МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
д.е.н, доцент	д.е.н, доцент
_____ С.В.Легомінова	_____ С.В.Легомінова
«___»_____20__ р.	«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

СТУДЕНТ: Кравченко Катерина Андріївна _____

(підпис)

КЕРІВНИК: к.т.н., доцент Дзюба Тарас Михайлович _____

(підпис)

НОРМОКОНТРОЛЕР: к.т.н., с.н.с. Рябчун Дмитро Ігорович _____

(підпис)

Київ – 2021

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
_____ С.В. Легомінова
(підпис)
“___”_____ 20__ р.

ЗАВДАННЯ

на дипломну роботу

студенту Кравченко Катерині Андріївні

1. Тема роботи «Нормативно-правове забезпечення інформаційної безпеки підприємства», затверджена наказом по університету від “13” жовтня 2020 р. № 230.
2. Термін здачі студентом оформленої роботи “10” січня 2021 р.
3. Об’єкт дослідження: забезпечення інформаційної безпеки підприємства.
4. Предмет дослідження: нормативно-правове забезпечення інформаційної безпеки підприємства.
5. Мета дослідження: дослідження засад нормативно-правового забезпечення інформаційної безпеки підприємства.
6. Перелік питань, які мають бути розроблені:
1. Дослідити нормативно-правові засади забезпечення інформаційної безпеки та захисту інформації в Україні.
2. Проаналізувати систему міжнародних стандартів з інформаційної безпеки, зокрема стандарти серії ISO / IEC 27 к.
3. Дослідити стандарт Cobit та розглянути можливі варіанти впровадження його на підприємстві.
7. Дата видачі завдання “14” жовтня 2020 р.

Науковий керівник Т.М.Дзюба

(підпис)

Завдання прийнято до виконання К.А.Кравченко

(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «16» _вересня_ 2020 р.

№ з/п	Етапи 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-правових засад забезпечення інформаційної безпеки та захисту інформації в Україні.	12.10.2020	
4.	Аналіз системи міжнародних стандартів з інформаційної безпеки, зокрема стандартів серії ISO/IEC 27к	22.10.2020	
5.	Розгляд стандарту Cobit та можливих варіантів впровадження його на підприємстві	02.11.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	23.11.2020	
7.	Оформлення роботи.	07.12.2020	
8.	Оформлення презентації.	14.12.2020	
9.	Отримання рецензії на роботу.	25.12.2020	
10.	Захист в ДЕК.	__.01.2021	

Студент К.А.Кравченко

(підпис)

Науковий керівник Т.М.Мужанова

(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню проблем нормативно-правового забезпечення інформаційної безпеки підприємства. Робота складається зі вступу, трьох розділів, що містять 5 рисунків та 4 таблиці, висновків та списку використаних джерел із 38 найменувань. Загальний обсяг роботи становить 81 аркушів, з яких 5 аркушів займають перелік умовних позначень і скорочень та список використаних джерел.

Об'єктом дослідження є забезпечення інформаційної безпеки підприємства. **Предметом дослідження -** нормативно-правове забезпечення інформаційної безпеки підприємства.

Метою роботи є вивчення засад нормативно-правового забезпечення інформаційної безпеки підприємства.

Як результат у роботі досліджено нормативно-правові засади забезпечення інформаційної безпеки та захисту інформації в Україні; проаналізовано систему міжнародних стандартів з інформаційної безпеки, зокрема стандарти серії ISO/IEC 27 к; досліджено особливості стандарту Cobit, зокрема розгляд методології Cobit 5; запропоновано приклад використання стандарту Cobit на підприємстві.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СТАНДАРТИ ISO/IEC 27к, COBIT.

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ.....……	8
ВСТУП …….....	9
Розділ 1 НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ...	10
1.1Закони України з питань інформаційної безпеки та захисту інформації.....	13
1.2 Нормативні документи з питань захисту інформації……..	22
1.3 Галузеві стандарти України з управління інформаційною безпекою	29
Висновки до першого розділу ……	33
Розділ 2 СИСТЕМА МІЖНАРОДНИХ СТАНДАРТІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ……	35
2.1 Види міжнародних стандартів у сфері ІБ та безпеки ІТ……	35
2.2 «ПОМАРАНЧЕВА КНИГА» (TCSEC)……...	39
2.3 Стандарт ISO / IEC 17799 «Управління інформаційною безпекою»	43
2.4 Стандарт ISO / IEC 15408 «Загальні критерії»	48
2.5 Стандарти серії ISO/IEC 27000 щодо системи управління ІБ	49
Висновки до другого розділу …….	56
Розділ 3 ДОСЛІДЖЕННЯ ТА ВПРОВАДЖЕННЯ СТАНДАРТУ COBIT…….…….	57
3.1. Огляд стандарту COBIT……	57
3.1.1 Моделі зрілості……	61
3.1.2. Критичні фактори успіху ……	65
3.1.3. Ключові індикатори цілі ……	66
3.1.4. Ключові індикатори результату ……	66
3.2. Методологія COBIT 5……	67
3.3. Приклад використання каскаду цілей COBIT 5……	70
Висновки до третього розділу ……	75
ВИСНОВКИ ……	77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……	78

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

IEC	International Electrotechnical Commission - Міжнародна електротехнічна комісія
ISO	International Organization for Standardization - Міжнародна організація по стандартизації
ITU-T	International Telecommunication Union - Telecommunications - Міжнародний союз телекомунікації
TCSEC	Trusted Computer System Evaluation Criteria - Крите́рії оці́нки за́хисту комп'ю́терної системи
АС	автоматизована система
ГСТУ СУІБ	галузевий стандарт України системи управління інфомарційної безпеки
ДССЗІ	Державна служба спеціального зв'язку та захисту інформації України
ІБ	інформаційна безпека
ІС	інформаційна система
ІТС	інформаційно-телекомунікаційна система
КЗЗ	комплекс засобів захисту
НД ТЗІ	нормативний документ технічного захисту інформації
ОО	об'єкта оцінки
ОС	операційна система
ПЗ	програмне забезпечення
ПІБ	політика інформаційної безпеки
РСО	режимно-секретні органи
СЗІ	служби захисту інформації
СУІБ	система управління інформаційною безпекою
СУІБ	системи управління інформаційною безпекою
ТЗІ	технічний захист інформації
ФВБ	Функціональні вимоги безпеки
КІС	корпоративні інформаційні системи

ВСТУП

Актуальність теми. Під час створення сучасної та ефективної системи забезпечення інформаційної безпеки будь-якого підприємства істотного значення набуває наявність відповідної нормативно-правової бази.

Вичення чинного законодавства дозволяє правомірно побудувати сиситему захисту підприємства в інформаційній сфері, в той час як дослідження міжнародних стандартів у сфері інформаційної безпеки дозволяє використовувати перевірені на практиці інновації та більш надійно захистити інформаційні ресурси підприємства.

Мета і завдання дослідження. **Мета роботи** полягає у дослідженні засад нормативно-правового забезпечення інформаційної безпеки підприємства.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити нормативно-правові засади забезпечення інформаційної безпеки та захисту інформації в Україні.
2. Проаналізувати систему міжнародних стандартів з інформаційної безпеки, зокрема стандарти серії ISO / IEC 27 к.
3. Дослідити стандарт Cobit, зокрема розглянути методологію Cobit 5.

Об’єкт дослідження - забезпечення інформаційної безпеки підприємства. **Предмет дослідження** – нормативно-правове забезпечення інформаційної безпеки підприємства.

Методи дослідження. Для вирішення зазначених вище наукових завдань в роботі використані загальнонаукові методи (узагальнення, аналізу та синтезу), методи системного аналізу, теорії інформаційної безпеки.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при впровадженні системи управління інформаційною безпекою підприємства з урахуванням актуальних законодавчих та нормативних вимог.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів забезпечення інформаційної безпеки відповідно до цілей бізнесу, можливостей та ресурсів підприємства.

Розділ 1
НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Правовий захист інформації як ресурсу признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами (Рис. 1.1).

