і спрямований на забезпечення єдиної політики в цій сфері.

Закон «Про стандартизацію» включає 6 розділів (Рис. 1.1.):

1. Загальні положення.

2. Організація стандартизації.

3. Основні засади, процедури розроблення і прийняття та застосування національних стандартів, кодексів усталеної практики та змін до них.

4. Інформаційне забезпечення та право власності на національні стандарти, кодекси усталеної практики та каталоги і використання коштів, одержаних від їх реалізації.

5. Міжнародне співробітництво та фінансування робіт зі стандартизації.

6. Прикінцеві та перехідні положення.

Рис.1.1 Структура Закону України «Про стандартизацію»

ЗУ «Про стандартизацію» регулює відносини, зв'язані з діяльністю в сфері стандартизації і застосування її результатів, поширюється на суб'єкти господарювання незалежно від форми власності і видів діяльності, органи державної влади, а також на відповідні громадські організації.

Також під час опису державної політики у сфері стандартизації, окрім закону України «Про стандартизацію», необхідно звернути увагу на Закон України «Про технічні регламенти та оцінку відповідності», який визначає правові та організаційні засади розроблення, прийняття та застосування технічних регламентів і передбачених ними процедур оцінки відповідності, а також здійснення добровільної оцінки відповідності.

Закон «Про технічні регламенти та оцінку відповідності» [2] включає 11 розділів:

1. Загальні положення.

2. Положення органів виконавчої влади у сфері технічного регулювання.

3. Технічні регламенти та процедури оцінки відповідності.

4. Особливості розроблення та прийняття технічних регламентів і процедур оцінки відповідності.

5. Надання інформації про технічні регламенти, стандарти та процедури оцінки відповідності.

6. Оцінка відповідності.

7. Призначені органи.

8. Визнання результатів оцінки відповідності.

9. Контроль та відповідальність.

10. Прикінцеві та перехідні положення.

11. Сертифікація продукції в державній системі сертифікації.

ЗУ «Про метрологію та метрологічну діяльність» [3] - це закон, що регулює відносини, які виникають в процесі провадження метрологічної діяльності, зокрема такі їх аспекти:

1. Одиниці вимірювання. Національні еталони. Вимірювання. Засоби вимірювальної техніки.

2. Повноваження й організація роботи Національної метрологічної служби.

3. Оцінка відповідності та повірка засобів вимірювальної техніки.

4. Метрологічний нагляд.

5. Калібрування засобів вимірювальної техніки.

6. Фінансування метрологічної діяльності.

7. Визнання результатів метрологічних робіт.

8. Відповідальність за порушення законодавства про метрологію та метрологічну діяльність.

Закон України «Про основні принципи та вимоги до безпечності та якості харчових продуктів» [4] регулює відносини між органами виконавчої влади, операторами ринку харчових продуктів та споживачами харчових продуктів і визначає порядок забезпечення безпечності та окремих показників якості харчових продуктів, що виробляються, перебувають в обігу, ввозяться (пересилаються) на митну територію України та/або вивозяться (пересилаються) з неї.

Закон «Про основні принципи та вимоги до безпечності та якості харчових продуктів» нормативно закріплює:

1. Повноваження органів виконавчої влади у сфері безпечності та окремих показників якості харчових продуктів, лабораторні дослідження.

2. Санітарні заходи та окремі показники якості харчових продуктів.

3. Державні засади державної реєстрації об'єктів санітарних заходів.

4. Вимоги до виробництва й обігу харчових продуктів.

5. Загальні гігієнічні вимоги щодо поводження з харчовими продуктами.

6. Основи міжнародної торгівлі й міжнародного співробітництва.

7. Засади нажання адміністративних послуг у зазначеній сфері.

Чинне законодавство України складає міцну нормативну базу стандартизації на усіх рівнях управління економікою. Однак слід зазначити, що законодавство ще не повною мірою відповідає суспільним вимогам. Перед нашим суспільством стоїть важливе завдання - розробити і прийняти цілу низку законів, які б забезпечили справжній захист споживачів. Адже тільки держава може і повинна бути надійним гарантом цих прав.

Види стандартів

Класифікувати стандарти можна відповідно до ступенів стандартизації. Стандартизація (розробка, затвердження, прийняття і видання стандартів) здійснюється на рівні:

- фірми (стандарт підприємства);
- групи фірм (стандарт концерну);
- міністерства (галузевий стандарт);
- національному (наприклад, нацстандарт України ДСТУ);
- регіональному (наприклад, EN);
- міждержавному (наприклад, в рамках СНД);
- міжнародному (стандарт ISO).

Стандартизація на рівні фірм, груп фірм розповсюджується лише на продукт, що виробляється на конкретному підприємстві або підприємствах групи. Розробляючи стандарт підприємство переслідує такі цілі:

- встановити підвищені вимоги до продукту чи послуги в порівнянні з вимогами, прийнятими у конкурентів;
- регламентувати внутрішні вимоги, раціоналізувати процеси і операції;
- забезпечити гарантії споживачам.

Національні стандарти розробляють національні органи зі стандартизації (на Україні - Державне підприємство «УкрНДНЦ»), галузеві - відповідними міністерствами і відомствами. Галузеві стандарти розробляються на продукцію за відсутності державних стандартів або необхідності встановлювати вимоги, що перевищують чи доповнюють вимоги національних стандартів.

Стандартизація на національному та галузевому рівнях має за мету:

- забезпечити потреби суспільства в розвитку за рахунок прийняття єдиних вимог на основі останніх досягнень науки і техніки;
- забезпечити захист здоров'я і життя споживачів, охорону навколишнього середовища, а також захист вітчизняного товаровиробника;
- усунути технічні бар'єри в торгівлі за рахунок прийняття міжнародних вимог.

Міжнародні та регіональні стандарти приймаються відповідно міжнародними і регіональними організаціями зі стандартизації. Міжнародна стандартизація спрямована на полегшення торговельних і виробничих відносин у світі, що особливо актуально при становленні глобальних міжнародних ринків, таких як Єдиний Європейський, Північно-Американський, Азіатсько-Тихоокеанський. Регіональна стандартизація спрямована на захист інтересів окремого регіону. Зокрема, стандартизація в Європі (регіональна стандартизація) призначена для забезпечення потреб Єдиного Європейського ринку.

У межах держави застосовуються тільки національні стандарти. Міжнародний або регіональний стандарт не обов'язковий до включення в

національний збірка стандартів. Кожна країна самостійно вирішує питання про прийняття міжнародного чи регіонального стандарту як національного.

1.2 Суб'єкти стандартизації в Україні

Стандартизацією займається призначений на національному, регіональному і міжнародному рівні орган стандартизації. Основними функціями даного органу згідно законодавства є: розробка, узгодження і затвердження стандартів.

В Законі України «Про стандартизацію» (ст.11) сказано, що функції національного органу стандартизації виконує державне підприємство, що не підлягає приватизації, утворене центральним органом виконавчої влади, що реалізує державну політику у сфері стандартизації.

Розпорядженням Кабміну України від 26.11.2014 № 1163-р визначено, що робота національного органу стандартизації лягає на *державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості»*.

Державне підприємство «УкрНДНЦ» займається питаннями:

- організації та координації щодо розробки, прийняття, перевірки, перегляду, скасування і відновлення дії національних стандартів;
- прийняття, скасування і відновлення дії національних стандартів;
- підготовка та затвердження програми робіт з національної стандартизації;
- координація діяльності технічних комітетів зі стандартизації;
- видання національних стандартів;
- формування та ведення національного фонду нормативних документів;
- забезпечення функціонування та розвитку національної системи стандартизації, технічна перевірка проектів стандартів, гармонізація національних стандартів з міжнародними та європейськими, координація діяльності національних технічних комітетів стандартизації, консультації щодо маркування продукції;
- сертифікація продукції, послуг та систем управління;

- оцінка відповідності продукції технічним регламентам;
- підготовка та підвищення кваліфікації фахівців у сфері стандартизації, сертифікації, метрології та систем управління, підготовка наукових кадрів вищої кваліфікації;
- видання наукового фахового журналу «Стандартизація, сертифікація, якість».

Аналізуючи вище сказане, можна зробити висновок, що перший крок здійснено - національним органом стає підприємство, хоча і державне. Іншими суб'єктами стандартизації відповідно до ст.8 зазначеного Закону є (рис.1.2):

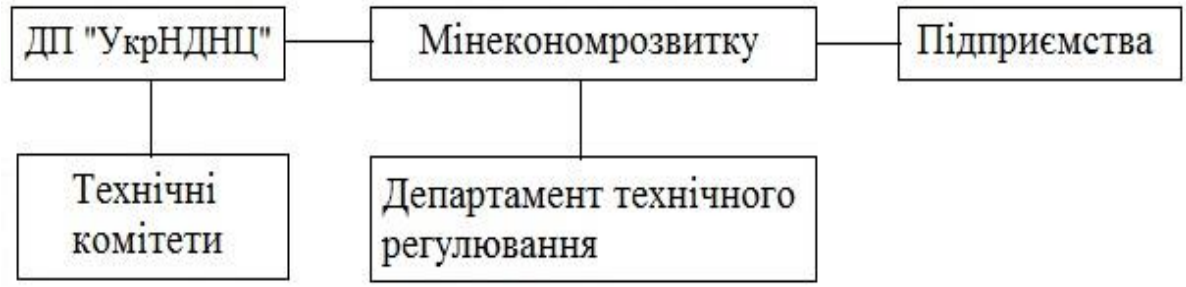

Рис. 1.2 Суб'єкти стандартизації в Україні

1. Центральним органом виконавчої влади, який забезпечує формування державної політики у сфері стандартизації - Міністерство економічного розвитку і торгівлі України.

Даний орган реалізує такі функції, як:

- забезпечення нормативно-правового регулювання у сфері стандартизації;
- визначення пріоритетних напрямків розвитку у сфері стандартизації;
- інформування і надання роз'яснень щодо реалізації державної політики у сфері стандартизації;
- узагальнення практики застосування законодавства у сфері стандартизації;
- погодження програми робіт з національної стандартизації.

2. Центральний орган виконавчої влади, що виконує держполітику у сфері технічного регулювання (стандартизації, метрології, сертифікації, оцінки відповідності, акредитації органів з оцінки відповідності, управління якістю) –

Департамент технічного регулювання, що є самостійним структурним підрозділом центрального апарату Мінекономрозвитку;

Цей департамент виконує такі завдання, як:

- вжиття обґрунтованих заходів для прийняття і дотримання суб'єктами стандартизації Кодексу доброчинної практики з розробки, прийняття та застосування стандартів відповідно до Угоди Світової організації торгівлі про технічні бар'єри у торгівлі, що є додатком до Марракеської Угоди про заснування Світової організації торгівлі від 15 квітня 1994 року;
- здійснення контролю за дотриманням національним органом стандартизації процедур у сфері стандартизації відповідно до принципів, норм і вимог, установлених цим Законом та іншими нормативно-правовими актами.

3. Технічні комітети стандартизації.

Функції технічних комітетів:

- участь у роботі відповідних технічних комітетів стандартизації міжнародних і регіональних організацій стандартизації;
- розроблення і погодження національних стандартів, кодексів усталеної практики та змін до них;
- участь у формуванні програми робіт з національної стандартизації;
- перевірка і перегляд національних стандартів та кодексів усталеної практики, розробниками яких вони є;
- погодження і надання пропозицій щодо скасування та відновлення дії національних стандартів, кодексів усталеної практики та змін до них.

4. Підприємства, установи та організації, що здійснюють стандартизацію.

З усіх перелічених суб'єктів стандартизації необхідно особливу увагу звернути на технічні комітети. Відповідно до каталогу, розміщеного національним органом стандартизації (ДП «УкрНДНЦ»), нині в Україні діє 321 технічний комітет, 13 з них знаходяться на окупованій території. Слід додати, що ДП «УкрНДНЦ» повідомляє про те, що на засіданні керівної ради національного

органу стандартизації від 25.02.2019 № 1, було підтримано ідею щодо призупинення діяльності 24 непрацюючих ТК стандартизації (рис 1.3):

Рисунок 1.3 Співвідношення ТК на лютий 2019 року.

Коли розпочався військовий конфлікт на території нашої країни, то частина ТК, які працювали на нині тимчасово окупованих територіях на деякий час принили свою діяльність.

Ще до неактивних ТК відносять ті, які протягом двох років не подають пропозицій до Програми робіт з національної стандартизації, не проводять засідань ТК, не подають щорічних звітів щодо своєї діяльності, не надсилають інформацію за вимогою національного органу стандартизації, не виконують робіт з національної стандартизації та не мають оновленого Положення про ТК, розробленого відповідно до ДСТУ 1.14:2015. Робота цих ТК фактично не здійснюється.

1.3 Порядок розробки і видання державних стандартів

Державні стандарти в Україні розробляються відповідно до основоположного стандарту ДСТУ 1.2:2003 «Національна стандартизація. Порядок розроблення національних нормативних документів» [6]. Цей стандарт встановлює вимоги щодо порядку розробки, узгодження, затвердження, державної реєстрації,

видання, впровадження, перевірки, перегляду, зміни чи скасування державних стандартів України.

Розробкою державних стандартів займаються ТК зі стандартизації, міністерства (відомства), головні (базові) організації зі стандартизації чи організації (підприємства), які мають необхідний науково-технічний потенціал у відповідній сфері. Дану розробку проводять відповідно до плану державної стандартизації з врахуванням норм діючого законодавства України, вимог стандартів державної системи стандартизації та документів міжнародних та регіональних організацій по стандартизації, а також з використанням результатів науково-дослідних, дослідно-конструкторських, проектних робіт і патентних досліджень.

За побудовою, змістом, оформленням стандарти повинні відповідати ДСТУ 1.5:2003 «Державна система стандартизації України. Загальні вимоги до побудови, викладу, оформлення та змісту стандартів» [6].

Згідно із Законом України «Про стандартизацію» правила і порядок розробки, схвалення та прийняття національних стандартів, що установлюються центральним органом виконавчої влади в сфері стандартизації, передбачати:

- критерії врахування чи відхилення пропозицій щодо розробки національних стандартів;
- критерії визначення розробників національних стандартів;
- визначення пріоритетів щодо застосування міжнародних (регіональних) стандартів;
- механізм апеляції;
- інформування зацікавлених сторін про стан робіт у сфері національної стандартизації. Термін розгляду проекту національного стандарту і надання відзивів не може бути меншим, ніж 60 днів із дня його опублікування;
- ознайомлення за рівних умов з проектами національних стандартів усіх зацікавлених сторін.