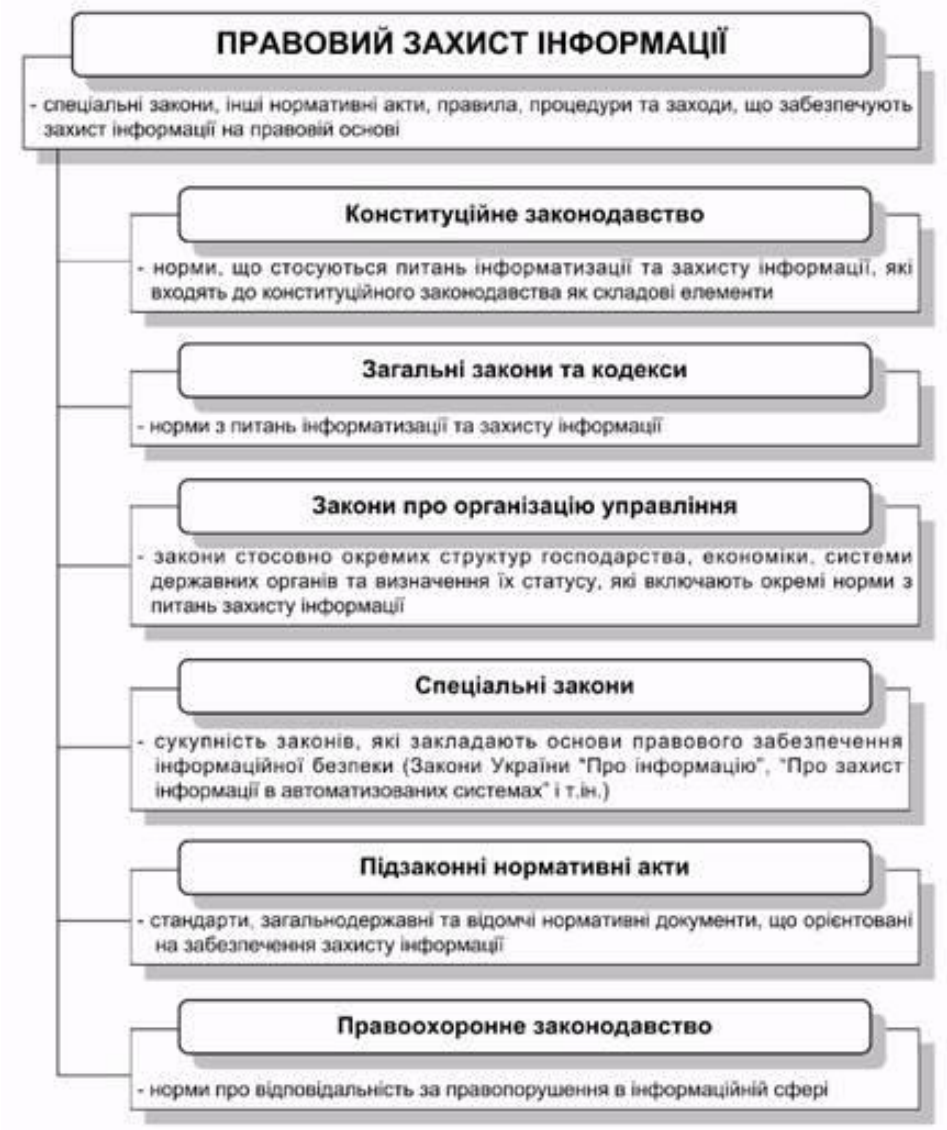

Рис.1.1. Правовий захист інформації.

У нашій державі такими правилами (актами, нормами) є Конституція України, закони України, цивільне, адміністративне, кримінальне право, викладене у відповідних кодексах. Що стосується відомчих нормативних актів, то вони визначаються наказами, керівництвами, положеннями та інструкціями, які видаються відомствами, організаціями та підприємствами, що діють у межах певних структур.

Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу та змісту, співвіднесення його зі всією системою законів та правових актів України.

Вимоги інформаційної безпеки повинні органічно входити до усіх рівнів законодавства, у тому числі й у конституційне законодавство, основні загальні закони, закони з організації державної системи управління, спеціальні закони, відомчі правові акти і т.ін. Звичайно використовується наступна структура правових актів, які орієнтовані на правовий захист інформації [1].

Конституційне законодавство. Норми, що стосуються питань інформатизації та захисту інформації, входять до нього як складові елементи. Відповідно до статті 34 Конституції України “кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір” [2].

Загальні закони, кодекси які включають норми з питань інформатизації та інформаційної безпеки. Так стаття 302 Цивільного кодексу (книга друга “Особисті немайнові права фізичної особи”) визначає, що “фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію”.

Закони про організацію управління, стосовно окремих структур господарства, економіки, системи державних органів та визначення їхнього статусу. Такі закони включають окремі норми з питань захисту інформації.

Спеціальні закони, які відносяться до конкретних сфер відносин, галузей господарства, процесів. До їхнього числа входять Закони України "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про доступ до публічної інформації", "Про державну таємницю", "Про основні засади забезпечення кібербезпеки України". Власне склад і зміст

цього блоку законів і створює спеціальне законодавство як основу правового забезпечення інформаційної безпеки [2].

Підзаконні нормативні акти із захисту інформації. Стандарти, загальнодержавні та відомчі нормативні документи, що орієнтовані на забезпечення захисту інформації.

Правоохоронне законодавство України, яке містить норми про відповідальність за правопорушення у сфері інформатизації.

Спеціальне законодавство в галузі безпеки інформації може бути представлене сукупністю законів. В їхньому складі особливе місце займають Закони "Про інформацію" та "Про захист інформації в інформаційно-телекомунікаційних системах", які закладають основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

• інформації та інформаційних систем;

• суб'єктів - учасників інформаційних процесів;

• правовідносин виробників та споживачів інформаційної продукції;

• власників (джерел) інформації - оброблювачів та споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян та держави.

Ці закони також визначають основи захисту інформації у системах обробки і при її використанні з урахуванням категорій доступу до відкритої інформації і до інформації з обмеженим доступом. Ці закони містять, крім того, загальні норми з організації та ведення інформаційних систем, включаючи банки даних державного призначення, порядок державної реєстрації, ліцензування, сертифікації, експертизи, а також загальні принципи захисту та гарантій прав учасників інформаційного процесу.

Таким чином, правовий захист інформації забезпечується нормативно-законодавчими актами, сукупність яких за рівнем представляє ієрархічну систему від Конституції України до функціональних обов'язків і контрактів конкретного виконавця, які визначають перелік відомостей, що підлягає охороні, і заходи відповідальності за їх розголошення [2].

1.1 Закони України з питань інформаційної безпеки та захисту інформації

Закон України «Про інформацію»

Базовим законом в сфері інформації є Закон України «Про інформацію». Він був прийнятий 1992 р., останні суттєві правки внесені 13 січня 2011 р. Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства та держави при одержанні, використанні, поширенні та зберіганні інформації.

Закон установлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу і суспільство від неправдивої інформації.

Закон визначає інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі. Відповідно об’єктами інформаційних відносин є документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров’я, а також у соціальній, екологічній, міжнародній та інших сферах.

Основні принципи інформаційних відносин:

- гарантованість права на інформацію;
- відкритість, доступність інформації та свобода її обміну;
- об'єктивність, вірогідність інформації;
- повнота і точність інформації;
- законність одержання, використання, поширення та зберігання інформації.

Усі громадяни України, юридичні особи та державні органи мають право на інформацію. Але реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні,

соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Згідно із Законом інформаційна діяльність розглядається як сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Важливе місце в Законі належить описові механізму функціонування інформаційних потоків у суспільстві. Так, держава здійснює контроль за режимом доступу до інформації. Завдання її при цьому полягає у забезпеченні додержання вимог законодавства про інформацію всіма державними органами, підприємствами, організаціями, недопущенні необґрунтованого віднесення відомостей до категорії інформації з обмеженим доступом. Державний контроль за додержанням установленого режиму здійснюється спеціальними органами, які визначають Верховна Рада і Кабінет Міністрів України [3].