Стадії розроблення стандартів наступні:

1) організація розробки стандарту;
2) розробка проекту стандарту (першої редакції);
3) розробка проекту стандарту (остаточної редакції);
4) затвердження та державна реєстрація стандарту;
5) видання стандарту (Рис.1.4.).

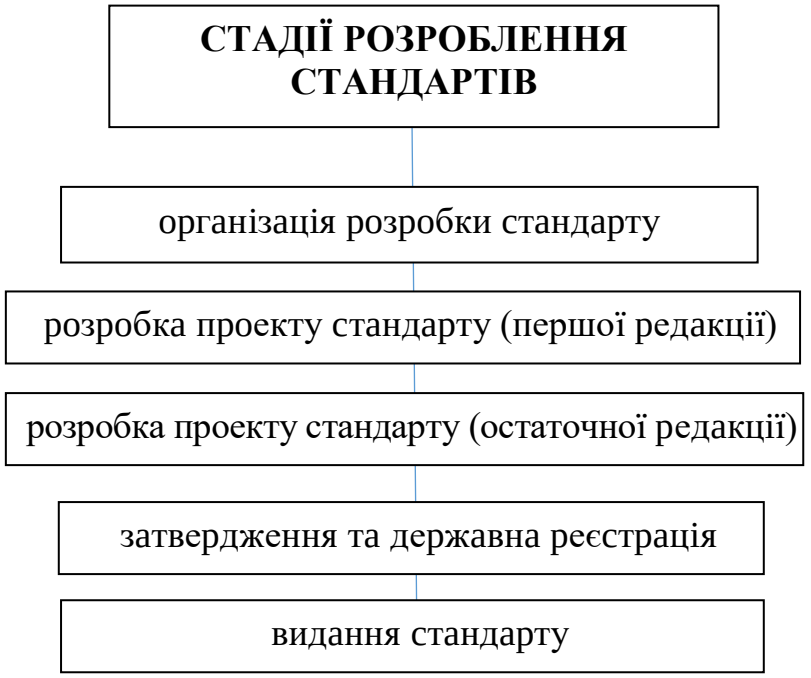

Рис.1.4 Стадії розроблення державних стандартів України

При організації розробки стандарту ТК, міністерства (відомства) чи за їх дорученням головні (базові) організації зі стандартизації розглядають обґрунтовані заявки на розробку стандарту та вносять пропозиції до плану державної стандартизації в ДП «УкрНДНЦ».

Перед розробкою першої редакції стандарту ТК міністерства (відомства) чи за їх дорученням головні (базові) організації по стандартизації укладають договір на розробку стандарту, а також технічне завдання щодо цієї процедури, до якого додають перелік організацій, котрим необхідно розіслати проект стандарту для отримання відзиву, та перелік організацій, з котрими необхідно погодити проект стандарту.

До переліку організацій, з якими необхідно погодити проект стандарту, внесено:

- замовника (якщо ним не є ДП «УкрНДНЦ»), чи основного споживача стандарту;
- ТК, який працює за напрямком стандарту, що розробляється (за відсутності такого ТК - головну (базову) організацію зі стандартизації міністерства чи відомства);
- науково -дослідну організацію ДП «УкрНДНЦ»;
- органи державного нагляду.

Після узгодження з ДП «УкрНДНЦ» технічне завдання на розробку стандарту затверджує голова ТК або керівник організації-розробника.

Відповідно до договору та технічного завдання ТК та інші уповноважені організації готують першу редакцію проекту стандарту, після чого її розсилають на відзив організаціям відповідно до переліку.

На наступній стадії ТК чи організація-розробник обробляє отримані відзиви та складає зведення. На основі зауважень та пропозицій, що містяться у зведенні, проект стандарту дороблюється та уточняється пояснювальна записка до нього. Дороблена редакція проекту стандарту разом з пояснювальною запискою відсилається організаціям для погодження в термін, не перевищуючий одного місяця з моменту одержання стандарту. Після погодження ТК відповідне міністерство (відомство) чи організація-розробник представляє на затвердження в ДП «УкрНДНЦ» остаточну редакцію проекту стандарту. Разом з проектом стандарту повинна бути представлена така документація:

- пояснювальна записка щодо остаточної редакції проекту стандарту;
- копія технічного завдання на розробку стандарту;
- зведення відзивів;
- оригінали документів, підтверджуючих узгодження проекту стандарту;
- протокол засідання ТК або науково-технічної ради організації-розробника.

ДП «УкрНДНЦ» організовує державну експертизу проекту стандарту, до якої можуть бути залучені науково-дослідні організації ДП «УкрНДНЦ», ТК, відомі вчені та спеціалісти визначеної галузі. Після проведення експертизи ДП

«УкрНДНЦ» розглядає проект стандарту та приймає рішення про його затвердження чи повернення проекту на доопрацювання. У випадку затвердження проекту стандарту видається наказ ДП «УкрНДНЦ».

Як правило, державні стандарти затверджують без обмеження терміну їх дії. Під час схвалення чи прийняття національного стандарту центральний орган виконавчої влади в сфері стандартизації визначає дату надання стандарту чинності з урахуванням часу на виконання підготовчих мір для його впровадження. Після затвердження стандарту ДП «УкрНДНЦ» проводить його реєстрацію. Перелік національних стандартів, схвалених і прийнятих протягом місяця, публікується в наступному місяці в офіційному виданні центрального органу виконавчої влади в сфері стандартизації.

Стандарт вважається впровадженим, якщо визначені в ньому вимоги дотримуються в організаціях, підприємствах встановленої галузі. Перевірку чинних національних стандартів на відповідність законодавству, інтересам держави, потребам споживачів, рівню розвитку науки і техніки, вимогам міжнародних і регіональних стандартів здійснюють відповідні технічні комітети чи інші уповноважені суб'єкти стандартизації. Стандарти на продукцію перевіряються не рідше одного разу на п'ять років. За результатами перевірки відповідні технічні комітети чи інші суб'єкти стандартизації дають пропозиції про перегляд, зміни чи скасування стандартів до центрального органу виконавчої влади у сфері стандартизації. Перегляд, в результаті якого розробляється новий національний стандарт чи вносяться зміни в діючий стандарт, здійснюється у порядку, установленому для розробки стандартів.

Припинення дії національного стандарту здійснює центральний орган виконавчої влади в сфері стандартизації у випадку припинення випуску продукції, регламентованої цим стандартом, а також у випадку розроблення, схвалення чи прийняття замість нього іншого стандарту за поданням відповідного технічного комітету стандартизації чи іншого суб'єкта стандартизації. Інформація про зміни, текст змін національних стандартів публікується в офіційному виданні

центрального органу виконавчої влади у сфері стандартизації не пізніше, чим за 90 днів до терміну надання їм чинності.

Міжнародні (регіональні) стандарти впроваджуються як національні стандарти за умови їх прийняття центральним органом виконавчої влади в сфері стандартизації. Прийняття міжнародного (регіонального) стандарту - це опублікування національного стандарту, що ґрунтується на відповідному міжнародному (регіональному) стандарті, чи підтвердження того, що міжнародний (регіональний) стандарт має той же самий статус, що і національний стандарт, із зазначенням будь-яких відхилень від міжнародного (регіонального) стандарту.

Стандарти застосовуються на добровільних засадах, якщо інше не встановлено законодавством. Також стандарти застосовуються безпосередньо чи шляхом посилання на них в інших документах.

Застосування стандартів чи їх окремих положень є обов'язковим:

- для всіх суб'єктів господарювання, якщо це передбачено в технічних регламентах чи інших нормативно-правових актах;
- для учасників угоди (контракту) про розроблення, виготовлення чи постачання продукції, якщо в ній (ньому) є посилання на певні стандарти;
- для виробника чи постачальника продукції, якщо він склав декларацію про відповідність продукції певним стандартам чи застосував позначення цих стандартів у її маркуванні;
- для виробника чи постачальника, якщо його продукція сертифікована щодо дотримання вимог стандартів.

Міжнародні (регіональні) стандарти і стандарти інших країн, якщо їхні вимоги не суперечать законодавству України, можуть бути застосовані в Україні в установленому порядку шляхом посилання на них у національних та інших стандартах. Стандарти, застосовані під час виготовлення продукції, повинні зберігатися у виробника протягом 10 років після випуску останнього виробу даного виду продукції.

Висновки до першого розділу

Встановлено, що загальні положення та основні поняття в сфері стандартизації встановлено у Законі України «Про стандартизацію» та інших дотичних нормативно-правових актах. Відповідно до законодавства головними суб'єктами в сфері стандартизації в Україїн є: центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації (Міністерство економічного розвитку і торгівлі України); центральний орган виконавчої влади, що реалізує державну політику у сфері стандартизації (Департамент технічного регулювання, що є самостійним структурним підрозділом центрального апарату Мінекономрозвитку); національний орган стандартизації (ДП «УкрНДНЦ»); технічні комітети стандартизації; підприємства, установи та організації, що здійснюють стандартизацію.

У результаті вивчення процедури розробки стандартів в Україні встановлено такі п’ять головних її етапів: організація розробки стандартів; розробка проекту стандартів (першої редакції); організація розробки стандартів (остаточна редакція); затвердження та державна реєстрація стандарту; видання стандарту. Також потрібно відзначити, що стандарти застосовуються на добровільних засадах, якщо інше не установлено законодавством.

РОЗДІЛ 2.
МІЖНАРОДНІ СТАНДАРТИ ISO З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Огляд сімейства міжнародних стандартів ISO/IEC 27к

ISO (Міжнародна організація зі стандартизації) і IEC (Міжнародна електротехнічна комісія) формують спеціалізовану систему всесвітньої стандартизації. Державні органи, які є членами ISO або IEC, беруть участь в розробці міжнародних стандартів через технічні комітети, створені відповідної організацією для стандартизації окремих областей технічної діяльності. Технічні комітети ISO і IEC співпрацюють в областях взаємних інтересів.

Сімейство міжнародних стандартів на системи управління інформаційною безпекою 27к, що розробляється ISO/IEC JTC 1/SC 27, включає міжнародні стандарти, що визначають вимоги до систем управління інформаційною безпекою, управління ризиками, метрики і вимірювання, а також керівництво по впровадженню.

Для цього сімейства стандартів використовується послідовна схема нумерації, починаючи з 27000 і далі. Сімейство ISO/IEC 27к включає понад 50 стандартів, хотілося б окремо виділити 9 з них, які безпосередньо стосуються управління інформаційною безпекою, зокрема:

ISO/IEC 27000:2018 Інформаційні технології. Методи безпеки. Система управління інформаційною безпекою. Огляд і словник [7].

ISO/IEC 27001:2013 Інформаційні технології. Методи безпеки. Система управління інформаційною безпекою. Вимоги [8]. Даний стандарт визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою в контексті організації. Вона також включає вимоги щодо оцінки та поводження з ризиками інформаційної безпеки, пристосованих до потреб організації. Вимоги, викладені в ISO / IEC 27001:2013, є

загальними і призначені для застосування до всіх організацій, незалежно від типу, розміру або характеру.

ISO/IEC 27006:2015 Інформаційна безпека. Методи безпеки. Рекомендації органам аудиту й сертифікації СУІБ [9]. ISO / IEC 27006:2015 визначає вимоги та надає вказівки для органів, що здійснюють аудит та сертифікацію системи управління інформаційною безпекою, на додаток до вимог, що містяться в ISO / IEC 17021-1 та ISO / IEC 27001. Цей стандарт допомагає підтримати акредитацію органів сертифікації СУІБ.

Вимоги, що містяться в зазначеному документі, повинні бути продемонстровані з точки зору компетентності та надійності будь-яким органом, що надає сертифікацію СУІБ, а керівництво, що міститься в цьому міжнародному стандарті, надає додаткову інтерпретацію цих вимог для будь-якого органу, що надає сертифікацію СУІБ. Цей міжнародний стандарт може використовуватися як критерій документа для акредитації, експертної оцінки або інших процесів аудиту.

ISO/IEC 27002:2013 Інформаційні технології. Методи безпеки. Кодекс правил для управління інформаційною безпекою [10] - надає керівні принципи для організаційних стандартів інформаційної безпеки та методів управління інформаційною безпекою, включаючи вибір, впровадження та управління засобами контролю з урахуванням середовища (ризиків) інформаційної безпеки організації. Стандарт призначений для використання організаціями, які мають намір: вибирати засоби в процесі впровадження системи управління інформаційною безпекою на основі ISO/IEC 27001; впроваджувати загальноприйняті засоби контролю інформаційної безпеки; розробити власні керівні принципи управління інформаційною безпекою.

ISO/IEC 27003:2017 Інформаційні технології. Методи безпеки. Керівництво з впровадження СУІБ [11]. ISO/IEC 27003:2017 надає пояснення та рекомендації щодо ISO/IEC 27001:2013.

ISO/IEC 27004:2016 Інформаційні технології. Методи безпеки. Управління інформаційною безпекою. Вимірювання, моніторинг, аналіз та оцінка [12]. ISO/IEC 27004:2016 надає керівні принципи, призначені для надання допомоги організаціям у оцінці продуктивності інформаційної безпеки та ефективності системи управління інформаційною безпекою з метою виконання вимог ISO/IEC 27001:2013. Вона встановлює засади: моніторингу та вимірювання результатів інформаційної безпеки; моніторингу та вимірювання ефективності системи управління інформаційною безпекою (СУІБ), включаючи її процеси та контроль; аналізу й оцінки результатів моніторингу та вимірювання.

ISO/IEC 27004:2016 застосовується до всіх типів і розмірів організацій.

ISO/IEC 27005:2018 Інформаційні технології. Методи безпеки. Управління ризиками інформаційної безпеки [13]. Цей документ містить рекомендації щодо управління ризиками інформаційної безпеки. Стандарт підтримує загальні поняття, зазначені в ISO/IEC 27001 і призначений для сприяння задовільному впровадженню інформаційної безпеки на основі підходу до управління ризиками.

Для повного розуміння цього документа важливе знання понять, моделей, процесів і термінології, описаних у ISO/IEC 27001 і ISO/IEC 27002. Стандарт застосовується до всіх типів організацій (наприклад, комерційних підприємств, державних установ, неприбуткових організацій), які мають намір управляти ризиками та, які можуть поставити під загрозу інформаційну безпеку організації.