Обмеження права на одержання відкритої інформації забороняється законом. Закон визначає порядок доступу до інформації: дає визначення інформаційного запиту, порядку його розгляду відповідними посадовими особами, визначає порядок відшкодування витрат, пов’язаних із задоволенням запиту, а також встановлює перелік документів та інформації, що не підлягає наданню для ознайомлення за запитами.

Інформація є об’єктом права власності громадян, організацій (юридичних осіб) і держави. Інформація може бути об’єктом права власності як у повному обсязі, так і об’єктом лише володіння, користування чи розпорядження. Власник інформації щодо об’єктів своєї власності має право здійснювати будь-які законні дії. Підставами виникнення права власності на інформацію є створення інформації своїми силами і за свій рахунок, договір на створення інформації, договір, який містить умови переходу права власності на інформацію до іншої особи.

Не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять у собі:

- інформацію, визнану у встановленому порядку державною таємницею;
- конфіденційну інформацію;

- інформацію про оперативну і слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дізнання та суду у тих випадках, коли її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;
- інформацію, що стосується особистого життя громадян;
- документи, що становлять внутрівідомчу службову кореспонденцію (доповідні записки, переписка між підрозділами та інше), якщо вони пов'язані з розробкою напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю;
- інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Установа, до якої звернуто запит, може не надавати для ознайомлення документ, якщо він містить інформацію, яка не підлягає розголошенню на підставі нормативного акта іншої державної установи, а та державна установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречення;
- інформацію фінансових установ, підготовлену для контрольно-фінансових відомств [3].

Положення Закону України “Про інформацію” конкретизуються в інших законах про інформаційну діяльність та охорону прав інтелектуальної власності, які мають більш конкретний характер, а також у низці інших законодавчих і нормативних актів.

Закону України «Про доступ до публічної інформації»

Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [4].

Метою цього Закону є забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації. Цей Закон не поширюється на відносини щодо отримання інформації суб'єктами владних повноважень при здійсненні ними

своїх функцій, а також на відносини у сфері звернень громадян, які регулюються спеціальним законом.

Закон України «Про доступ до публічної інформації» визначає види інформації з обмеженим доступом:

- конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов;

- таємна інформація - інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю;

- службова інформація, до якої може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Закон України «Про доступ до публічної інформації» також встановлює обмеження доступу до таких видів інформації:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні [4].

Також цей Закон визначає поняття «інформація про особу» та визначає умови доступу до такої інформації [4].

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

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації. Суб'єктами відносин, пов'язаних з обробкою інформації, є:

- власники інформації чи уповноважені ними особи;
- власники АС чи уповноважені ними особи;
- користувачі;
- спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпоряковані йому регіональні органи.

Відповідно до закону державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинен утворити службу захисту інформації або призначити осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним [6].

Закон України «Про державну таємницю»

Основним нормативно-правовим актом, що визначає режим державної таємниці, є Закон України « Про державну таємницю». Цей Закон регулює

суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

Зокрема, цей Закон визначає:

- компетенцію органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці;
- здійснення права власності на секретну інформацію та її матеріальні носії;
- порядок віднесення інформації до державної таємниці;
- порядок засекречення і розсекреченя матеріальних носіїв інформації;
- порядок охорони державної таємниці.

Згідно зі ст. 1 Закону « Про державну таємницю», державна таємниця є видом таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Віднесення інформації до державної таємниці – це процедура ухвалення (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до зводу відомостей, що становлять державну таємницю. Володілець секретної інформації або власник матеріальних носіїв такої інформації реалізує свої права з урахуванням обмежень, установлених в інтересах національної безпеки України відповідно до цього Закону [7].

Якщо внаслідок обмеження прав на секретну інформацію або її матеріальні носії заподіюється шкода особі, якій належать такі права, відшкодування здійснюється за рахунок держави в порядку та розмірах, що визначаються в договорі між такою особою і державним органом (органами), якому (яким) державним експертом з питань таємниць надається право приймати рішення щодо суб’єктів, які мають доступ до цієї інформації та її

матеріальних носіїв. Державний експерт з питань таємниць здійснює відповідно до вимог цього Закону віднесення інформації до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка у ньому міститься, згідно із Зводом відомостей, що становлять державну таємницю, - "особливої важливості", "цілком таємно" або "таємно".

Державні органи, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням створюються на правах окремих структурних підрозділів режимно-секретні органи (далі - РСО), які підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із Службою безпеки України. У своїй роботі РСО взаємодіють з органами Служби безпеки України [7].

Закон України «Про основні засади забезпечення кібербезпеки України»

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [8].

Закон регулює засади державно-приватної взаємодії у сфері кібербезпеки (тобто поєднання зусиль держави і бізнес-суб’єктів у вирішенні проблем

захисту інформації в інформаційно-телекомунікаційних системах) шляхом визначення напрямів такої співпраці:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі [9].

Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти

запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.[9]

Закон України «Про захист персональних даних»

Закон України «Про захист персональних даних», що був прийнятий у 2010 році та набув чинності з початку 2011 року, запровадив прогресивні норми, які покликані охороняти конфіденційні дані та приватну інформацію громадян під час їх обробки та зберігання у різноманітних базах даних.

Зокрема Закон визначає терміни у сфері захисту персональних даних, окреслює загальні та особливі вимоги до обробки персональних даних, засади їх використання, збирання, накопичення та зберігання, поширення, видалення або знищення. Також у Законі названо суб'єктів відносин, пов'язаних із персональними даними, та їх права, визначено порядок доступу до персональних даних, а також встановлено повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних.

Під персональними даними Закон розуміє відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Суб'єктами відносин, пов'язаних із персональними даними, визначені:

- суб'єкт персональних даних;
- володілець персональних даних;
- розпорядник персональних даних;
- третя особа;
- Уповноважений Верховної Ради України з прав людини.

Відповідно до Закону забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних [10].

Закон України «Про захист персональних даних» є базовим документом, на основі якого почалася і триває активна робота із розробки цілої низки

підзаконних актів, що деталізуватимуть норми Закону на стадії їх практичного застосування.

1.2 Нормативні документи з питань захисту інформації

Вимоги щодо захисту інформації регулюють нормативні документи системи технічного захисту інформації (далі – НД ТЗІ), які затверджує Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

Цей документ визначає основи організації і порядок виконання робіт по захисту інформації в інформаційно-телекомунікаційних системах (далі - ІТС), порядок ухвалення рішень по складу комплексної системи захисту інформації залежно від умов функціонування ІТС і видів оброблюваної інформації, визначення об'єму і змісту робіт, етапності робіт, основних завдань і порядку виконання роботи кожен етап. Дія цього НД ТЗІ поширюється тільки на ІТС, в яких здійснюється обробка інформації автоматизованим способом.

Відповідно, для таких ІТС для яких діють всі нормативно - правові акти і нормативні документи по створенню АС і по захисту інформації в АС. НД ТЗІ не встановлює нових норм, а систематизує в одному документі вимоги, норми і правила, які безпосередньо або побічно витікають з положень чинних нормативних документів.

Цей НД ТЗІ побудований у вигляді керівництва, яке утримує перелік робіт і посилання на чинних нормативних документах, відповідно до яких ці роботи необхідно виконувати. Якщо якийсь з етапів або видів робіт не нормовано, наводиться короткий зміст робіт і якими результатами вони повинні закінчуватися.

НД ТЗІ призначений для суб'єктів інформаційних стосунків (власників або розпорядників ІТС, користувачів), діяльність яких пов'язана з обробкою інформації, що підлягає захисту, розробників комплексних систем захисту інформації в ІТС, для постачальників компонентів ІТС, а також для фізичних і

юридичних осіб, що здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ. Встановлений сьогоденням НД ТЗІ порядок обов'язковий для усіх суб'єктів системи ТЗІ в Україні незалежно від їх організаційно - правової форми і форми власності, в ІТС яких обробляється інформація, яка належить до державних інформаційних ресурсів [11].