ISO/IEC 27007:2017 Інформаційні технології. Методи безпеки. Керівні принципи з аудиту УІБ [14]. ISO/IEC 27007 надає вказівки щодо управління програмою аудиту системи управління інформаційною безпекою, проведення аудитів та компетенції аудиторів СУІБ, на додаток до рекомендацій, що містяться в ISO 19011:2011. Зазначений стандарт застосовується до тих, хто потребує розуміння або проведення внутрішнього або зовнішнього аудиту СУІБ або для управління програмою аудиту СУІБ.

ISO/IEC 27011:2016 Інформаційні технології. Настанови з управління інформаційною безпекою для телекомунікаційних компаній, що базуються на

ISO/IEC 27002 [15]. Сфера застосування цієї рекомендації ISO/IEC 27011:2016 визначає керівні принципи, що підтримують впровадження засобів контролю інформаційної безпеки в телекомунікаційних організаціях. Прийняття стандарту ISO/IEC 27011:2016 дозволить телекомунікаційним організаціям відповідати вимогам управління інформаційною безпекою базової лінії щодо конфіденційності, цілісності, доступності та будь-якого іншого відповідного об'єкта безпеки.

У контексті багатьох порушень інформаційної безпеки організацій, що забезпечували протидію пандемії COVID, варто окрему увагу звернути на стандарт ISO/IEC 27799:2016 Інформатика в охороні здоров’я. Управління інформаційною безпекою у сфері охорони здоров’я з використанням ISO/IEC 27002 [16]. ISO 27799:2016 надає керівні принципи для організаційних стандартів інформаційної безпеки та методів управління інформаційною безпекою, включаючи вибір, впровадження та управління засобами контролю з урахуванням середовища (ризиків) інформаційної безпеки організації. Він визначає керівні принципи для підтримки інтерпретації та впровадження в інформатиці охорони здоров'я ISO/IEC 27002 і є супутником цього міжнародного стандарту.

ISO 27799:2016 надає керівництво з впровадження елементів управління, описаних у ISO/IEC 27002, і доповнює їх там, де це необхідно, щоб вони могли ефективно використовуватися для управління інформацією про здоров'я. Впроваджуючи ISO 27799:2016, організації охорони здоров'я та інші охоронці медичної інформації зможуть забезпечити мінімальний необхідний рівень безпеки, який відповідає обставинам їхньої організації, а також підтримуватиме конфіденційність, цілісність та доступність особистої медичної інформації під їх догляд.

Зазначений стандарт застосовується до медичної інформації у всіх її аспектах, незалежно від форми інформації (слів і цифр, звукових записів, малюнків, відео та медичних зображень), незалежно від того, які засоби використовуються для її зберігання (друк або запис на папері або електронному

зберіганні), і будь-які засоби, що використовуються для його передачі (від руки, через факс, через комп'ютерні мережі або поштою), оскільки інформація завжди належним чином захищена.

ISO 27799:2016 та ISO/IEC 27002 разом визначають, що потрібно з точки зору інформаційної безпеки у сфері охорони здоров'я, вони не визначають, яким чином ці вимоги повинні задовольнятися. Тобто, у максимально можливій мірі, ISO 27799: 2016 є технологічно нейтральним. Нейтральність щодо впровадження технологій є важливою особливістю. Технології безпеки все ще переживають швидкий розвиток, і темпи цих змін зараз вимірюються місяцями, а не роками. На відміну від цього, під час періодичного перегляду очікується, що міжнародні стандарти загалом залишаться чинними протягом багатьох років. Так само важливо, що технологічний нейтралітет залишає постачальників товарів і послуг вільними для того, щоб запропонувати нові або розвиваючі технології, які відповідають необхідним вимогам, описаним ISO 27799:2016.

2.2 ISO/IEC 27001 як основа сертифікації з управління інформаційною безпекою

ISO/IEC 27001 - це міжнародний стандарт, розроблений Міжнародною організацією зі стандартизації, який описує, як керувати інформаційною безпекою в організації. Остання публікація була випущена в 2013 році, і його повна назва на сьогоднішній день - «ISO/IEC 27001:2013». Перша версія стандарту, опублікована в 2005 році, створена на основі Британського стандарту BS 7799-2.

ISO/IEC 27001 може бути впроваджений в будь-якій організації: комерційній або некомерційній, приватній або державній, маленькій або великій. Він був написаний провідними світовими експертами в області інформаційної безпеки і пропонує методологію для ведення інформаційної безпеки підприємства. Крім того, компанія може отримати сертифікацію, це означає, що незалежний орган з

сертифікації підтверджує, що організація впровадила ІБ в відповідності з стандартом ISO 27001.

ISO/IEC 27001 став найпопулярнішим у світі стандартом інформаційної безпеки, і багато компаній були сертифіковані у відповідності з ним.

Стандарт ISO/IEC 27001 сфокусований на захисті конфіденційності, цілісності та доступності інформації в організації. Це реалізовується шляхом виявлення потенційних проблем з інформацією (тобто оцінкою ризику), а потім визначення необхідних кроків для запобігання появі таких проблем (тобто зниження або обробки ризиків). Тому основна філософія ISO/IEC 27001 базується на управлінні ризиками: виявляти, визначати, де виникають ризики, а потім систематично обробляти їх.

Також відповідно цього стандарту, СУІБ - це системний підхід до управління чутливою інформацією в організації, щоб вона залишалася завжди в безпеці. СУІБ включає людей, процеси та IT-системи, застосовуючи процес управління ризиками.

Захисні заходи (або контролі), які повинні бути впроваджені, зазвичай виступають у формі політики, процедури та технічного забезпечення (наприклад, програмного забезпечення та обладнання). Однак, в більшості випадків, організація вже має все необхідне обладнання і програмне забезпечення, однак не використовує їх належним чином, тому велика частина впроваджень ISO/IEC 27001 буде пов'язана з організаційними правилами, закріпленими у документах, які необхідні для запобігання порушень в системі безпеки. В цілому таке впровадження потребує управління політикою, процедурою, людьми, активами і т.д. У стандарті описано, як правильно з’єднати всі ці елементи в системі менеджменту інформаційної безпеки.

Тому управління інформаційною безпекою - це не тільки IT-безпека (тобто фаєрволи, антивірус і т.д.). Це також управління процесами, правовим захистом, управління персоналом, фізичним захистом тощо.

При впровадженні стандарту ISO/IEC 27001організації отримують такі основні переваги в бізнесі:

*Відповідність правовим вимог*ам – з’являється все більше законів, нормативних актів і договірних вимог, що пов’язані з інформаційною безпекою. І за рахунок впровадження стандарту ISO/IEC 27001 можуть бути вирішені основні проблеми у цій сфері, оскільки цей стандарт надає організації ідеальну методології підтримання всіх документів.

Досягнення ринкової переваги –організація, яка пройшла сертифікацію на основі зазначеного стандарту, отримує переваги над конкурентами в очах своїх клієнтів, які велику уваги приділяють захисту інформації.

Зниження витрат – основна філософія даного стандарту спрямована на передбачення появи інцидентів, що пов’язані з порушенням безпеки, тому що будь-який інцидент, великий чи малий, коштує грошей. І найголовніше, інвестиція в ISO/IEC 27001 є набагато економніша, ніж вкладення коштів у реагування на інциденти.

Покращення організаційного процесу – у типових організацій, що швидко розвиваються, немає часу призупинитись і визначити свої процеси і процедури. Як наслідок, співробітники часто не знають, хто, що і коли має робити. Впровадження ISO/IEC 27001 допомагає вирішити такі ситуації, тому що це сприяє регламентуванню і документальнеому оформленню організаціями своїх основних процесів (навіть тих, які не пов’язані з безпекою) і дозволяє скоротити втрату часу персоналу.

Загалом, керівництво організації має розуміти, що інформаційна безпека є частиною управління загальними організаційними ризиками з галузями, які перетинаються з кібербезпекою, управлінням безперервної діяльності та IT-управлінням.

ISO/IEC 27001 розбитий на 11 розділів і Додаток А. Розділи з 0 по 3 є вступними (і не обов'язкові для впровадження), а розділи з 4 по 10 є обов'язковими, тобто всі їхні вимоги мають бути впроваджені в організації, якщо

вона хоче відповідати стандарту. Контролі з програми А мають бути впроваджені, тільки якщо вони заявлені як застосовні в Заяві про можливість застосування.

Згідно з додатком SL Директиви ISO/IEC Міжнародної організації зі стандартизації назви розділів в стандарті ISO/IEC 27001 аналогічні назвам розділів стандарту ISO 22301:2012, нового стандарту ISO 9001:2015 та інших стандартів управління, що дозволяє спростити інтеграцію цих стандартів.

Розділ 0: Вступ - пояснює мету стандарту ISO/IEC 27001 і його сумісність з іншими стандартами управління.

Розділ 1: Область застосування - пояснює, що цей стандарт застосовний в організації будь-якого типу.

Розділ 2: Нормативні посилання - відносяться до ISO/IEC 27000 як до стандарту, в якому дано терміни та визначення.

Розділ 3: Терміни та визначення - знову ж відносяться до ISO/IEC 27000.

Розділ 4: Особливості організації. Цей розділ є частиною фази планування в циклі «Планування, реалізація, контроль, коригування» та визначає вимоги для розуміння зовнішніх і внутрішніх проблем, зацікавлених сторін та їх вимог, а також для визначення області застосування системи менеджменту інформаційної безпеки.

Розділ 5: Відповідальність керівництва. Цей розділ є частиною фази планування в циклі «Планування, реалізація, контроль, коригування» та визначає обов'язки топ-менеджменту, ролі та обов'язки персоналу, а також зміст політики інформаційної безпеки верхнього рівня.

Розділ 6: Планування. Цей розділ є частиною фази планування в циклі «Планування, реалізація, контроль, коригування» та визначає вимоги для оцінки й обробки ризиків, заяви про можливість застосування, плану по обробці ризиків і постановки завдань для інформаційної безпеки.

Розділ 7: Підтримка. Цей розділ є частиною фази планування в циклі «Планування, реалізація, контроль, коригування» та визначає вимоги до

доступності ресурсів, компетенцій, інформованості, комунікації та контролю документації та записів.

Розділ 8: Функціонування. Цей розділ є частиною фази реалізації в циклі «Планування, реалізація, контроль, коригування» та визначає впровадження оцінки і обробки ризиків, а також контрзаходів та інших процесів, необхідних для досягнення цілей інформаційної безпеки.

Розділ 9: Оцінка ефективності. Цей розділ є частиною фази перевірки в циклі «Планування, реалізація, контроль, коригування» та визначає вимоги до моніторингу, вимірюванню, аналізу, оцінки, внутрішнього аудиту й аналізу управління.

Розділ 10: Удосконалення. Цей розділ є частиною фази коригування в циклі «Планування, реалізація, контроль, коригування» й визначає вимоги до невідповідностей, виправлень, коригувальних дій і безперервного вдосконалення.

Додаток А. Ця програма містить каталог з 114 контролів (захисних заходів), розміщених в 14 розділах (розділи з А.5 по А.18).

Щоб впровадити ISO/IEC 27001 в організації, необхідно виконати такі 16 кроків: отримати підтримку топ-менеджменту; використовувати методологію управління проектом; визначити сферу застосування системи управління інформаційної безпеки; написати політику інформаційної безпеки верхнього рівня; визначити методологію оцінки ризиків; здійснити оцінку і обробку ризиків; написати Заяву про застосування; написати план обробки ризиків; визначити, як виміряти ефективність контрзаходів і системи менеджменту інформаційної безпеки; впровадити всі відповідні контролі та процедури; впровадити програми навчання та інформування; здійснювати всю щоденну діяльність, прописану в організаційній документації системи менеджменту інформаційної безпеки; контролювати і оцінювати організаційну систему менеджменту інформаційної безпеки; здійснити внутрішній аудит; здійснити аналіз управління; впровадити коригувальні дії.

Як згадувалося раніше, ISO/IEC 27001 був вперше опублікований у 2005 році, а його нова версія з'явилася в 2013 році, тому поточна дійсна версія – це стандарт ISO/IEC 27001:2013. Найважливіші зміни в версії 2013 відносяться до структури основної частини стандарту, визначення зацікавлених сторін, цілей, засад моніторингу та вимірювання. Крім того, в додатку А було скорочено кількість контрзаходів з 133 до 114 і збільшено кількість розділів з 11 до 14. Деякі вимоги були видалені з версії 2013, наприклад: запобіжні дії і вимоги до документів певних процедур.

Однак, всі ці зміни практично не змінили стандарт загалом. Його основна філософія як і раніше заснована на оцінці та обробці ризиків, а фаза циклу «Планування, реалізація, контроль, коригування» містить аналогічні заходи. Цю нову версію стандарту простіше читати і розуміти, і її набагато легше інтегрувати з іншими стандартами управління, такими як ISO 9001, ISO 22301 та іншими.

2.3 Основні положення стандарту ISO/IEC 27000:2018

2018 рік був дуже важливим для сфери інформаційної безпеки, оскільки була прийнята оновлена версія міжнародного стандарту ISO/IEC 27000 «Інформаційні технології. Методи безпеки. Система управління інформаційною безпекою. Огляд і словник». Вихід даного стандарту був викликаний дослідженням питань безпеки мікропроцесорів, а також впровадженням великих ініціатив кібербезпеки, таких як правила захисту даних ЄС, тому за висновком експертів ISO/IEC 27000 був розроблений в потрібний час.

ISO/IEC 27000:2018 містить огляд системи управління інформаційною безпекою (СУІБ), а також термінів і визначень, що використовуються в серії стандартів ISO/IEC 27k. Нова версія, розроблена для застосування в організації всіх типів і розмірів, від багатьох національних підприємств, випущена в лютому 2018 року.

ISO/IEC 27000:2018 містить інформацію про те, який взаємозв’язок існує між стандартами: область діяльності, роль, функції і відносини один з одним.

Вдосконалений стандарт забезпечує додаткові переваги, оскільки він об'єднав важливу термінологію, що використовують інші стандарти в серії ISO/IEC 27k. ISO/IEC 27000:2018 був розроблений об'єднаним технічним комітетом ISO/IEC JTC 1 «Інформаційні технології», підкомітетом ПК 27 «Методи забезпечення інформаційної безпеки», секретаріат якого належить Німецькому інституту зі стандартизації DIN, члену ISO від Німеччини. Даний стандарт можуть отримати організації, що є національним членом ISO або придбати в інтернет-магазині ISO.

Цей стандарт застосовується до всіх типів і розмірів організації (наприклад, комерційні підприємства, державні установи, неприбуткові організації).

Терміни та визначення, наведені в цьому документі:

- охоплюють загально визначені терміни та визначення стандартів СУІБ;
- не охоплюють усі терміни та визначення, що застосовуються в межах сімейства стандартів СУІБ;
- не обмежують сімейство СУІБ стандартів при визначенні нових термінів, що використовуються.

Варто відзначити, що у порівнянні з попередньою версією стандарту ISO/IEC 27000:2018 основні зміни були внесені у наступні його частини:

- Передмова і вступ;

- Нормативні посилання (додано);

- Терміни та визначення (вилучено терміни: аналітична модель, дані, критерій прийняття рішень, виконавчий менеджмент, проект СУІБ, результати вимірювання, об’єкт, шкала, зацікавлена сторона, одиниця виміру, валідація, верифікація);

- Сімейство стандартів СУІБ (оновлено);

- Додатки А і В (вилучено).

Також у новій версії стандарту пояснюється значення вербальних форм, що використовуються у тексті документа:

- «необхідно» означає вимогу;
- «повинен» вказує на рекомендацію;
- «має» означає дозвіл;
- «може» означає можливість.

За даним стандартом СУІБ складається з політик, процедур, керівних принципів та пов'язаних з ними ресурсів і заходів, які колективно керуються організацією, для забезпечення захисту своїх інформаційних активів.

СУІБ - це системний підхід до створення, впровадження, експлуатації, моніторингу, перегляду, підтримки, поліпшення інформаційної безпеки організації для досягнення бізнес-цілей. Вона ґрунтується на оцінці ризику та рівнях прийняття ризику організації, призначених для ефективного лікування та управління ризиками. Аналіз вимог щодо захисту інформаційних активів та застосування відповідного контролю для забезпечення захисту цих інформаційних активів, у разі потреби, сприяє успішному впровадженню СУІБ.

Наступні основні принципи також сприяють успішному впровадженню СУІБ:

- усвідомлення необхідності інформаційної безпеки;
- розподіл відповідальності за інформаційну безпеку;
- включення зобов'язань керівництва та інтересів зацікавлених сторін;
- підвищення суспільних цінностей;
- оцінки ризиків, що визначають відповідний контроль для досягнення прийнятного рівня ризику;
- безпека, включена як істотний елемент інформаційних мереж і систем;
- активне запобігання та виявлення інцидентів інформаційної безпеки;
- комплексний підхід до управління інформаційною безпекою;
- постійну переоцінку інформаційної безпеки та внесення відповідних змін.

ISO/IEC27000:2018 дає більш чітке розуміння, для чого організації СУІБ. А саме в стандарті сказано, що переваги впровадження СУІБ в основному є

результатом зниження ризиків інформаційної безпеки (тобто зменшення ймовірності та/або впливу інцидентів інформаційної безпеки). Зокрема, переваги, які реалізуються організацією для досягнення стійкого успіху від прийняття стандартів СУІБ, включають наступне:

1. структуру, що підтримує процес визначення, впровадження, експлуатації та підтримки комплексного, економічно ефективного, ціннісного, інтегрованого та узгодженого СУІБ, що відповідає потребам організації в різних операціях і сайтах;

2. допомогу керівництву у послідовному та відповідальному управлінні своїм підходом до менеджменту інформаційної безпеки в контексті управління ризиками та загальноорганізаційного управління, включаючи навчання та навчання власників бізнесу та систем щодо цілісного управління інформаційною безпекою;

3. пропагування прийнятих у всьому світі, кращих методів інформаційної безпеки в неприписаній манері, надаючи організаціям широту для прийняття та вдосконалення відповідних контролів, що відповідають їхнім конкретним умовам, і підтримувати їх перед внутрішніми та зовнішніми змінами;

4. забезпечення спільної мови та концептуальної основи інформаційної безпеки, що полегшує довіру до ділових партнерів у відповідних СУІБ, особливо якщо вони вимагають сертифікації відповідно до ISO/IEC 27001 акредитованим органом з сертифікації;

5. збільшення довіри зацікавлених сторін до організації;

6. задоволення суспільних потреб та очікувань;

7. ефективніше економічне управління інвестиціями в інформаційну безпеку.

Висновки до другого розділу

Досліджено сімейство міжнародних стандартів на системи управління інформаційною безпекою ISO/IEC 27к, що розробляється Технічним комітетом

ISO/IEC JTC 1/SC 27 і включає понад 50 стандартів, 9 з яких стосуються власне управління інформаційною безпекою.

Аналізуючи сімейство стандартів ISO/IEC 27к, варто окремо виділити стандарт ISO 27001, який фактично є найпопулярнішим у світі стандартів з управління інформаційною безпекою, і багато компаній були сертифіковані у відповідності до його вимог. Стандарт ISO/IEC 27001 сфокусований на захисті конфіденційності, цілісності та доступності інформації в організації. Це реалізовується шляхом виявлення потенційних проблем з інформацією (тобто оцінки ризиків), а потім визначення необхідних кроків для запобігання появі таких проблем (тобто зниження або обробки ризиків).

Останнім оновленим стандартом сімейства ISO/IEC 27к є ISO/IEC 27000:2018. Вдосконалений стандарт забезпечує додаткові переваги, оскільки він об'єднав важливу термінологію, що використовують інші стандарти в серії ISO/IEC 27к, а також описує взаємозв’язки між стандартами з управління інформаційною безпекою: сфери діяльності, роль, функції і зв'язки один з одним.

РОЗДІЛ 3.
СТАНДАРТИЗОВАНІ ВИМОГИ ДО УПРАВЛІННЯ БЕЗПЕКОЮ ІТ ІНШИХ ЕКСПЕРТНИХ ОРГАНІЗАЦІЙ

3.1 Підхід до управління інформаційною безпекою COBIT

COBIT - це структура управління IT, розроблена Асоціацією аудиту і контролю інформаційних систем (ISACA), щоб допомогти підприємствам розробляти, організовувати та впроваджувати стратегії управління інформацією і корпоративного управління.

COBIT (Control Objectives for Information and Related Technologies), вперше випущений в 1996 році, спочатку був розроблений як набір цілей управління IT, щоб допомогти спільноті фінансового аудиту краще орієнтуватися в розвитку IT-середовищ. У 1998 році ISACA випустила версію 2, яка розширила структуру для застосування поза аудиторської спільноти. Пізніше, в 2000-х, ISACA розробила версію 3, в якій були впроваджені методи управління IT та інформацією, що використовуються сьогодні в структурі.

COBIT 4 був випущений в 2005 році, далі розробили COBIT 4.1 в 2007 році. Ці оновлення включали додаткову інформацію про управління, пов'язаному з інформаційними та комунікаційними технологіями. У 2012 році був випущений COBIT 5, а в 2013 році ISACA випустила додаток до COBIT 5, який включав додаткову інформацію для підприємств, що стосується управління ризиками та управління інформацією.

ISACA анонсувала оновлену версію COBIT в 2018 році, відмовившись від номера версії і назвавши її COBIT 2019. Ця оновлена версія COBIT призначена для постійного розвитку з «більш частими і плавними оновленнями», згідно ISACA. COBIT 2019 був введений для створення більш гнучких, спільних стратегій управління, які враховують нові і мінливі технології.

COBIT 2019 оновлює рамки для сучасних підприємств, звертаючи увагу на нові тенденції, технології і потреби в безпеці. Ця структура, як і раніше добре поєднується з іншими структурами управління IT, такими як ITIL, CMMI і TOGAF, що робить її відмінним варіантом в якості зонтичної структури для уніфікації процесів у всій організації.

Нові концепції і термінологія були введені в Базову модель COBIT, яка включає 40 цілей керівництва і управління для створення програми управління. Система управління продуктивністю тепер забезпечує більшу гнучкість при використанні вимірів зрілості і можливостей. В цілому, структура призначена для надання підприємствам більшої гнучкості при налаштуванні стратегії управління IT.

Як і інші структури управління IT, COBIT допомагає узгодити бізнес-цілі з IT-цілями, встановлюючи зв'язки між ними і створюючи процес, який може допомогти подолати розрив між IT - або ізольованими IT - відділами - і зовнішніми відділами.

Одна з основних особливостей COBIT полягає в тому, що він орієнтований саме на безпеку, управління ризиками та управління інформацією. На цьому наголошується в COBIT 2019 з більш чітким визначенням того, що таке COBIT, а що ні. Наприклад, ISACA стверджує, що COBIT 2019 не є основою для організації бізнес-процесів, управління технологіями, прийняття рішень, пов'язаних з IT, або визначення IT-стратегії або архітектури. Швидше, він розроблений строго як структура для керівництва та управління корпоративними IT в рамках всієї організації. В оновленій версії це краще пояснюється для підприємств, тому менше плутанини в тому, як слід використовувати і впроваджувати COBIT.

Задачами оновленого COBIT 2019 є:

- Зосередження уваги на сферах та факторах проектування, які дають більше ясності при створенні системи управління для потреб бізнесу.
- Гармонізація зі світовими стандартами, структурами і передовими методами для підвищення актуальності структури.

- Створення моделі, яка дозволяє отримувати зворотний зв'язок від глобального співтовариства управління для заохочення більш швидких оновлень і поліпшень.
- Регулярні оновлення, що випускаються на постійній основі.
- Створення додаткових рекомендацій та інструментів для підтримки підприємств при розробці «найбільш підходящої системи управління, що робить COBIT 2019 більш розпорядчим».
- Узгодження з CMMI (Інтегрована модель зрілості можливостей), яка також є розробкою ISACA.
- Виявлення додаткової підтримки для прийняття рішень, включаючи нові функції спільної роботи в Інтернеті.

COBIT 2019 також вводить концепції «пріоритетної галузі», які описують конкретні теми і проблеми корпоративного управління, які можуть бути вирішені за допомогою менеджменту, побудованого на досягненні конкретних цілей. Деякі приклади цих пріоритетних областей включають малі і середні підприємства, кібербезпеку, цифрову трансформацію і хмарні обчислення. Пріоритетні області будуть додаватися і змінюватися в міру необхідності на основі тенденцій, досліджень і відгуків - немає обмежень на кількість цільових областей, які можуть бути включені в COBIT 2019.

У COBIT 2019 показано, що для досягнення цілей керівництва та управління кожною організацією необхідно створювати, адаптувати та підтримувати систему керівництва, що складається з компонентів, а компоненти - це фактори, які індивідуально та колективно сприяють ефективному функціонуванню систем управління.

Тому нижче описано компоненти COBIT 2019:

1. Структура COBIT 2019: Введення і методологія: основне керівництво, яке знайомить з основними принципами COBIT поряд зі структурою загальної концепції.

2. Концепція COBIT 2019: Цілі керівництва та управління: додаткове керівництво, в якому детально розглядається основна модель COBIT і 40 цілей керівництва і управління. Кожна мета описана, включаючи її мету, і те, як вона пов'язана з підприємством і як погоджує цілі.

3. COBIT 2019 Вказівки з проектування: супутнє керівництво, яке пропонує докладні рекомендації з розробки унікальної системи управління для кожної організації.

4. Керівництво по впровадженню COBIT 2019: керівництво, яке допомагає компаніям реалізувати стратегію корпоративного управління після її розробки. Сюди входять кращі практики, способи уникнути пасток і способи інтеграції корпоративної стратегії COBIT 2019 зі стратегією COBIT 5.

Особливу увагу потрібно звернути на принципи та переваги COBIT. Однією із важливих змін в COBIT 2019 є те, що тепер він заохочує зворотний зв'язок від спільноти практиків. Організації можуть придбати Керівництво по дизайну COBIT 2019, також ISACA планувала випустити краудсорсингову версію COBIT на початку 2019 року, в якій фахівці-практики змогли б залишати коментарі, пропонувати поліпшення, нові концепції та ідеї. Проте робота над цією версією продовжується і на сьогоднішній день.

COBIT 2019 покликаний бути більш директивним, щоб направляти компанії в розробці стратегії управління, а також дозволяти організаціям більш комфортно адаптувати унікальну, найбільш підходящу стратегію управління. Згідно асоціації аудиту та контролю інформаційних систем, він визначає «компоненти для побудови і підтримки системи управління: процеси, політики і процедури, організаційні структури, інформаційні потоки, навички, інфраструктуру, культуру і поведінку». Ці компоненти, які раніше називалися в COBIT 5 «інструментами підтримки», краще визначають, що потрібно бізнесу для сильної системи управління.

Також відповідно до бачення ISACA, COBIT 2019 найкраще підходить клієнтам, які використовують кілька структур, таких як ITIL, ISO/IEC 2000 і

CMMI, з певними розрізненими структурами в IT, що використовують свою власну структуру або стандарт. Він також добре підходить для організацій, які повинні слідувати певним нормативним вимогам уряду і місцевої влади.

Структура COBIT 2019 допомагає узгодити існуючі структури в організації і зрозуміти, як кожна структура буде вписуватися в загальну стратегію. Це також може допомогти організації відслідковувати продуктивність цих та інших платформ, особливо з точки зору відповідності вимогам безпеки, інформаційної безпеки та управління ризиками.

Він також призначений для того, щоб вище керівництво краще розуміло, як технології можуть відповідати цілям організації. На думку фахівців ISACA, топ-менеджери можуть безпосередньо зіставити больові точки в бізнесі з певними аспектами структури, наголошуючи на необхідності «керованої контролем IT». Ця структура дає IT-директорам та іншим керівникам IT спосіб продемонструвати рентабельність інвестицій в IT-проект і те, як це допоможе досягти ключових бізнес-цілей.

Рисунок 3.1 Принципи COBIT

Якщо організація вже пройшла сертифікацію по COBIT 5 через ISACA або перебуває в процесі отримання сертифікату, ISACA продовжить підтримувати

акредитацію і проведення навчання та сертифікації COBIT 5 і «продовжить жити разом з навчанням COBIT 2019».

Сертифікати COBIT 2019 включають:

- COBIT Bridge Workshop: одноденний курс, що охоплює концепції, моделі і ключові визначення в COBIT 2019 з упором на відмінності з COBIT 5.
- Іспит COBIT 2019 Foundation: готує учасників до іспиту на сертифікат COBIT 2019 Foundation, який охоплює «контекст, компоненти, переваги та основні причини, за якими COBIT використовується в якості структури управління інформацією і технологіями». Після дводенного курсу фахівці організації зможуть отримати сертифікат в фондах COBIT 2019.
- Іспит з розробки та впровадження COBIT 2019: цю сертифікацію запустили у квітні 2019 року і вона охоплює розробку спеціально підібраної системи управління за допомогою COBIT.