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі (затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53) - це нормативний документ організації, який визначає завдання, функції, штатну структуру служби захисту інформації (далі - СЗІ), повноваження та відповідальність її співробітників, взаємодію з іншими підрозділами та із зовнішніми організаціями.

Виконання вимог Положення є обов'язковим для всіх організацій державної форми власності України, а також для недержавних організацій, діяльність яких пов'язана з передаванням, обробленням та накопиченням інформації, що належить державі. В організаціях, де штатним розкладом не передбачено створення СЗІ, заходи щодо забезпечення захисту інформації в АС здійснюють призначені наказом керівника організації працівники. У цьому випадку положення про посадові (функціональні) обов'язки цих працівників має містити пункти, які б передбачали виконання ними вимог, що висувають до СЗІ.

Структуру СЗІ, її склад і чисельність визначають на підставі фактичних потреб АС із забезпечення вимог політики безпеки інформації. Чисельність і склад СЗІ мають бути достатніми для виконання всіх завдань із захисту інформації в АС [12].

Відповідальність за діяльність СЗІ покладено на її керівника.

Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації (далі - ТЗІ). Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян-суб`єктів підприємницької діяльності, органів державної влади, органів

місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

НД призначений для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, підприємств, організацій, установ, діяльність яких пов'язана з інформацією, необхідність охорони якої визначено законодавством України, а також виконавців робіт з ТЗІ.

Атестація комплексу ТЗІ здійснюється за відповідними програмою і методиками випробувань. На підставі результатів випробувань складається висновок щодо відповідності стану ТЗІ, який забезпечується комплексом, вимогам нормативних документів з ТЗІ [13].

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступуНД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

Цей нормативний документ установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи тощо.

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою.

Цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З розвитком нових тенденцій в галузі і за умови достатньої обґрунтованості документ є відкритим для включення до його складу Адміністрацією Державної служби спеціального зв'язку та захисту інформації України нових послуг [14].

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

Цей документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

Цей документ призначений для постачальників (розробників), споживачів (замовників, користувачів) автоматизованих систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації (інформації, яка потребує захисту), а також для державних органів, які здійснюють функції контролю за обробкою такої інформації.

Мета цього документа - надання нормативно-методологічної бази для вибору і реалізації вимог з захисту інформації в автоматизованій системі.

Автоматизована система являє собою організаційно-технічну систему, що об’єднує ОС, фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і призначенням АС.

В цьому документі за сукупністю характеристик АС (конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість різноманітних ступенів обмеження доступу оброблюваної інформації, кількість користувачів і

повноважень користувачів) виділено три ієрархічні класи АС, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас «1» - одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

Клас «2» - локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Клас «3» - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу [15].

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу

Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до технічних та організаційних заходів захисту інформації WEB-сторінки в мережі Інтернет.

Згідно з визначеними НД ТЗІ 2.5-004-99 специфікаціями він встановлює мінімально необхідний перелік послуг безпеки інформації та рівнів їх реалізації у комплексах засобів захисту інформації WEB-сторінки від несанкціонованого доступу.

Мета цього НД ТЗІ – надання нормативно-методологічної бази для розроблення комплексу засобів захисту від несанкціонованого доступу до інформації WEB-сторінки під час створення комплексної системи захисту інформації.

Цей НД ТЗІ призначений для суб’єктів відносин (власників або розпорядників WEB-сторінки, операторів (провайдерів), користувачів), діяльність яких пов’язана з розробкою та експлуатацією WEB-сторінки, розробників комплексної системи захисту інформації та постачальників окремих її компонентів, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності WEB-сторінки на відповідність вимогам ТЗІ [16].

Встановлені цим НД ТЗІ вимоги є обов’язковими для виконання державними органами, Збройними Силами України, іншими військовими формуваннями, утвореними відповідно до законів України, Радою Міністрів Автономної республіки Крим та органами місцевого самоврядування, а також підприємствами, установами та організаціями (далі - установи) усіх форм

власності під час захисту інформації, що належить до державних інформаційних ресурсів на WEB-сторінках. [17]

Для захисту інших видів інформації власники WEB-сторінок користуються цим НД ТЗІ на власний розсуд.

Згідно НД ТЗІ 2.5-010-03, WEB-сторінка установи може бути розміщена на власному сервері або на сервері, що є власністю оператора. Власник сервера зобов'язаний гарантувати власнику інформації рівень захисту відповідно до вимог даного НД ТЗІ.

Щоб захистити інформацію WEB-сторінки в АС створюються КСЗІ, що є сукупністю організаційних та інженерно-технічних заходів, а також програмно-апаратних засобів, які забезпечують захист інформації. [17]

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

Цей нормативний документ встановлює вимоги до порядку розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання і передачі (далі - оброблення) інформації з обмеженим доступом або інформації, захист якої гарантується державою.

Положення цього документа розповсюджуються на державні органи, а також підприємства, установи і організації всіх форм власності, які володіють, користуються і розпоряджаються інформацією, яка належить до державних інформаційних ресурсів, або інформацією, вимога щодо захисту якої встановлена законом. Власники (користувачі) іншої інформації, положення цього документа застосовують на свій розсуд [18].

Технічне завдання на комплексну систему захисту інформації (далі – КСЗІ) повинно розроблятись з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу автоматизованих систем.

Перелік вимог з захисту інформації повинен передбачати розроблення та використання сучасних ефективних засобів і методів захисту, які дають

можливість забезпечити виконання цих вимог з найменшими матеріальними затратами.

Технічне завдання на КСЗІ є одним із обов'язкових засадничих документів під час проведення експертизи АС на відповідність вимогам захищеності інформації [18].

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

- визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;
- створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;
- оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

Документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. д.) критичної інформації (інформації, що вимагає захисту), а також для державних органів, що здійснюють функції контролю за обробкою такої інформації.

Необхідно визнати, що на сьогоднішній день проблема захисту інформації не має остаточного вирішення. Тому цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З часом, як наслідок практичного застосування, а також з появою і розвитком нових тенденцій і підходів, в цей нормативний документ і інші нормативні і методологічні документи, що на ньому базуються, будуть вноситися відповідні корективи [19].

1.3 Галузеві стандарти України з управління інформаційною безпекою

Засади управління інформаційною безпекою визначають національні стандарти України: ДСТУ ISO/IEC 27001:2015 «Інформаційні технології Методи захисту. Системи управління інформаційною безпекою. Вимоги", ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки", а також галузеві стандарти України, прийняті Національним банком України для регулювання засад забезпечення інформаційної безпеки установ банківської сфери. Усі зазначені стандарти розроблені на основі відповідних міжнародних стандартів серії ISO 27к.

Національні стандарти з управління інформаційною безпекою були внесені Технічним комітетом стандартизації «Інформаційні технології» (ТК 20) за участю Технічного комітету стандартизації «Банківські та фінансові системи і технології» (ТК 105), Міжнародним науково-навчальним центром інформаційних технологій та систем НАН України та Міносвіти і науки України і затверджені наказами ДП «УкрНДНЦ».

Перелічені галузеві стандарти були внесені ТК 105 „Банківські та фінансові системи і технології", Державним підприємством „Український державний науково-дослідний інститут технологій товарногрошового обігу, фінансових і фондових ринків" (ДП „УКРЕЛЕКОН") і затверджені Постановами Правління Національного банку України.

ГСТУ СУІБ 1.0/ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)

Цей 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.

Система управління інформаційною безпекою забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам, що ризиками належним чином управляють. Важливо, щоб система управління інформаційною безпекою була частиною та інтегрувалася в процеси організації та загальну структуру управління, щоб інформаційну безпеку розглядали в процесах розроблення, інформаційних системах і заходах безпеки. Очікують, що впровадження системи управління інформаційною безпекою буде масштабованим відповідно до потреб організації.