Під час дослідження даного питання вдалося знайти та проаналізувати єдину доступну схему сертифікації COBIT 2019, але ISACA зазначає, що «сімейство продуктів COBIT 2019 і навчання не обмежені».[33] ISACA продовжить оцінку розробки майбутніх навчальних модулів на основі відгуків і потреб ринку.

3.2 Рекомендації в галузі інформаційної безпеки NIST

NIST - National Institute of Standards and Technology - американський національний інститут стандартизації. У його складі функціонує компетентний і авторитетний у США центр з комп'ютерної безпеки - CSRC, який об'єднує фахівців федеральних служб, університетів, найбільших IT-компаній США.

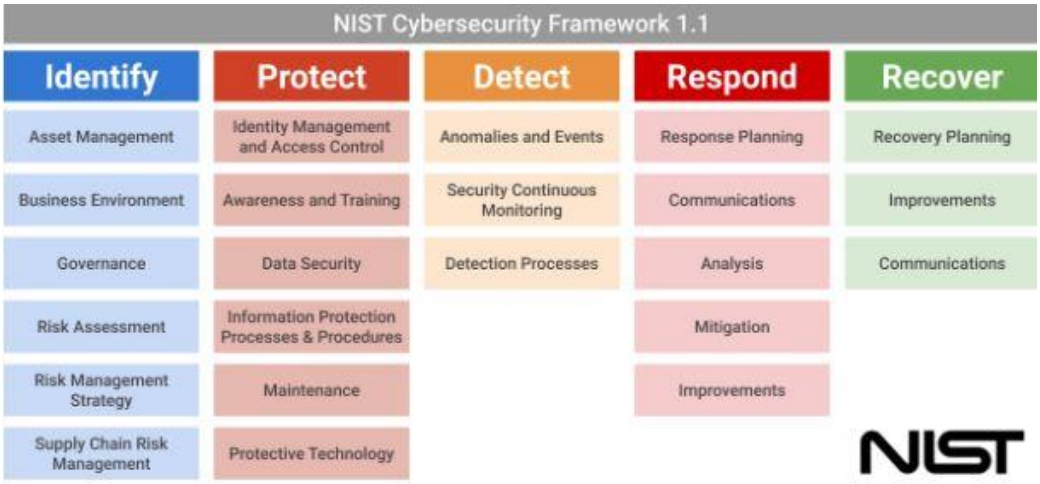

Рисунок 3.2 Завдання NIST в кібербезпеці

Публікації серії Special Publication (SP) 800 NIST надають інформацію, що представляє інтерес для спільноти фахівців з комп'ютерної безпеки. Серія включає керівні принципи, рекомендації, технічні специфікації і річні звіти про діяльність NIST в області кібербезпеки.

Публікації SP 800 розроблені для задоволення і підтримки вимог безпеки і конфіденційності інформації та інформаційних систем федерального уряду США. NIST розробляє публікації серії SP 800 у відповідності зі своїми обов'язками відповідно до Федерального закону про модернізацію інформаційної безпеки (FISMA) від 2014 року.

Ця серія, створена в 1990 році, присвячена дослідженням, керівним принципам і зусиллям Лабораторії інформаційних технологій в області комп'ютерної безпеки, а також її спільних дій з промисловістю, урядом і академічними організаціями.

У CSRC створені три робочі групи, які розподіляють всю діяльність центру з великим напрямками:

- управління інформаційною безпекою;
- технічні питання забезпечення інформаційної безпеки;
- криптографічний захист інформації.

Розділ, присвячений у*правлінню інформаційною безпекою,* містить традиційний для менеджменту у сфері інформаційної безпеки набір рекомендацій,

які рекомендуються для застосування у всіх державних установах США. Багато документів, що стосуються інформаційної безпеки регулярно переглядаються - в дужках вказано рік випуску останньої версії (цим пояснюється недотримання порядку номерів самих документів).

Хотілося б окремо виділити деякі з цих документів. Перший на який потрібно звернути свою увагу це - *SP 800-50 (2003)*. Зазначена публікація пропонує вказівки щодо створення програми підвищення обізнаності і навчання персоналу в області безпеки IT. В документі можна знайти інформацію про те, як розділяти зони відповідальності учасників процесу, шукати потрібні ресурси, знаходити можливі проблеми на етапі впровадження програми, обновляти та вдосконалювати програму.

Наступний документ SP *800-84 (2006)* надає рекомендації щодо засад тестування планів безпеки IT. Також у цьому документі можна знайти відповіді на запитання, як правильно ділити зони відповідальності, приклади документів, приватні методики: «настільний» тест, симуляції, тестування в реальній обстановці.

Документ *SP 800-100 (2006)* дає розширений огляд елементів програми управління інформаційною безпекою для менеджерів, зокрема, як правильно налагодити процес забезпечення ІБ в організації. Також в публікації описано життєвий цикл IT-систем, вимоги до безпечної взаємодії IT-систем. Потрібно звернути увагу на те, що в даному документі також є інформація про навчання і підвищення обізнаності працівників у сфері ІБ, управління ризиками ІБ, оцінювання, сертифікацію, контроль, управління безперервністю й інцидентами.

SP 800-60 (2008) надає вказівки органам влади США щодо підходів до класифікації інформації та інформаційних систем за вимогами до безпеки. В цьому документі розроблена методика присвоєння і класифікатор (рекомендовані значення) рівнів впливу порушення конфіденційності, цілісності і доступності в залежності від виду (призначення) оброблюваної інформації.

Документ *SP 800-115 (2008)* описує технічні питання оцінки рівня ІБ. В документі надаються способи оцінки, самооцінка, внутрішній аудит, зовнішній аудит, тестування на проникнення. Також показана організація процесу та проведення оцінювання, аналіз результатів, використання результатів в процесі вдосконалення ІБ організації.

SP 800-118 (2009) регулює питання управління паролями. В документі розказано про існуючі загрози при використанні парольної аутентифікації та методи забезпечення безпеки зберігання парольної бази, а також протидії атакам соціальної інженерії.

У документі *SP 800-37 (2010)* описано, як управляти ризиками ІБ в федеральних інформаційних системах. В даному документі представлена деталізована методика управління ризиками ІБ, ролі і зони відповідальності учасників процесу, опис супутніх документів.

Завдяки *SP 800-34 (2010)* організації можуть займатися плануванням і забезпеченням безперервності в федеральних інформаційних системах. У публікації показано взаємозв'язок різних рівнів забезпечення безперервності, оцінку впливу різних видів інцидентів на сервіси та вибір стратегій. Також описано, як розробляти і тестувати плани, основні технології забезпечення безперервності функціонування інформаційних систем і сервісів.

Документ *SP 800-137 (2011)* висвітлює питання моніторингу ІБ в федеральних інформаційних системах. У документі описані можливі рівні моніторингу безпеки: організація в цілому / бізнес-процеси / IT-системи, розробка стратегії моніторингу, визначення метрик, аналіз даних, що надходять, використання результатів в процесі вдосконалення ІБ організації.

SP 800-61 (2012) надає вказівки щодо управління інцидентами ІБ, зокрема планування процесу, створення групи реагування і регламентів її функціонування, виявлення інцидентів, пріоритезація, вибір стратегії протидії, зниження шкоди, відновлення систем, забезпечення взаємодії виконавців в процесі реагування на інцидент.

У *SP 800-40 (2012)* описано рекомендації з управління оновленнями безпеки, розгоянуто питання і проблеми процесу управління оновленнями, проаналізовано технології підтримки програмного забезпечення та їх актуальність [35].

3.3 Принципи ефективного управління IT-сервісами ITIL

ITIL (англ. Information Technology Infrastructure Library - Бібліотека інфраструктури інформаційних технологій) є сукупністю книг, які зібрали найкращу світову практику організації чи підрозділу, що надає послуги в IT сфері, кожна з книг висвітлює певний напрям управління у сфері IT. Назва ITIL є зареєстрованою торговою маркою, яка належить британській урядовій організації OGC (англ. Office of Government Commerce).

ITIL підтримує організації і приватних осіб в отриманні оптимальної віддачі від IT і цифрових послуг. Бібліотека допомагає визначити напрям діяльності постачальника послуг за допомогою чіткої моделі можливостей і погоджує їх з бізнес-стратегією і потребами клієнтів.

ITIL є професійно визнаною схемою сертифікації, яка надає вичерпне, практичне і перевірене керівництво по створенню системи управління послугами, пропонує загальний глосарій термінів для підприємств, що використовують IT-послуги.

ITIL використовують мільйони професіоналів по всьому світу, які використовують книги як керівництво по використанню IT в якості інструменту для полегшення змін, трансформації та зростання бізнесу. ITIL виступає за те, щоб IT і цифрові послуги відповідали потребам бізнесу і підтримували його основні цілі та завдання.

Велике дослідження, проведене британською компанією AXELOS за участю різноманітних груп зацікавлених сторін у кількості понад 2 тис., показало, що ITIL має фундаментальне значення для бізнесу, сприяє трансформації і допомагає організаціям усвідомити цінність.

ITIL підтримується схемою сертифікації, яка дозволяє практикам продемонструвати свої здібності в прийнятті та адаптації структури для задоволення своїх конкретних потреб. Щорічно організації вкладають значні кошти в користування та адаптацію ITIL в свою бізнес-практику і підвищення кваліфікації своїх співробітників за допомогою кваліфікацій ITIL.

Структура ITIL складається з п'яти книг, кожна з яких присвячена різним елементам життєвого циклу IT-послуг. Всі вони підтримують один одного, надаючи практичні рекомендації з планування, стимулювання і вдосконалення процесів розробки послуг або товарів.

1. Стратегія обслуговування визначається з огляду на те, якою є мета бізнесу і як планується її досягти. ITIL допоможе об'єднати IT-відділ організації з основними бізнес-процесами, включаючи управління портфелем послуг, фінансове управління і управління взаємовідносинами. Бібліотека допоможе визначити вимоги організації, а також перспективу, необхідну для прогнозування того, як зміни можуть вплинути на організаційні IT-операції.

2. Дизайн послуг - фокусується на дизайні IT-послуг, включаючи архітектури, процеси, політики, документацію і безперервність. Це допоможе організації оцінити свої послуги, щоб переконатися, що вони відповідають організаційним вимогам. Важливо відзначити, що ITIL надає рекомендації, як адаптувати послуги при виникненні серйозних змін або надзвичайних ситуацій.

3. Перехід сервісу - на цьому етапі розглядаються етапи між закінченням циклу розробки IT-служби та моментом, коли сервіс запускається для користувачів. Наприклад, у випадку оновлення обладнання, варто з’ясувати, чи потрібно запускати оновлення програмного забезпечення, щоб перехід пройшов без збоїв. Фокус уваги на даному етапі лягає на тестування, оцінки і документування змін, а також управління знаннями для забезпечення правильного прийняття рішень.

4. Операції обслуговування - це все про повсякденну роботу і управління організаційним продуктом або послугою, гарантуючи, що їх надання буде

здійснюватися відповідно до вимог, встановлених раніше. На даному етапі увагу звертають на принципи, процеси, операційні дії і функції, необхідні для забезпечення працездатності сервісу. Цей крок гарантує, що є добре обгрунтований процес управління проблемами на той випадок, коли це станеться.

5. Постійне поліпшення обслуговування. Ефективний процес управління IT-послугами не зводиться до завершення проекту. Замість цього слід підготуватися до постійних вдосконалень, фіксуючи будь-які процеси, що повторюються і оцінюючи, як їх можна поліпшити. Щоб допомогти в цьому, останній модуль ITIL надає інструменти і рекомендації для оцінки ризиків і факторів успіху в рамках послуги або продукту.

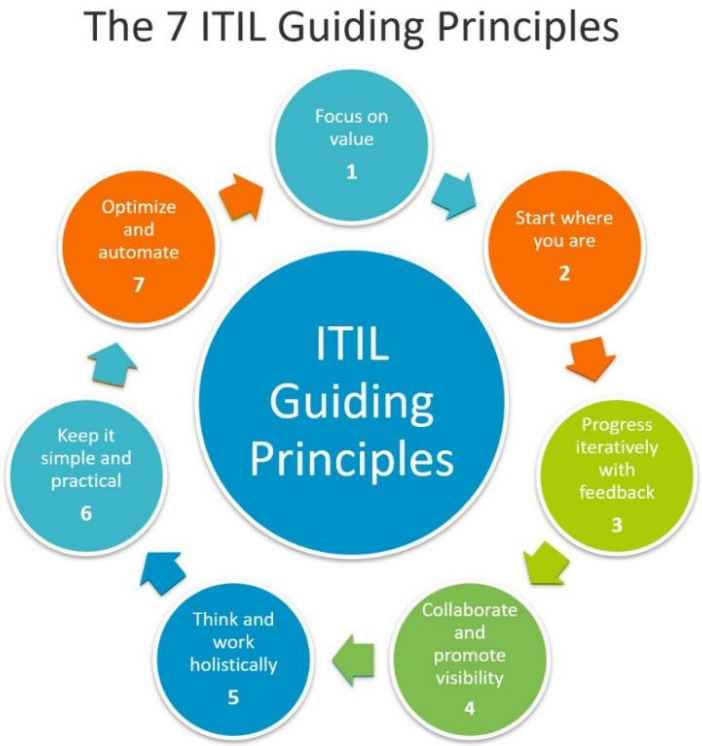

Рисунок 3.3 Керівні принципи ITIL

Нижче аргументовано, яка різниця між ITIL V3 і ITIL 4 та чому підприємствам потрібно сфокусувати свій вибір на ITIL 4.

ITIL 4 - це вдосконалена версія ITIL V3, мета якої - більш чітке об'єднання програмного забезпечення з сучасною системою управління IT-послугами. Він набагато більш гнучкий, з великим упором на спільну роботу. Він також є

ініціативою спільноти, і фахівці-практики ITIL допомагають оновлювати структуру, постійно враховуючи додаткові розробки в світі IT.

Ось деякі з найбільш важливих оновлень ITIL 4:

- Інтеграція - ITIL 4 розроблений для інтеграції з іншими популярними методами і стандартами ITSM, такими як Agile, Lean і DevOps.
- Клієнти. На відміну від ITIL V3, ITIL 4 розглядає клієнтів як найважливішу частину створення і підтримки цінності.
- Система цінностей послуг (SVS) - описує, як різні елементи організації працюють разом для створення матеріальної цінності. У цьому рівнянні найбільш важливими вхідними даними є «Попит» і «Можливості», а на виході - «Цінність», створена продуктами і послугами IT. Тим часом, SVS регулюється Керівними принципами, управлінням, ланцюжком створення вартості послуг (SVC), практиками та постійним вдосконаленням.
- Гнучкість - SVS не є жорсткою системою; скоріше, система визнає, що різні елементи, її складові можуть бути об'єднані різними способами в залежності від поточного сценарію або мінливих потреб контролюючої організації.
- Комунікація - нова структура заохочує спілкування заради усунення розрізненого мислення. Щоб отримати від SVS якомога більше користі, практикуючим фахівцям ITIL рекомендується застосовувати його у всій організації.

Сертифікація ITIL відіграє важливу роль в сучасному бізнесі. Цифрові сервіси, якими всі користуються щодня не були розроблені у вакуумі; скоріше, вони були побудовані з використанням постійного процесу управління проектами, який враховував не тільки цілі послуги, а й потенційні проблеми при її розробці, надання та підтримки. Коротше кажучи, потрібно було врахувати величезну кількість чинників.

Процес якісного управління IT-послугами - це знання того, як інтегрувати ці фактори в процес розробки, і саме тут на допомогу приходить ITIL. Він охоплює весь життєвий цикл розробки, від визначення вимог з точки зору бізнесу та IT,

проектування і створення рішення до надання та підтримку послуги в стані постійного аналізу і поліпшення.

Використання цієї стратегії дає підприємствам ряд переваг. Особливо це може скоротити кількість часу і грошей, які витрачаються даремно протягом усього життєвого циклу розробки послуг, а також підвищити якість кінцевого продукту. Це, в свою чергу, може значно підвищити задоволеність клієнтів після впровадження послуги або продукту, а також моральний дух співробітників, що працюють над ними.

Інвестуючи в навчальний курс і впроваджуючи ITIL на підприємстві, можна розраховувати на те, що в компанії з'явиться краще розуміння своїх клієнтів, щоб надавати послуги, які відповідають їхнім потребам. Це допоможе побудувати довгострокові відносини і поліпшити репутацію. Також буде можливість побудувати правильний алгоритм того, як скласти керівництво з прогнозування проблем з сервісом і реагування на них з урахуванням безлічі факторів, таких як взаємодія з користувачем, а не просто зосередження уваги на IT-розробці.

Особливу увагу потрібно звернути на те, що завдяки впровадженню рекомендацій ITIL відбудеться підвищення продуктивності і покращення управління ресурсами. Працівники підприємства зможуть керувати ризиками без порушень або ненавмисного саботажу сервісу. Також буде можливість створення стабільного середовища розробки послуг, яке підтримує постійні зміни.

Ще одним плюсом впровадження ITIL стане забезпечення узгодженості між IT та іншими підрозділами компанії. Це може бути життєвоважливо для розробки архітектури підприємства. Відбудеться поліпшення процесу управління ризиками за рахунок прогнозування та зменшення кількості помилок і збоїв в обслуговуванні. Також працівники підприємства зможуть швидко адаптуватися до технологічних змін з дотриманням нормативних вимог, щоб продовжувати розвиватися й підтримувати свою конкурентну перевагу. Крім того проходження всесвітньо визнаної сертифікації ITIL сприятиме підвищенню авторитету бізнесу [38].

Важливо пам'ятати, що всі окремі модулі ITIL можуть бути дуже корисні для бізнесу. Кожен з них дає корисну інформацію, допомагаючи встановити чіткий процес розробки ITSM.

Висновки до третього розділу

Досліджено відкритий IT-стандарт COBIT, який містить ряд документів зі стандартами щодо оптимізації управління IT. Стандарт сприяє чіткішій координації дій IT-департаменту та керівництва компанії, об'єднує в собі ряд інших стандартів, що дозволяє на високому рівні якості отримувати інформацію про стан IT та управляти цілями і задачами IT.

Завдання COBIT полягає в ліквідації розриву між керівництвом компанії з їх баченням бізнес-цілей та IT-департаментом, що здійснює підтримку інформаційної інфраструктури, яка повинна сприяти досягненню цих цілей. Стандарт детально описує цілі і принципи управління, об'єкти управління, чітко визначені всі IT-процеси (завдання), що протікають в компанії, і вимоги до них, охарактеризовано можливий інструментарій (практики) для їх реалізації.

Аналізуючи спеціальні публікації (SP) NIST варто звернути увагу на те, що вони насамперед спрямовані на упровадження політики управління ризиками інформаційної безпеки. Публікації NIST серії 800 визначають керівні принципи, надають вказівки і рекомендації за різними напрямами забезпечення кібербезпеки, зокрема класифікування інформації та інформаційних систем за вимогами безпеки, управління ризиками та інцидентами інформаційної безпеки, забезпечення безперервності захисту ІС, оцінювання рівня інформаційної безпеки та іншими. Крім рекомендацій, які розроблені для підтримки безпеки інформаційних систем федерального уряду США, NIST публікує технічні специфікації й річні звіти про свою діяльність в галузі кібербезпеки.

Також було досліджено бібліотеку ITIL, яка представляє новий підхід до розробки і надання послуг в сфері IT – через призму життєвого циклу IT-послуг.

Бібліотека складається з п'яти взаємопов’язаних книг, кожна з яких присвячена різним елементам життєвого циклу IT-послуг (стратегія й управління обслуговуванням, проектування, впровадження та вдосконалення послуг).

Методологічний підхід ITIL дозволяє забезпечити ефективне функціонування IT-служб, задовольнити потреби бізнес-користувачів, забезпечити стабільний і прогнозований розвиток ІС підприємства. ITIL пропонує бізнесу шляхом грамотної розробки й підтримання безпечного IT-середовища найкращим чином управляти ризиками, розробляти продукти, поліпшувати взаємини з клієнтами, оптимізувати витрати, прискорювати перебіг процесів і збільшувати число послуг. ITIL виступає за те, щоб IT і цифрові послуги відповідали потребам бізнесу і підтримували його основні цілі та завдання.

РОЗДІЛ 4.
ВІТЧИЗНЯНА ПРАКТИКА СТАНДАРТИЗАЦІЇ З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

4.1 Аналіз вітчизняного нормативно-правового забезпечення з інформаційної безпеки та захисту інформації

На сьогодні розпочато створення механізмів реалізації законів, підготовку законопроектів, що регламентують суспільні відносини в інформаційній сфері. Разом з тим, аналіз стану інформаційної безпеки України показує, що її рівень не повною мірою відповідає потребам суспільства і держави. Тому, формування бази правового забезпечення інформаційної безпеки є важливою складовою у процесі розвитку законодавства України в інформаційній сфері та захисту інформації в сучасних інформаційно-комунікаційних системах і мережах.

Метою розділу є аналіз існуючої нормативно-правової бази в галузі забезпечення інформаційної безпеки сучасних ІКСМ.

Під поняттям нормативно-правового забезпечення слід розуміти сукупність правових норм, що визначають порядок створення, правовий статус і функціонування захищених ІКСМ, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів.

Тобто нормативно-правове забезпечення регламентує та визначає порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації; статус інформаційної системи з точки зору інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов’язані з інформаційною безпекою; правові положення окремих видів процесу керування

та управління доступом в захищених ІКСМ; порядок створення й використання захищених ІКСМ; етапи побудови комплексу систем захисту інфомрації.

Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно-апаратних засобів слід керуватися низкою нормативно-правових документів та актів.

Нижче наводиться список законодавчих актів, нормативно-правових актів (НПА) та нормативних актів, які також стосуються інформаційної безпеки (стосовно захисту інформації) в Україні:

- Закон України «Про інформацію» від 02.10.1992 №2657 - XII;
- Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 №80/94.;
- Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII;
- Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI;
- Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373;
- Постанова Кабінету Міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 р. №1893.

Питання захисту інформації в ІТКС регулюють такі нормативні документи:

- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96;
- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

- НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп’ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);
- НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);
- НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53);
- НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);
- НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22).;
- НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;
- НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу;
- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;

Дослідження показали, що всі вище зазначені нормативні-документи визначають основи та положення організації захисту інформації на всіх етапах життєвого циклу ІКСМ. Основою побудови комплексної системи захисту

інформації сучасних ІКСМ, згідно нормативних документів є надання нормативно-методологічної бази для вибору і реалізації вимог до захисту інформації та інформаційних ресурсів в ІКСМ. Порядок вибору вимог до захисту інформації в ІКСМ визначається згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» .

Унормуванню питань управління інформаційною безпекою присвячені державні стандарти:

- ДСТУ СУІБ 1.0/ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)
- ДСТУ СУІБ 2.0/ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD)

З 01 січня 2017 року введено в дію *ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)*

Цей національний стандарт є перекладом ISO/IEC 27001:2015 Information technology - Security techniques - Information security management systems - Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги) зі зміною Cor. 1:2014.

Технічний комітет стандартизації, відповідальний за цей стандарт в Україні, - ТК 105 «Банківські та фінансові системи і технології».

Стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття системи управління інформаційною безпекою є стратегічним рішенням для організації. На проектування та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації,

вимоги щодо безпеки, застосовувані організаційні процеси, розмір і структура організації [31].

У цьому ж році введено в дію *ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)*

Цей стандарт ідентичний ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls (Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки) зі зміною Cor 1:2014.

Технічний комітет стандартизації, відповідальний за цей стандарт в Україні, - ТК 105 «Банківські та фінансові системи і технології».

Цей міжнародний стандарт розроблено для організацій для використання як довідкової інформації щодо вибору заходів безпеки під час впровадження системи управління інформаційною безпекою (СУІБ) на базі ISO/IEC 27001 [10] або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки. Цей стандарт також призначено для використання в розробленні настановчих документів з управління інформаційною безпекою, специфічних для промисловості та організацій, з урахуванням специфічних ризиків інформаційної безпеки їх середовища [32].

4.2 Сучасна практика стандартизації у сфері управління інформаційної безпеки в Україні

Прес-служба Мінекономрозвитку повідомляє, що з 1 січня 2019 року переважна більшість технічних стандартів Радянського Союзу - ГОСТів, розроблених до 1992 року, втратили чинність в Україні.

Необхідність припинення дії на території України радянських ГОСТів визначена Програмою діяльності Кабінету Міністрів України. Згідно з нею у 2015 році ДП «Український науково-дослідний і навчальний центр проблем

стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») були видані відповідні накази про скасування ГОСТів із втратою чинності протягом 2016-2018 років та з повною відмовою від них, починаючи з 1 січня 2019 року. Всього мали бути скасовані 12090 радянських ГОСТів.

Проте скасування такої кількості стандартів викликало певні труднощі у багатьох сферах діяльності, часто виникало питання чи можуть виробники користуватися ГОСТом, який втратив чинність. Мінекономрозвитку роз'яснив, як можна скористатись ГОСТом, який втратив чинність: «У разі якщо суб’єкт господарювання має наміри застосувати стандарт та використовувати його позначення, а потрібний йому ГОСТ скасовано, необхідно знайти заміну такому документу».

Для цього можна звернутися до Національного фонду нормативних документів (ДП «УкрНДНЦ»). Каталог національних нормативних документів розміщено на офіційному веб-сайті ДП «УкрНДНЦ). Загальна кількість національних стандартів на сьогодні становить 15133 документи.

ДП «УкрНДНЦ» також має доступ до всіх міжнародних та європейських стандартів. Міжнародні стандарти можна придбати в ДП «УкрНДНЦ» або звернутися безпосередньо до міжнародних організацій стандартизації. Але тут потрібно звернути увагу на питання застосування цих стандартів на національних територіях, і самим швидким та дешевим способом їх застосування є прийняття міжнародного або європейського стандарту як національного (наприклад, на мові оригіналу, або методом перекладу).

Також існує фонд галузевих нормативних документів, інформацію про які можна отримати у відповідних центральних органах виконавчої влади у визначених сферах діяльності.

Пунктом 1 частини першої статті 16 Закону встановлено, що підприємства, установи та організації мають право у відповідних сферах діяльності та з урахуванням своїх господарських і професійних потреб організовувати та виконувати роботи із стандартизації, зокрема: розробляти, приймати, перевіряти,

переглядати та скасовувати стандарти, кодекси усталеної практики, технічні умови і зміни до них, установлювати процедури їх розроблення, прийняття, перевірки, перегляду, скасування та застосування.

Тобто законодавство передбачає низку механізмів для отримання необхідного стандарту, враховуючи те, що використав право, надане підприємству вищезазначеної нормою Закону суб'єкт господарювання має право отримати свій власний документ, розроблений за своїми власними правилами.".

Також слід відмітити те, що НОС прийняв низку наказів, якими з 01.01.2019 року відновлено чинність деяких ГОСТів, розроблених до 1992 року. ГОСТ відновлені терміном до 01.01.2020, 01.01.2021, 01.01.2022.

Незважаючи на втрату чинності великої кількості радянських союзів, на Україні триває процес гармонізації стандартів з кращими європейськими та міжнародними стандартами.

Таким чином, у 2016 році прийнято 5105 національних нормативних документів (стандарти, ТУ, регламенти), з яких 91% гармонізовано з міжнародними та європейськими. У 2019 планується прийняти 3000 стандартів.

Також віце прем'єр-міністр Кубів заявив : «До 2020 року 80 відсотків технічних стандартів в Україні буде гармонізовано зі стандартами Європейського Союзу» [17].

Ще залишається важливим процес підписання Угоди про взаємне визнання Україною та ЄС сертифікатів відповідності на промислову продукцію (Agreements on Conformity Assessment and Acceptance of Industrial Products) (ACAA) як протокол до Угоди про асоціацію між Україною та ЄС. ACAA полегшить доступ на ринок шляхом усунення технічних бар'єрів в торгівлі промисловими товарами, адже імпортер платить двічі - за сертифікацію у власній країні, а потім - у нашій країні. Таким чином, кінцева ціна такого двічі сертифікованого товару збільшується, її платить наш споживач.

Укладення ACAA дасть можливість:

- вільно просуватись на внутрішньому ринку ЄС без додаткових процедур оцінки відповідності, адже роботи з оцінки відповідності українських органів визнаватимуться в ЄС, Швейцарії, Норвегії, Ісландії, Туреччині та потенційно в США, Канаді, Японії, Австралії, Новій Зеландії (ці країни без додаткової сертифікації визнають товари один одного);
- отримання українськими виробниками права нанесення європейського знаку відповідності СЕ (після прийняття АСАА дається 4 роки перехідного періоду для українського товаровиробника);
- вимоги українських технічних регламентів до продукції та пов'язаних процесів стануть ідентичними вимогам відповідних директив ЄС;
- взаємного визнання промислової продукції, що відповідає вимогам, згідно яких вона законно перебуває на ринку однієї зі сторін [18].