Цей стандарт може бути використано зацікавленими внутрішніми та зовнішніми сторонами для оцінки можливості організації відповідати власним вимогам щодо інформаційної безпеки. Послідовність, з якою вимоги надано в цьому стандарті, не відображає їх важливості чи послідовності, з якою їх має бути впроваджено. Перелік пунктів понумеровано лише для цілей забезпечення посилань. ISO/IEC 27000 надає огляд і словник систем управління інформаційною безпекою з посиланням на сімейство стандартів щодо систем управління інформаційною безпекою (охоплюючи ISO/IEC 27003, ISO/IEC 27004 та ISO/IEC 27005) з пов’язаними термінами та визначеннями.

Стандарт використовує високорівневу структуру, ідентичні назви підрозділів, ідентичний текст, загальні терміни та основні визначення, які надано в додатку SL ISO/IEC Directives, Part 1, Consolidated ISO Supplement, тому підтримує сумісність з іншими стандартами систем управління, які визначено в додатку SL. Такий загальний підхід, визначений в додатку SL, буде корисним тим організаціям, що обирають застосування одній системі управління, яка забезпечує виконання вимог двох або більше стандартів систем управління.

ГСТУ СУІБ 1.0/ISO/IEC 27001:2015 визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації. Цей стандарт також містить вимоги для оцінювання та оброблення ризиків інформаційної

безпеки, пов’язаних з потребами організації. Вимоги, наведені в цьому стандарті, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи. Вилучення будь-якої з вимог, наведених в розділах 4-10 неприпустимо в разі, якщо організація прагне відповідати цьому стандарту [20].

ГСТУ СУІБ 2.0/ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою

Галузевий стандарт України СУІБ 2.0/ISO/IEC 27002:2015 є прийнятий зі змінами ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою).

Ціль стандарту СУІБ 2.0/ISO/IEC 27002:2015 забезпечити, що події інформаційної безпеки та слабкі місця, пов’язані з інформаційними системами, доведені до відома у спосіб, який дозволяє своєчасно вжити коригувальну дію.

Повинні бути наявними офіційно оформлені процедури звітування про події та ескалацію. Весь найманий персонал, контрактори і користувачі третьої сторони повинні бути проінформовані щодо процедур звітування про різні види подій та слабких місць, які можуть впливати на безпеку активів організації. Вони повинні бути зобов’язані якнайшвидше звітувати про будь-які події та слабкі місця інформаційної безпеки у визначену точку контакту.

Щодо звітування про події інформаційної безпеки, то слід зазначити, що треба якнайшвидше звітувати через належні канали управління.

Повинна бути розроблена офіційно оформлена процедура звітування про події інформаційної безпеки, а також процедури реагування та ескалації, де встановлено дії, яких треба вжити після отримання звіту про події інформаційної безпеки. Повинна бути встановлена контактна особа для звітування про подій інформаційної безпеки. Треба забезпечити, що ця контактна особа була відома у межах всієї організації, завжди доступна і здатна адекватно і своєчасно відреагувати [21].

Весь найманий персонал, контрактори і користувачів третьої сторони повинні бути поінформовані щодо своєї відповідальності якнайшвидше звітувати про будь-які події інформаційної безпеки. Вони також повинні бути

поінформовані щодо процедури звітування про події інформаційної безпеки і контактну особу. Процедури звітування повинні включати:

- відповідні процедури зворотного зв'язку для забезпечення того, щоб ті, хто звітував про події інформаційної безпеки, були сповіщені про результати після того, як проблему було оброблено й закрито;
- форми звітування про подію інформаційної безпеки для підтримування звітування і допомоги особі, що звітує, запам'ятати всі необхідні дії у разі події інформаційної безпеки;
- правильну поведінку, якої треба дотримуватися у разі події інформаційної безпеки, тобто:
- негайно записувати усі важливі подробиці (наприклад, тип невідповідності або порушення, збій, який мав місце, повідомлення на екрані, незвичайний режим роботи);
- не виконувати жодних власних дій, а негайно звітувати контактній особі;
- посилання на офіційно оформлений дисциплінарний процес поводження із найманим персоналом, контакторами і користувачами третьої сторони, які здійснили порушення безпеки [21].

У середовищі високого ризику може бути наданий сигнал щодо змушення, яким особа, яку примушують, може позначити такі проблеми. Процедури реагування на сигнал щодо змушення повинні відображати ситуацію високого ризику, яку позначають такі сигнали.

У стандарті [21] зазначені такі приклади подій та інцидентів інформаційної безпеки є:

- втрата послуги, обладнання або засобів обслуговування;
- збій або перевантаження системи;
- людські помилки;
- невідповідності політиці або настановам;
- порушення заходів фізичної безпеки;
- неконтрольовані зміни системи;
- збій програмного забезпечення або апаратних засобів;
- порушення доступу.

Щодо звітування слабких місць інформаційної безпеки, то треба вимагати від усього найманого персоналу, контракторів та користувачів третьої сторони, які користуються інформаційними системами та послугами, звертати увагу та звітувати щодо будь-яких спостережених або очікуваних слабких місць у системах чи послугах.

Ціллю управління інцидентами інформаційної безпеки та вдосконаленням є забезпечити застосування до управління інцидентами інформаційної безпеки послідовного та ефективного підходу.

Повинні бути наявними відповідальності та процедури ефективної обробки подій та слабких місць інформаційної безпеки одразу ж після звітування про них. До реагування, моніторингу, оцінювання та загального управління інцидентами інформаційної безпеки повинен застосовуватися процес безперервного вдосконалення.

Там, де потрібні докази, вони повинні бути зібрані, щоб забезпечити відповідність правовим вимогам.

В даному документі [21] при вивченні інцидентів інформаційної безпеки вказано, що при контролі повинні бути наявними механізми, які дозволяють визначати кількість і здійснювати моніторинг типів, обсягів та вартості інцидентів інформаційної безпеки.

Інформація, отримана від оцінювання інцидентів інформаційної безпеки, повинна використовуватися для ідентифікації інцидентів, які повторюються або мають великий вплив.

Оцінювання інцидентів ІБ може вказати на потребу в удосконалених або додаткових контролях для обмеження частоти, ушкодження та вартості майбутніх інцидентів або може бути взяте до уваги в процесі перегляду політики безпеки [21].

Висновки до першого розділу

Таким чином, правовий захист інформації забезпечується нормативно-правовими актами, сукупність яких за рівнем представляє ієрархічну систему від Конституції України, Законів України у сфері інформаційної безпеки та

захисту інформації, підзаконних та нормативних актів до функціональних обов'язків і контрактів конкретного виконавця, які визначають перелік відомостей, що підлягає охороні, і заходи відповідальності за їх розголошення.

Закони України "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про доступ до публічної інформації", "Про державну таємницю", "Про основні засади забезпечення кібербезпеки України" є основними законами, що регулюють питання забезпечення інформаційної безпеки та захисту інформації.

Технічний захист інформації займає особливо важливе місце в загальному комплексі заходів щодо забезпечення ІБ та призначений для забезпечення організаційними, інженерними та технічними заходами, методами і засобами конфіденційності, цілісності та доступності інформації, яка обробляється в ІТС, циркулює на підприємстві та становить державну та іншу встановлену законами таємницю. Вимоги щодо захисту інформації регулюють нормативні документи системи технічного захисту інформації (НД ТЗІ), які затверджує Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

Засади управління інформаційною безпекою визначають національні та галузеві стандарти України. Галузеві стандарти України, прийняті Національним банком України для регулювання засад забезпечення інформаційної безпеки установ банківської сфери, представлені ГСТУ ISO/IEC 27001:2015 «Інформаційні технології Методи захисту. Системи управління інформаційною безпекою. Вимоги” та ГСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”.

Зазначені стандарти створені на основі відповідних міжнародних стандартів серії ISO 27к і визначають вимоги до розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою.