Щоб Україна та її виробники приєдналися до цього кола та без перепон могли продавати продукцію до ЄС, потрібно продовжувати реформувати та гармонізувати систему технічного регулювання.

Взагалі гармонізація стандарту - це приведення його змісту у відповідність з іншим стандартом для забезпечення взаємозамінності продукції (послуг), взаємного розуміння результатів випробувань і інформації, що міститься в стандартах.

Розрізняють декілька методів гармонізації, один з яких - метод «обкладинки», який зводиться до перекладу обкладинки європейського чи міжнародного стандарту, а сам текст залишається на мові оригіналу. У Законі «Про стандартизацію» зафіксовано використання, окрім української, однієї з мов відповідних міжнародних або регіональних організацій стандартизації (ст.7). Недоліком іншого методу є різне тлумачення стандарту, в результаті - випуск невідповідної стандартам (або й небезпечної) продукції.

Гармонізовані (еквівалентні) стандарти можуть містити деякі відмінності: по формі, в пояснювальних примітках, в окремих спеціальних вказівках і т.д. Тому керівництво ISO/IEC пропонує такі терміни: ідентичні стандарти та уніфіковані

стандарти. Ідентичні стандарти - гармонізовані стандарти, повністю ідентичні за змістом і за формою. Нерідко це точний переклад стандарту (міжнародного, регіонального), прийнятого в національній системі стандартизації. Ці стандарти можуть відрізнятися лише позначенням (шифром, кодом). Уніфіковані стандарти - це гармонізовані стандарти, які за змістом ідентичні, але відрізняються за формою подання. У результаті гармонізації законодавства прогнозується зменшення кількість перевірок бізнесу, скасування ліцензування та сертифікації більшості видів діяльності, адже ЗВТ передбачає не лише відмову від стягнення мит та зняття технічних бар'єрів, але й взаємний доступ до ринків послуг, можливість відкриття філій, створення спільних проектів тощо.

Таким чином, гармонізуючи з ЄС нормативно-правову базу і стандарти, Україна прагне перейти до так званого «роздержавлення системи стандартизації». Проте, що важливо, це може бути прийнято як вседозволеність з боку виробників. Тому норми ЄС слід приймати напряму, мовою оригіналу, адже у них вже давно проведено категоризацію, встановлено вимоги до найменування, маркування, традиційних технологій тощо. Виробники і постачальники повинні забезпечити виконання всіх вимог відповідних технічних регламентів перед введенням в обіг об'єктів технічних регламентів, що супроводжується декларацією про відповідність та/або сертифікатом відповідності, а також маркуванням продукції Національним знаком відповідності, якщо це передбачено відповідним технічним регламентом.

Далі будуть наведені три стандарти в сфері УІБ, що є гармонізовані з міжнародними стандартами ISO/IEC [22]:

1. ДСТУ ISO/IEC 27000:2017 Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів (ISO/IEC 27000:2016, IDT)

2. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги. Поправка (ISO/IEC 27001:2013; Cor 1:2014, IDT)

3. ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2015, IDT)

Окрему увагу потрібно звернути на Державний Стандарт України ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT) Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів - на заміну ДСТУ ISO/IEC 27000:2015 (ISO/IEC 27000:2014, IDT) (Рис.4.1).

Найменування документа (укр.)	Наказ від 04.08.2017 № 207 Про прийняття національних нормативних документів, гармонізованих з європейськими нормативними документами, поправки до національного нормативного документа, скасування національних нормативних документів
Дата прийняття	04.08.2017
Статус	Діючий
Вид документа	Наказ
Шифр документа	207
Розробник	ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»)
Орган, що прийняв	ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»)

Рис. 4.1 Опис стандарту ISO ДСТУ ISO/IEC 27000:2017.

Цей стандарт надає огляд систем управління інформаційною безпекою, а також терміни та визначення, які зазвичай використовують у сімействі стандартів СУІБ. Цей стандарт застосовний для всіх типів та розмірів організацій (наприклад, комерційних підприємств, державних установ, неприбуткових організацій).

Використовуючи сімейство стандартів ДСТУ ISO/IEC, організації можуть розробляти та впроваджувати основні положення управління безпекою своїх інформаційних ресурсів, зокрема фінансової інформації, інтелектуальної власності й детальної кадрової інформації або довіреної їм клієнтами, або третіми сторонами інформації. Ці стандарти можна також використовувати для підготування до незалежного оцінювання їх СУІБ стосовно захисту інформації.

Скасуванню підлягають національні стандарти України з питань інформаційної безпеки, які були прийняті наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193: ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки», ДСТУ ISO/IEC 27005:2015 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки».

Скасованим стандартом можна користуватись виключно як довідковим матеріалом без посилання на них у технічній, юридичній тощо документації, яку готує виробник (підприємство). Такі стандарти не є чинними та не визнані національними органами стандартизації.

Виробник може сам розробляти та запропонувати свої ДСТУ або затвердити Технічні умови під свою продукцію.

Під час застосування стандарту, який є обов'язковим, слід також врахувати те, що стандарти, як правило, містять посилання на інші стандарти, положення яких становлять разом сутність цього стандарту, і вимог таких стандартів слід також додержуватися.

У жовтні 2017 року вийшов оновлений стандарт ISO/IEC 27007:2018 «Інформаційні технології - Методи забезпечення безпеки - Керівництво по аудиту систем менеджменту інформаційної безпеки», який публікується з 2011 року. Стандарт був приведений у відповідність з ISO/IEC 27001: 2013.

ISO/IEC 27007: 2017 містить рекомендації з управління програмою аудиту системи управління інформаційною безпекою (СУІБ), проведення внутрішніх і зовнішніх аудитів СУІБ, а також компетентності і оцінки аудиторів СУІБ .

Крім того, він надає рекомендації для аудиту всіх вимог, викладених в ISO/IEC 27001: 2013 і використовується в поєднанні з інструкцією, викладеною в ISO 19011: 2011, слідуючи тій же структурі, що і цей міжнародний стандарт.

Також комітет ISO/IEC JTC 1 опублікував новий стандарт ISO/IEC 27021: 2017 «Інформаційні технології - Методи забезпечення безпеки - Вимоги до

компетенції професіоналів систем менеджменту інформаційної безпеки», який визначає вимоги до компетенції професіоналів СМІБ, або які беруть участь в створенні, впровадженні, обслуговуванні і постійному вдосконаленні одного або декількох процесів СМІБ, які відповідають вимогам ISO/IEC 27001.

Професійну оцінку відповідності систем менеджменту організацій законодавчим актам, вимогам міжнародних та національних стандартів в Україні здійснює з 2008 року ТОВ «Інтерсерт-УКРАЇНА» - офіційний представник німецького органу з сертифікації систем менеджменту і персоналу TÜV Thüringen (ТЮФ Тюрінген) з багаторічним практичним досвідом роботи кращих топ - менеджерів. ТОВ «Інтерсерт-УКРАЇНА» проводить аудити у 39-ти галузях економіки в країнах Європи відповідно до Європейської класифікації підприємств.

У той же час Кабінет Міністрів України 13 вересня 2017 року ухвалив постанову, яка вносить зміни до деяких законодавчих актів України, щоб узгодити їх із Законом України «Про стандартизацію». Про це повідомляє прес-служба Мінекономрозвитку. Але це стосується тільки питань здійснення торгівлі та взаємовідносин з Світовою організацією торгівлі. Відповідно до документу, із законодавчих актів мають бути виключені положення щодо: обов’язковості застосування національних стандартів; погодження проектів національних стандартів з державними органами; нормативно-правового регулювання відносин, пов’язаних із розробленням стандартів і технічних умов підприємств, установ та організацій; нагляду за дотриманням стандартів та штрафних санкцій за недотримання вимог стандартів.

У європейській практиці посилання на певні стандарти в актах законодавства, зокрема в директивах ЄС, є поодинокими випадками.

Важливість застосування стандартів у навчальній та науково-дослідній повсякденній діяльності в організації зобов'язує виконувати деякі рекомендаційні вимоги:

- відстежувати на новинних веб-сайтах зміни в стандартах (як правило міжнародні стандарти через рік-два уточняються, а переклад з англійської відбувається з великим запізненням або за гроші),
- використовувати скасовані стандарти можна тільки в якості додаткового довідкового матеріалу та без посилання на їх як нормативне джерело (через велику кількість застарілого матеріалу в мережі Інтернет).

4.3 Ключові проблеми гармонізації вітчизняної системи технічного регулювання з кращими практиками ЄС

Стандартизація відіграє важливу роль у створенні вимог, які забезпечують національне виробництво конкурентоспроможної продукції, і, таким чином, спрямована на забезпечення якісного розвитку економіки України. На сучасному етапі основним завданням цього напрямку є створення ефективної, адекватної, визнаної на міжнародному рівні національної системи стандартів, вимоги якої гармонізовано з вимогами міжнародних та європейських організацій стандартизації. Це дозволятиме використати досвід та досягнення розвинутих країн у національній економіці, сприятиме виходу українських товарів на світовий ринок.

В Україні існує проблема технічного регулювання, яке є надмірним і застарілим. Україна повинна виконувати положення договору про технічні бар’єри в торгівлі і віддавати пріоритет міжнародним стандартам порівняно з регіональними та іншими національними стандартами. Необхідно швидко впроваджувати міжнародні стандарти шляхом поєднання перекладу найважливіших з них, а для решти - впровадження мовою оригіналу.

Досвід колишніх соціалістичних держав (Чехія, Угорщина, Болгарія та ін.) показує, що членство в ЄС і СОТ сприяє розвитку економіки, насамперед за рахунок ліквідації торговельних бар’єрів та обмежень, і забезпечує доступ до капіталу, новітніх технологій та ринків збуту продукції.

Законодавча база України містить низку норм, що суперечать політиці ЄС та СОТ. Це може призвести до серйозних суперечностей, оскільки певні норми України не відповідають угодам, укладеним із СОТ, і зобов'язанням, взятим на себе Україною.

В ЄС система стандартизації та підтвердження відповідності пройшла два етапи формування. В 1985 році було прийнято директиви «нового», а потім і «глобального підходу» до технічної гармонізації. Гармонізовані стандарти (ISO, IEC та інші), на які є посилання у директивах, є лише одним можливим способом забезпечення відповідності продукції. Виробники не зобов'язані їх використовувати, хоча більшість із них обирає цей шлях. В ЄС процеси стандартизації служать як державним, так і приватним інтересам. Виробники, які дотримуються добровільних стандартів ЄС або ISO, вважаються такими, що дотримуються основоположних вимог директив Нового підходу.

Міжнародну систему добровільної стандартизації очолює три загальновизнані організації: Міжнародна організація зі стандартизації (ISO), Міжнародна електротехнічна комісія (IEC) та Міжнародний союз телекомунікацій (ITU). ISO є найбільшим світовим розробником міжнародних стандартів. ISO, IEC та ITU заклали підвалини стратегічного партнерства із СОТ для поширення вільної та чесної світової системи торгівлі. Політичні угоди, досягнуті у межах СОТ, потребують доповнення їх технічними угодами .

Сертифікація, що базується на цих стандартах, допомагає виробникам провадити експортну діяльність, а прийняття стандартів сприяє поширенню практики ефективного виробництва і нових технологій. Система спирається, передусім, на забезпечення механізмів внутрішнього моніторингу та контролю у підприємств, та на належне їх використання.

Системи технічного регулювання ЄС та України мають ряд відмінностей. В ЄС існує дві категорії технічних вимог: - обов'язкові і добровільні (90% стандартів ЄС є суто добровільними, інші 10% є рекомендованими до використання як такі, що підтверджують відповідність директивам. Обов'язкові

вимоги стосуються лише здоров'я і безпеки споживачів (включаючи інформування споживачів), добровільні стандарти - таких параметрів продукції/послуг, як якість, надійність, міцність тощо.

Зовсім протилежною є ситуація в Україні, де обов'язковою є стандартизація практично всієї продукції, яка не забезпечує якості і є бар'єром для впровадження інновацій через надмірно детальні вимоги, що є обов'язковими до виконання. Обов'язкова сертифікація також поширюється на продукти харчування, для яких міжнародна практика передбачає абсолютно інший регуляторний підхід.

В Україні добре функціонує система органів стандартизації та сертифікації, яка має розгалужену мережу сертифікаційних центрів в областях, причому більшість із них оснащені сучасними лабораторіями та залучають компетентний персонал. При новій системі, заснованій на моделі ЄС, всі ці активи можна було би і надалі застосовувати у набагато більш ефективний спосіб для підтримки економічного зростання та для вигоди споживачів .

Інституційні проблеми, які виникають при реєстрації нового стандарту, полягають в значних затратах часу і коштів; нові стандарти, або так звані технічні умови потрібно розробити і зареєструвати. Суб'єктам господарювання більшість нових продуктів в Україні легше впроваджувати на основі технічних умов. Для забезпечення відповідності правилам ЄС українські виробники основних засобів повинні будуть дотримуватись двох наборів регламентів та специфікацій для одного й того ж виробничого процесу – «старого» та «нового». Інакше можлива втрата головних експортних партнерів для українських підприємств з пострадянських країн, що мають подібну систему, побудовану на основі ГОСТів.

Інтеграція до СОТ та майбутні переговори з Угоди про Вільну Торгівлю з Європейським Союзом пропонують Україні винятково позитивні перспективи, які можуть бути досягнуті шляхом реформ. Першочерговими завданнями цих реформ мають бути:

- Встановлення добровільності стандартів та впровадження обов'язкових вимог щодо безпеки та інформування.

- Скорочення обсягів обов’язкової сертифікації.
- Перехід до системи контролю, що базується на ринкових перевірках та відповідальності виробника.
- Швидке впровадження міжнародних стандартів шляхом поєднання перекладу найважливіших з них, а для решти - пряме впровадження мовою оригіналу.

На наступному етапі Україна має переглянути та пересортувати різні функції до нової інституційної структури.

Приєднання України до міжнародних угод спростить процедури сертифікації. У певних випадках, система технічного регулювання імпортованої продукції є простішою за ту, що застосовується до вітчизняних виробників. Цей факт не змінює загальної картини, коли система технічного регулювання є тягарем як для імпортерів, так і для вітчизняних виробників . Цей підхід дозволяє збалансувати витрати та вигоди управління та є базовим принципом для технічного регулювання у розвинутих країнах.