Розділ 2
СИСТЕМА МІЖНАРОДНИХ СТАНДАРТІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Види міжнародних стандартів у сфері інформаційної безпеки та безпеки ІТ

Відповідно до міжнародних і національних стандартів забезпечення інформаційної безпеки в будь-якій компанії передбачає наступне:

• визначення цілей забезпечення інформаційної безпеки комп'ютерних систем;

• створення ефективної системи управління інформаційною безпекою (далі - СУІБ);

• розрахунок сукупності деталізованих якісних і кількісних показників для оцінки відповідності інформаційної безпеки поставленим цілям;

• застосування інструментарію забезпечення інформаційної безпеки і оцінки її поточного стану;

• використання методик управління безпекою, що дозволяють об'єктивно оцінити захищеність інформаційних активів і управляти інформаційною безпекою компанії.

Розглянемо найбільш відомі міжнародні стандарти з інформаційної безпеки та захисту інформації, які можуть бути використані в вітчизняних умовах.

Використання міжнародних і національних стандартів забезпечення інформаційної безпеки сприяє вирішенню наступних п'яти завдань:

- по-перше, визначення цілей забезпечення інформаційної безпеки комп'ютерних систем;

- по-друге, створення ефективної СУІБ;

- по-третє, розрахунок сукупності деталізованих не тільки якісних, а й кількісних показників для оцінки відповідності інформаційної безпеки заявленим цілям;

- по-четверте, застосування інструментарію забезпечення інформаційної безпеки і оцінки її поточного стану;

- по-п'яте, використання методик управління безпекою з обґрунтованою системою метрик і заходів забезпечення розробників інформаційних систем, що дозволяють об'єктивно оцінити захищеність інформаційних активів і управляти інформаційною безпекою компанії.

Починаючи з початку 80-х років, були створені десятки міжнародних і національних стандартів у галузі інформаційної безпеки, які в певній мірі доповнюють один одного [22].

Стандарт - це документ, що встановлює необхідні характеристики продукції, процесів її виробництва, експлуатації та зберігання, виконання робіт або надання послуг. Стандарт може ставити й інші вимоги - наприклад, до символіки або термінології.

Мета стандарту - забезпечення необхідного рівня якості товарів і послуг; єдиних характеристик товарів і послуг.

Залежно від статусу стандарти діляться на:

- міжнародні - прийняті міжнародною організацією зі стандартизації;
- регіональні - прийняті регіональною організацією зі стандартизації;
- національні - прийняті національним органом стандартизації;
- відомчі - прийняті органом стандартизації певного відомства.

Основними областями стандартизації ІБ є:

- управління ІБ;
- аудит ІБ;
- методи забезпечення ІБ;
- криптографія тощо (Рис.2.1.).

Стандартизація в області ІБ необхідна для вироблення:

1) вимог щодо ІБ;

2) підходів до вирішення проблем ІБ;

3) якісних показників для оцінки ІБ.

Рис. 2.1. Види стандартів з ІБ та області стандартизації.

Стандарти потрібні експертам з ІБ і фахівцям з сертифікації як інструмент для оцінки рівня ІБ.

Ключову роль у стандартизації з управління інформаційною безпекою відіграють декілька міжнародних організацій, серед яких насамперед варто згадати міжнародні організації зі стандартизації, що входять у структуру ООН:

- ISO (International Organization for Standardization - Міжнародна організація по стандартизації) - серії стандартів ISO;

- IEC (International Electrotechnical Commission - Міжнародна електротехнічна комісія) - серії стандартів IEC;

- ITU-T (International Telecommunication Union - Telecommunications - Міжнародний союз по телекомунікації) - стандарти серії X (мережі передачі даних, взаємозв'язок відкритих систем і безпеки).

Загалом міжнародні стандарти можна розділити на дві групи.

1 група - оціночні стандарти. Вони призначені для оцінки і класифікації ІС і засобів захисту інформації за вимогами безпеки. Ними керуються для того, щоб відповісти на питання: чи відповідає ІС і засоби захисту вимогам ІБ [23].

Перелік оціночних стандартів представлено в Таблиці 2.1.

Таблиця 2.1.

Оціночні стандарти з безпеки ІТ.

Назва стандарту	**Рік**	**Країна**
Критерії оцінки довіреної комп'ютерної системи (Trusted Computer System Evaluation Criteria, TCSEC)	1985	США
Критерії оцінки безпеки інформаційних технологій (Information Technology Security Evaluation Criteria, ITSEC)	1991	Франція, Німеччина, Великобританія, Нідерланди
Федеральні критерії безпеки інформаційної технології (Federal Criteria for Information Technology Security)	1993	США
Канадські критерії оцінки довіреної комп’ютерного продукту (Canadian Trusted Computer Product Evaluation Criteria)	1993	Канада
Загальні критерії безпеки інформацій ой технологи і (Common Criteria for Information Technology Security Evaluation, CCITSE)	1996	США, Канада, Франція, Великобританія, Нідерланди
Критерії оцінки безпеки інформаційній технології (Evaluation Criteria for Information Technology Security 15408)	1999	ISO / IEC

2 група - так звані специфікації. Вони регламентують різні питання реалізації та використання методів і засобів захисту інформації. Ними керуються для того, щоб відповісти на питання: як забезпечити ІБ, які підходи, методи і засоби необхідно для цього використовувати.

Перелік оціночних стандартів представлено в Таблиці 2.2.

Таблиця 2.2.

Стандарти, що описують специфікації ІБ

Назва стандарту	**Рік**	**Країна**	**Номер стандарту**
Архітектура безпеки для взаємодії відкритих систем (Security architecture for Open Systems Interconnection)	1991	ITU-T	X.800
Звід практичних правил УІБ (Code of Practice for Information Security Management)	1995	Великобританія	BS 7799
Звід практичних правил УІБ	2000	ISO / IEC	17799
СУІБ. Звід норм і правил УІБ	2005	ISO / IEC	27002
СУІБ. вимоги	2005	ISO / IEC	27001

Далі ми розглянемо більш докладно вище названі стандарти.

2.2 «Помаранчева Книга» (TCSEC)

Розробка і публікація «Помаранчевої книги» (Trusted Computer System Evaluation Criteria, TCSEC) стали важливою віхою в становленні теорії ІБ. Такі базові поняття, як «політика безпеки», «монітор безпеки звернень» або «адміністратор безпеки» вперше у відкритій літературі з'явилися саме в «Помаранчевій книзі».

Згідно з «Помаранчевою книгою» система повинна забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу.

Крім того, «Помаранчева книга» визначає 4 рівня довіреності (безпеки) ІС - D, C, B і A (по зростанню від D до A). Рівень D призначений для систем, визнаних незадовільними. З урахуванням нашої 5-бальної шкали оцінки, отримаємо такі рівні безпеки з оцінкою: 2 (D), 3 (C), 4 (B), 5 (A).

У міру переходу від рівня С до А до надійності систем пред'являються все більш жорсткі вимоги. Рівні С і В поділяються на класи (С1, С2, В1, В2, В3) з поступовим зростанням надійності. Таким чином, «Помаранчева книга» визначає 6 класів безпеки: С1, С2, В1, В2, В3, А1.

Необхідний рівень безпеки ІС зростає від групи D до групи А, а в межах однієї групи - зі збільшенням номера класу. Кожен клас характеризується певним фіксованим набором вимог до підсистеми забезпечення ІБ, реалізованої в ІС [24].

1. Група С - Discretionary Protection (виборчий захист) - об'єднує ІС, щоб забезпечити набір засобів захисту, що застосовуються користувачем, включаючи кошти загального контролю і обліку суб'єктів та їх дій.

Ця група має два класи:

1) клас С1 - Discretionary Security Protection (виборчий захист безпеки) - об'єднує ІС з поділом користувачів і даних;

2) клас С2 - Controlled Access Protection (захист контрольованого доступу) - об'єднує ІС, щоб забезпечити більш тонкі засоби захисту в порівнянні з ІС класу С1, що роблять користувачів індивідуально помітними в їх діях за допомогою процедур контролю входу та контролю за подіями, що зачіпають безпеку ІС і ізоляцію даних.

2. Група В - Mandatory Protection (повноважний захист) - має три класи:

1) клас В1 - Labeled Security Protection (меточного захист безпеки) - об'єднує ІС, що відповідають всім вимогам класу С2, додатково реалізують заздалегідь визначену модель безпеки, що підтримують мітки суб'єктів і об'єктів, повний контроль доступу. Вся видається інформація реєструється, всі виявлені при тестуванні недоліки повинні бути усунені;

2) клас В2 - Structured Protection (структурований захист) - об'єднує ІС, в яких реалізована чітко визначена і задокументована формалізована модель забезпечення безпеки, а міточний механізм поділу і контролю доступу, реалізований в системах класу В1, поширений на всіх користувачів, всі дані і всі види доступу. У порівнянні з класом В1 посилені вимоги щодо ідентифікації користувачів, контролю за виконанням команд керування, посилена підтримка адміністратора і операторів системи. Повинні бути проаналізовані і перекриті

всі можливості обходу захисту. ІС класу В2 вважаються «выдносно невразливими» для несанкціонованого доступу;

3) клас В3 - Security Domains (області безпеки) - об'єднує ІС, що мають спеціальні комплекси безпеки. В ІС цього класу повинен бути механізм реєстрації всіх видів доступу будь-якого суб'єкта до будь-якого об'єкту. Повинна бути повністю виключена можливість несанкціонованого доступу. Система безпеки повинна мати невеликий обсяг і прийнятну складність для того, щоб користувач міг у будь-який момент протестувати механізм безпеки. ІС цього класу повинні мати кошти підтримки адміністратора безпеки; механізм контролю повинен бути поширений аж до сигналізації про всі події, які зачіпають безпеку; повинні бути кошти відновлення системи. ІС цього класу вважаються стійкими до несанкціонованого доступу.

3. Група А - Verified Protection (перевірений захист) - об'єднує ІС, характерні тим, що для перевірки реалізованих в системі засобів захисту оброблюваної або інформації, що зберігається застосовуються формальні методи. Обов'язковою вимогою є повне документування всіх аспектів проектування, розробки і виконання ІС.

Виділено єдиний клас А1 - Verified Desing (перевірена розробка) - об'єднує системи, функціонально еквівалентні системам класу В3 і не потребують будь-яких додаткових коштів. Відмінною рисою ІС цього класу є аналіз формальних специфікацій проекту системи і технології виконання, що дає в результаті високу ступінь гарантованості коректного виконання ІС. Крім цього, системи повинні мати потужні засоби управління конфігурацією і засоби підтримки адміністратора безпеки [24].

Основний зміст вимог по класах безпеки приведено в таблиці 2.3.

Таблиця 2.3.

Класи вимог відповідно до "Помаранчевої книги"

Вимоги	**Класи**					
	C1	**C2**	**B1**	**B2**	**B3**	**A1**
1. Вимоги до політики безпеки						
1.1. Довільне керування доступом	+	+	=	=	+	=
1.2. Повторне використання об'єктів	-	+	=	=	=	=
1.3. Мітки безпеки	-	-	+	+	=	=
1.4. Цілісність міток безпеки	-	-	+	+	=	=
1.5. Примусове управління доступом	-	-	+	+	=	=
2. Вимоги до підзвітності						
2.1. Ідентифікація та аутентифікація	+	+	+	=	=	=
2.2. Надання надійного шляху	-	-	-	+	+	=
2.3. Аудит	-	+	+	+	+	=
3. Вимоги до гарантованості						
3.1. Операційна гарантованість						
3.1.1. Архітектура системи	+	+	+	+	+	=
3.1.2. Цілісність системи	+	=	=	=	=	=
3.1.3. Аналіз таємних каналів передачі інформації	-	-	-	+	+	+
3.1.4. Надійне адміністрування	-	-	-	+	+	=
3.1.5. Надійне відновлення	-	-	-	-	+	=
3.2. Технологічна гарантованість						
3.2.1. Тестування	+	+	+	+	+	+
3.2.2. Верифікація специфікацій архітектури	-	-	+	+	+	+
3.2.3. Конфігураційне управління	-	-	-	+	=	+
3.2.4. Надійне поширення	-	-	-	-	-	+
4. Вимоги до документації						
4.1. Керівництво користувача за засобами безпеки	+	=	=	=	=	=
4.2. Керівництво адміністратора за засобами безпеки	+	+	+	+	+	+
4. 3. Тестова документація	+	=	=	+	=	+
4.4. Опис архітектури	+	=	+	+	+	+

Позначення: «-» - немає вимог до даного класу;

«+» - нові або додаткові вимоги;

«=» - вимоги збігаються з вимогами попереднього класу.

Дуже важливий методологічний недолік «Помаранчевої книги» - явна орієнтація на виробника і оцінювача, а не на покупця систем. Вона не дає відповідь на питання, як безпечним чином будувати систему, як нарощувати окремі компоненти і конфігурацію в цілому. «Критерії» розраховані на статичні, замкнуті системи, які, ймовірно, домінують у військовому середовищі, але вкрай рідкісні в середовищі комерційної. Покупцям потрібні більш динамічні і структуровані критерії.

Проте слід підкреслити, що публікація «Помаранчевої книги» без жодного перебільшення стала епохальною подією в області захисту комерційних інформаційних систем. З'явився загальновизнаний понятійний базис, без якого навіть обговорення проблем безпеки було б скрутним. Саме в цьому бачиться головна цінність «Помаранчевої книги».

В даний час «Помаранчева книга» особливо не використовується для оцінки інформаційних систем і становить інтерес виключно з історичної точки зору.

2.3 Стандарт ISO / IEC 17799 «Управління інформаційною безпекою»

Міжнародний стандарт ISO / IEC 17799: 2000 (BS 7799-1:2000) «Управління інформаційною безпекою - Інформаційні технології» («Information technology - Information security management») є одним з найбільш відомих стандартів в області захисту інформації. Даний стандарт був розроблений на основі першої частини Британської стандарту BS 7799-1: 1995 «Практичні рекомендації з управління інформаційною безпекою» («Information security management - Part 1: Code of practice for information security management») і відноситься до нового покоління стандартів інформаційної безпеки комп'ютерних ІС.

Поточна версія стандарту ISO / IEC 17799: 2000 (BS 7799-1:2000) розглядає такі актуальні питання забезпечення інформаційної безпеки організацій та підприємств:

- необхідність забезпечення інформаційної безпеки;
- основні поняття і визначення інформаційної безпеки;
- політика інформаційної безпеки компанії;
- організація інформаційної безпеки на підприємстві;
- класифікація та управління корпоративними інформаційними ресурсами;
- кадровий менеджмент та інформаційна безпека;
- фізична безпека;
- адміністрування безпеки КІС;
- управління доступом;
- вимоги щодо безпеки до КІС в ході їх розробки, експлуатації і супроводу;
- управління бізнес-процесами компанії з точки зору інформаційної безпеки;
- внутрішній аудит ІБ.

Друга частина стандарту BS 7799-2 2000 «Специфікації систем управління інформаційною безпекою» («Information security management - Part 2: Specification for information security management systems»), визначає можливі функціональні специфікації корпоративних СУІБ з точки зору їх перевірки на відповідність вимогам першої частини даного стандарту [25].

Додаткові рекомендації для управління інформаційною безпекою містять керівництва Британського інституту стандартів - British Standards Institution (BSI), видані в 1995-2003 рр. у вигляді такої серії:

• «Введення в проблему управління інформаційною безпекою» («Information security managment: an introduction»);

• «Можливості сертифікації на вимоги стандарту BS 7799» («Preparing for BS 7799 sertification»);

• «Керівництво BS 7799 з оцінки та управління ризиками» («Guide to BS 7799 risk assessment and risk management»);

• «Керівництво для проведення аудиту на вимоги стандарту» («BS 7799 Guide to BS 7799 auditing»);

• «Практичні рекомендації з управління безпекою інформаційних технологій» («Code of practice for IT management»).

Відповідно до стандарту ISO / IEC 17799 основна увага при проектуванні і створенні ефективної системи безпеки організації приділяється комплексному підходу до управління ІБ, яке повинно здійснюватися із застосуванням технічних і організаційних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, що захищається. Порушення будь-якого з цих принципів може привести як до незначних збитків організації, так і до її банкрутства.