Висновки до четвертого розділу

Аналіз показав, що основи законодавства України у сфері інформаційної безпеки закладено, однак воно потребує подальшого розвитку та вдосконалення з багатьох аспектів. На сьогодні державні стандарти у сфері управління інформаційної безпеки (ДСТУ ISO/IEC) є гармонізованими міжнародними стандартами. Це можна спостерігати на прикладі розглянутих у розділі стандартів ДСТУ ISO/IEC 27002:2015, ДСТУ ISO/IEC 27001:2015, які були введені в дію у 2017 році.

Однією з причиною гальмування у розробленні державних стандартів в Україні, особливо у галузі інформаційної безпеки та захисту інформації, є брак коштів, недостатня правова та нормативна база. Слід також відмітити таку тенденцію у сфері стандартизації: спроби створення стандартів, які описують

ідеологію застосування тих або інших принципів побудови захисту інформації в ІКСМ, однак не окреслюють конкретні алгоритми.

Така тенденція у розвитку міжнародних стандартів може бути дуже корисною з точки зору побудови системи державних стандартів. ISO/IEC 27007 Такий шлях створення стандартів України є достатньо дешевим і швидким, який одночасно дозволить усунути велику кількість проблем, які вже виникали в інших державах при створенні стандартів у галузі інформаційної безпеки та захисту інформації.

ВИСНОВКИ

Встановлено, що загальні положення та основні поняття в сфері стандартизації встановлено у Законі України «Про стандартизацію» та інших дотичних нормативно-правових актах. Відповідно до законодавства головними суб'єктами в сфері стандартизації в Україін є: центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації (Міністерство економічного розвитку і торгівлі України); центральний орган виконавчої влади, що реалізує державну політику у сфері стандартизації (Департамент технічного регулювання, що є самостійним структурним підрозділом центрального апарату Мінекономрозвитку); національний орган стандартизації (ДП «УкрНДНЦ»); технічні комітети стандартизації; підприємства, установи та організації, що здійснюють стандартизацію.

У результаті вивчення процедури розробки стандартів в Україні встановлено такі п’ять головних її етапів: організація розробки стандартів; розробка проекту стандартів (першої редакції); організація розробки стандартів (остаточна редакція); затвердження та державна реєстрація стандарту; видання стандарту. Також потрібно відзначити, що стандарти застосовуються на добровільних засадах, якщо інше не установлено законодавством.

Досліджено сімейство міжнародних стандартів на системи управління інформаційною безпекою ISO/IEC 27к, що розробляється Технічним комітетом ISO/IEC JTC 1/SC 27 і включає понад 50 стандартів, 9 з яких стосуються власне управління інформаційною безпекою.

Особливої уваги приділено стандарту ISO/IEC 27001, відповідно до вимог якого проводять сертифікацію систем управління інформаційною безпекою на підприємствах та в організаціях по всьому світі. Стандарт ISO/IEC 27001 сфокусований на захисті конфіденційності, цілісності та доступності інформації в організації. Це реалізовується шляхом виявлення потенційних проблем з

інформацією (тобто оцінки ризиків), а потім визначення необхідних кроків для запобігання появі таких проблем (тобто зниження або обробки ризиків).

Останнім оновленим стандартом сімейства ISO/IEC 27к є ISO/IEC 27000:2018. Вдосконалений стандарт забезпечує додаткові переваги, оскільки він об'єднав важливу термінологію, що використовують інші стандарти в серії ISO/IEC 27к, а також описує взаємозв’язки між стандартами з управління інформаційною безпекою: сфери діяльності, роль, функції і зв'язки один з одним.

Досліджено відкритий IT-стандарт COBIT, який містить ряд документів зі стандартами щодо оптимізації управління IT. Стандарт сприяє чіткішій координації дій IT-департаменту та керівництва компанії, об'єднує в собі ряд інших стандартів, що дозволяє на високому рівні якості отримувати інформацію про стан IT та управляти цілями і задачами IT.

Завдання COBIT полягає в ліквідації розриву між керівництвом компанії з їх баченням бізнес-цілей та IT-департаментом, що здійснює підтримку інформаційної інфраструктури, яка повинна сприяти досягненню цих цілей. Стандарт детально описує цілі і принципи управління, об'єкти управління, чітко визначені всі IT-процеси (завдання), що протікають в компанії, і вимоги до них, охарактеризовано можливий інструментарій (практики) для їх реалізації.

Встановлено, що спеціальні публікації NIST серії 800 (SP 800) спрямовані насамперед на впровадження політики управління ризиками інформаційної безпеки. Публікації NIST SP 800 визначають керівні принципи, надають вказівки і рекомендації за різними напрямами забезпечення кібербезпеки, зокрема класифікування інформації та інформаційних систем за вимогами безпеки, управління ризиками та інцидентами інформаційної безпеки, забезпечення безперервності захисту ІС, оцінювання рівня інформаційної безпеки та іншими.

Також було досліджено бібліотеку ITIL, яка представляє новий підхід до розробки і надання послуг в сфері IT – через призму життєвого циклу IT-послуг. Бібліотека складається з п'яти взаємопов’язаних книг, кожна з яких присвячена різним елементам життєвого циклу IT-послуг (стратегія й управління

обслуговуванням, проектування, впровадження та вдосконалення послуг). Методологічний підхід ITIL дозволяє забезпечити ефективне функціонування IT-служб, задовольнити потреби бізнес-користувачів, забезпечити стабільний і прогнозований розвиток ІС підприємства. ITIL виступає за те, щоб IT і цифрові послуги відповідали потребам бізнесу і підтримували його основні цілі та завдання.

Аналіз показав, що основи законодавства України у сфері інформаційної безпеки закладено, однак воно потребує подальшого розвитку та вдосконалення з багатьох аспектів. На сьогодні державні стандарти у сфері управління інформаційної безпеки (ДСТУ ISO/IEC) є гармонізованими міжнародними стандартами. Це можна спостерігати на прикладі розглянутих у розділі стандартів ДСТУ ISO/IEC 27002:2015, ДСТУ ISO/IEC 27001:2015, які були введені в дію у 2017 році.

Однією з причиною гальмування у розробленні державних стандартів в Україні, особливо у галузі інформаційної безпеки та захисту інформації, є брак коштів, недостатня правова та нормативна база. Слід також відмітити таку тенденцію у сфері стандартизації: спроби створення стандартів, які описують ідеологію застосування тих або інших принципів побудови захисту інформації в ІКСМ, однак не окреслюють конкретні алгоритми. Така тенденція у розвитку міжнародних стандартів може бути дуже корисною з точки зору побудови системи державних стандартів. ISO/IEC 27007 Такий шлях створення стандартів України є достатньо дешевим і швидким, який одночасно дозволить усунути велику кількість проблем, які вже виникали в інших державах при створенні стандартів у галузі інформаційної безпеки та захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про стандартизацію: Закон України від 2 жовтня 2018р. № 2581-VIII // Відомості Верховної Ради України. – 2014р. – №31. – ст. 1058.

2. Про технічні регламенти та оцінку відповідності: Закон України від 15 січня 2015р. № 124-VIII // Відомості Верховної Ради України. – 2015р. - №14. – ст.96

3. Про метрологію та метрологічну діяльність: Закон України від 9 листопада 2017р. № 2189-VIII // Відомості Верховної Ради України. – 2014р. – №1. – ст.1

4. Про основні принципи та вимоги до безпечності та якості харчових продуктів: Закон України від 6 грудня 2018р. № 2639-VIII // Відомості Верховної Ради України. – 2019р. - №7. – ст. 41

5. ДСТУ 1.2:2003. Національна стандартизація. Порядок розроблення національних нормативних документів. / Нац. стандарт України. – Вид. офіц. – [Чинний від 2003-24-02]. – Київ : Держспоживстандарт, 2003.

6. ДСТУ 1.5:2003. Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів. / Нац. стандарт України. – Вид. офіц. – [Чинний від 2003-07-01]. – Київ : Держспоживстандарт, 2003

7. ISO/IEC 27000:2018. Інформаційні технології. Методи безпеки. СУІБ. Огляд і словник./ Міжнародний стандарт. – 2012. URL: https://www.iso.org/ru/standart/73906.html (дата звернення: 09.12.2020).

8. ISO/IEC 27001:2013. Інформаційні технології. Методи безпеки. СУІБ. Вимоги. / Міжнародний стандарт. – 2013. URL: https//www.iso.org/ru/isoiec-27001-information-security.html (дата звернення: 09.12.2020).

9. ISO/IEC 27006:2015. Інформаційна безпека. Методи безпеки. Рекомендації органам аудиту й сертифікації СУІБ. / Міжнародний стандарт. – 2007. URL: https//www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf (дата звернення: 09.12.2020).

10. ISO/IEC 27002:2013. Інформаційні технології. Методи безпеки. Кодекс правил для управління інформаційною безпекою. / Міжнародний стандарт. – 2005. URL: https//www.intercert.com.ua/articles/posts/345-iso-ies-27002-2013-osnova-dlya-vibora-sredstv-upravleniya-smib (дата звернення: 09.12.2020).

11. ISO/IEC 27003:2017. Інформаційні технології. Методи безпеки. Керівництво з упровадження УІБ. / Міжнародний стандарт. – 2010. URL: https//www.uk.wikipedia.org/wiki/ISO_IEC_27003 (дата звернення: 09.12.2020).

12. ISO/IEC 27004:2016. Інформаційні технології. Методи безпеки. УІБ. Вимірювання. / Міжнародний стандарт. – 2009. URL: https//www.iso.org/ru/standart/64120.html (дата звернення: 09.12.2020).

13. ISO/IEC 27005:2018. Інформаційні технології. Методи безпеки. Управління ризиками інформаційної безпеки. – 2008. URL: https//www.iso.org/ru/standart/75281.html (дата звернення: 09.12.2020).

14. ISO/IEC 27007:2017. Інформаційні технології. Методи безпеки. Настанова з аудиту СУІБ. / Міжнародний стандарт. – 2011. URL: https//www.iso.org/ru/standart/67398.html (дата звернення: 09.12.2020).

15. ISO/IEC 27011:2016. Інформаційні технології. Методи безпеки. Настанови з УІБ для телекомунікаційних компаній. / Міжнародний стандарт. – 2008. URL: https//www.iso.org/ru/standart/64143.html (дата звернення: 09.12.2020).

16. ISO/IEC 27799:2016. Інформатика в охороні здоров'я. УІБ в охороні здоров'я. / Міжнародний стандарт. – 2008. URL: https//www.iso.org/ru/standart/62777.html (дата звернення: 09.12.2020).

17. Україна планує до 2020 року гармонізувати з європейськими 80% стандартів. URL: http://discovery.4uth.gov.ua/oformlenna-doslidnoie-roboti/skladanna-spisku-vikoristanoie-literaturi (дата звернення: 10.12.2020).

18. Аналіз національної системи стандартизації та сертифікації у контексті угоди про асоціацію України з ЄС. URL: http://zt.knteu.kiev.ua/files/2015/3(80)/uazt_2015_3_8 (дата звернення: 10.12.2020).

19. Радянські ГОСТи втратили чинність. URL: https://www.kmu.gov.ua/ua/news/z-1-sichnya-2019-roku-bilshe-90-radyanskih-gostiv-vtratili-chinnist-v-ukrayini (дата звернення: 12.12.2020).

20. Формування інформаційної безпеки. URL: file:///C:/Users/mr.lbdnts/Downloads/ssia.pdf (дата звернення: 12.12.2020).

21. Переглянутий ключовий стандарт по ІБ. URL: https://www.iso.org/ru/news/ref2266.html (дата звернення: 12.12.2020).

22. ДСТУ (Державний стандарт України) . URL: http://online.budstandart.com/ua/catalog/ klassifikator-po-vidam-dokumentov/dstu (дата звернення: 12.12.2020).

23. Зміни в нормативних документах України з питань ЗІ. URL: http://www.dut.edu.ua/ua/news-1-611-5143-zmini-v-normativnih-dokumentah-ukraini-z-pitan-zahistu-informacii---v-navchalniy-proces-universitetu (дата звернення:15.12.2020).

24. ISO/IEC 27000. Серия стандартов. URL: https://intercert.com.ua/articles/regulatory-documents/210-iso-27000 (дата звернення: 15.12.020).

25. До уваги користувачів стандартів та ТК стандартизації України. URL: http://uas.org.ua/ua/news/do-uvagi-koristuvachiv-standartiv-ta-tehnichnih-komitetiv-standartizatsiyi-ukrayini-tk/ (дата звернення: 15.12.2020).

26. Технічні комітети стандартизації. URL: https://protocol.ua/ua/pro_standartizatsiyu_ stattya_15/ (дата звернення: 15.12.2020).

27. Загальні положення з захисту інформації в комп’ютерних системах від НСД: НД ТЗІ 1.1-002-99. —[Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

28. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

29. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

30. Банки мають формувати зважений підхід до управління інформаційною безпекою. URL: https://bank.gov.ua/control/uk/publish/printable_article?art_id=17505162&showTitle=true (дата звернення: 19.12.2020).

31. ДСТУ ISO/IEC 27001:2015 IT. Методи захисту СУІБ. Вимоги (ISO/IEC 27001:2013). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910 (дата звернення: 19.12.2020).

32. ДСТУ ISO/IEC 27002:2015 IT. Методи захисту. Звід практик щодо заходів ІБ . URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911 (дата звернення: 19.12.2020).

33. What is COBIT? URL: https://www.cio.com/article/3243684/what-is-cobit-a-framework-for-alignment-and-governance.html (дата звернення: 19.12.2020).

34. COBIT. URL: https://www.vanharen.net/blog/cobit-in-3-minutes/ (дата звернення: 19.12.2020).

35. NIST SP 800. Бібліотека по інформаційній безпеці. URL: https://habr.com/ru/post/164371/ (дата звернення: 20.12.2020).

36. NIST Спеціальні публікації. URL: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information (дата звернення: 20.12.2020).

37. What is ITIL? URL: https://www.axelos.com/best-practice-solutions/itil/what-is-itil (дата звернення: 21.12.2020).

38. What is ITIL? Everything you need to know. URL: https://www.goodelearning.com/courses/it-service-management/itil-foundation/what-is-itil (дата звернення: 21.12.2020).

39. COBIT. URL: https://uk.wikipedia.org/wiki/COBIT (дата звернення: 21.12.2020).