З метою формування комплексних вимог до безпеки інформації стандарт визначає три основні показники:

- оцінка ризиків, з якими стикається організація (визначення загрози для ресурсів, їх вразливість і ймовірність виникнення загроз, а також можливу шкоду);
- дотримання законодавчих, нормативних та договірних вимог, які повинні виконуватися самою організацією, її партнерами по бізнесу, підрядниками та постачальниками послуг;
- формування комплексу принципів, цілей і вимог до обробки інформації, розроблених організацією для підтримки своєї діяльності.

Оцінка ризиків повинна допомогти визначити необхідні дії і пріоритети для управління ІБ і для реалізації обраних засобів захисту. Процес оцінки ризиків та вибору засобів захисту може виконуватися кілька разів, щоб охопити різні частини організації або окремі інформаційні системи. Засоби захисту повинні вибиратися з урахуванням витрат на реалізацію. При цьому витрати повинні відповідати ступеню ризиків і потенційним збитків при порушенні безпеки. З метою визначення необхідного рівня захисту інформаційних ресурсів повинні бути складені їх переліки та проведена класифікація інформації за рівнями конфіденційності.

Крім технічної реалізації засобів захисту інформації на основі результатів оцінки ризиків та обраного рівня захисту повинні бути розроблені організаційні заходи забезпечення ІБ, які повинні включати в себе наступні положення:

- розробка політики ІБ;

- розподіл відповідальності;
- навчання та підготовка персоналу;
- створення звітів про інциденти;
- підтримка безперервності бізнесу.
- визначення ІБ, її цілей і області дії;
- загальний опис принципів управління ІБ;
- короткий опис політики безпеки, принципів, стандартів, вимог;
- опис обов'язків, правила розподілу відповідальності;
- посилання на більш детальні інструкції та описи правил безпеки.

Практична організація ІБ

У розділах стандарту ISO / IEC 17799, представлених нижче, наведено практичні рекомендації щодо організації ІБ, які, як правило, відображаються в політиці безпеки організації або в окремих інструкціях з урахуванням специфіки самої організації.

1. Питання безпеки, пов'язані з персоналом
- Безпека при формулюванні завдань і набір співробітників.
- Навчання користувачів.
- Реакція на інциденти і збої в роботі.

2.Фізична безпека і захист територій
- Захищені території.
- Безпека обладнання.
- Загальні заходи.

3.Забезпечення безпеки при експлуатації
- Правила роботи та обов'язки.
- Планування розробки і приймання системи.
- Захист від зловмисного програмного забезпечення.
- Службові процедури.
- Управління обчислювальними мережами.
- Звернення з носіями і їх безпеку.
- Обмін інформацією та програмним забезпеченням.

4. Контроль доступу
- Вимоги до контролю доступу в організації.

- Управління доступом користувачів.
- Обов'язки користувачів.
- Контроль доступу до обчислювальної мережі.
- Контроль доступу до операційних систем.
- Контроль доступу до додатків.
- Моніторинг доступу та використання системи.
- Мобільні комп'ютери і засоби віддаленої роботи.

5.Розробка і обслуговування систем

- Вимоги до безпеки систем.
- Безпека в прикладних системах.
- Криптографічні засоби.
- Безпека системних файлів.
- Безпека при розробці та підтримці.

6. Забезпечення безперервності бізнесу

- Аспекти забезпечення безперервності бізнесу.

7. Відповідність вимогам

- Відповідність вимогам законодавства.
- Перевірка політики безпеки і відповідність технічним вимогам.

Вимоги безпеки інформації повинні враховуватися у всіх сферах життєдіяльності організації, в тому числі при формуванні та розподілі посадових обов'язків. Крім того, посадові обов'язки користувачів інформаційних ресурсів повинні містити більш конкретизовані і розширені (в порівнянні з викладеними в загальній політиці безпеки організації) вимоги до забезпечення безпеки інформації. Всі співробітники організації повинні проходити відповідну підготовку в області політики безпеки і процедур, прийнятих в організації з періодичної перепідготовкою [25].

2.4 Стандарт ISO / IEC 15408 «Загальні критерії»

Розробці «Загальних критеріїв» передувала розробка документа «Критерії оцінки безпеки інформаційних технологій» (англ. Evaluation Criteria

for IT Security, ECITS), розпочата в 1990 році, і виконана робочою групою 3-го підкомітету 27 першого спільного технічного комітету (або JTC1 / SC27 / WG3) Міжнародної організації зі стандартизації (ISO).

Даний документ послужив основою для початку роботи над документом Загальні критерії оцінки безпеки інформаційних технологій (англ. Common Criteria for IT Security Evaluation), розпочатої в 1993 році. У цій роботі брали участь урядові організації шести країн (США, Канада, Німеччина, Великобританія, Франція, Нідерланди).

Стандарт був прийнятий у 2005 році комітетом ISO і має статус міжнародного стандарту, ідентифікаційний номер ISO / IEC 15408.

Критерії призначені служити основою при оцінці характеристик безпеки продуктів і систем IT. Закладені в стандарті набори вимог дозволяють порівнювати результати незалежних оцінок безпеки. На підставі цих результатів споживач може приймати рішення про те, чи достатньо безпечні IT-продукти або системи для їх застосування з заданим рівнем ризику.

Стандарт встановлює основні поняття і принципи оцінки безпеки IT, а також визначає загальну модель оцінки, якої присвячені різні частини стандарту, призначеного в цілому для використання в якості основи при оцінці характеристик безпеки продуктів IT. Стандарт ISO / IEC 15408 складається з трьох частин [31].

Частина 1 «Введення і загальна модель» встановлює загальний підхід до формування вимог безпеки й оцінки безпеки, на їх основі розробляються основні конструкції (профіль захисту та завдання з безпеки) уявлення вимог безпеки в інтересах споживачів, розробників і оцінювачів продуктів і систем IT. Вимоги безпеки об'єкта оцінки (далі – ОО) за методологією стандарту визначаються, виходячи з цілей безпеки, які ґрунтуються на аналізі призначення ОО і умов середовища його використання (загроз, політики безпеки).

Частина 2 «Функціональні вимоги безпеки» містить універсальний каталог функціональних вимог безпеки (далі – ФВБ) і передбачає можливість їх деталізації і розширення за певними правилами.

Частина 3 «Компоненти довіри до безпеки »включає в себе систематизований каталог вимог довіри, що визначають заходи, які повинні бути прийняті на всіх етапах життєвого циклу продукту або системи ІТ для забезпечення впевненості в тому, що вони задовольняють пред'явленим до них функціональним вимогам. Тут же містяться оціночні рівні довіри, що визначають шкалу вимог, які дозволяють зі зростаючою ступенем повноти і строгості оцінити проектну, тестову і експлуатаційну документацію, правильність реалізації функцій безпеки ОО, уразливості продукту або системи ІТ, стійкість механізмів захисту і зробити висновок про рівень довіри до безпеки об'єкту оцінки.

Узагальнюючи вищесказане, можна відзначити, що каркас безпеки, закріпленний частиною 1 стандарту, заповнюється змістом з класів, сімейств і компонентів в частині 2, а частина 3 визначає, як оцінити міцність всієї «будови» [32].

2.5 Стандарти серії ISO/IEC 27000 щодо системи управління інформаційною безпекою

В даний час існує досить багато міжнародних стандартів, а також інших нормативних і керівних документів в області ІБ. Розглянемо сімейство стандартів ISO 27к, якими керуються при створенні, сертифікації та експлуатації СУІБ.

Сформована на даний час серія стандартів стосовно управління інформаційною безпекою представлена на рис. 2.2.

Головною метою СУІБ є забезпечення сталого функціонування підприємства, запобігання загрозам безпеки, захист його законних інтересів від протиправних посягань, недопущення розкрадання фінансових коштів, розголошення, втрати, витоку, перекручування та знищення службової інформації, забезпечення нормальної виробничої діяльності усіх підрозділів. Іншою метою СУІБ є підвищення якості надаваних послуг і гарантій безпеки майнових прав та інтересів клієнтів [26].

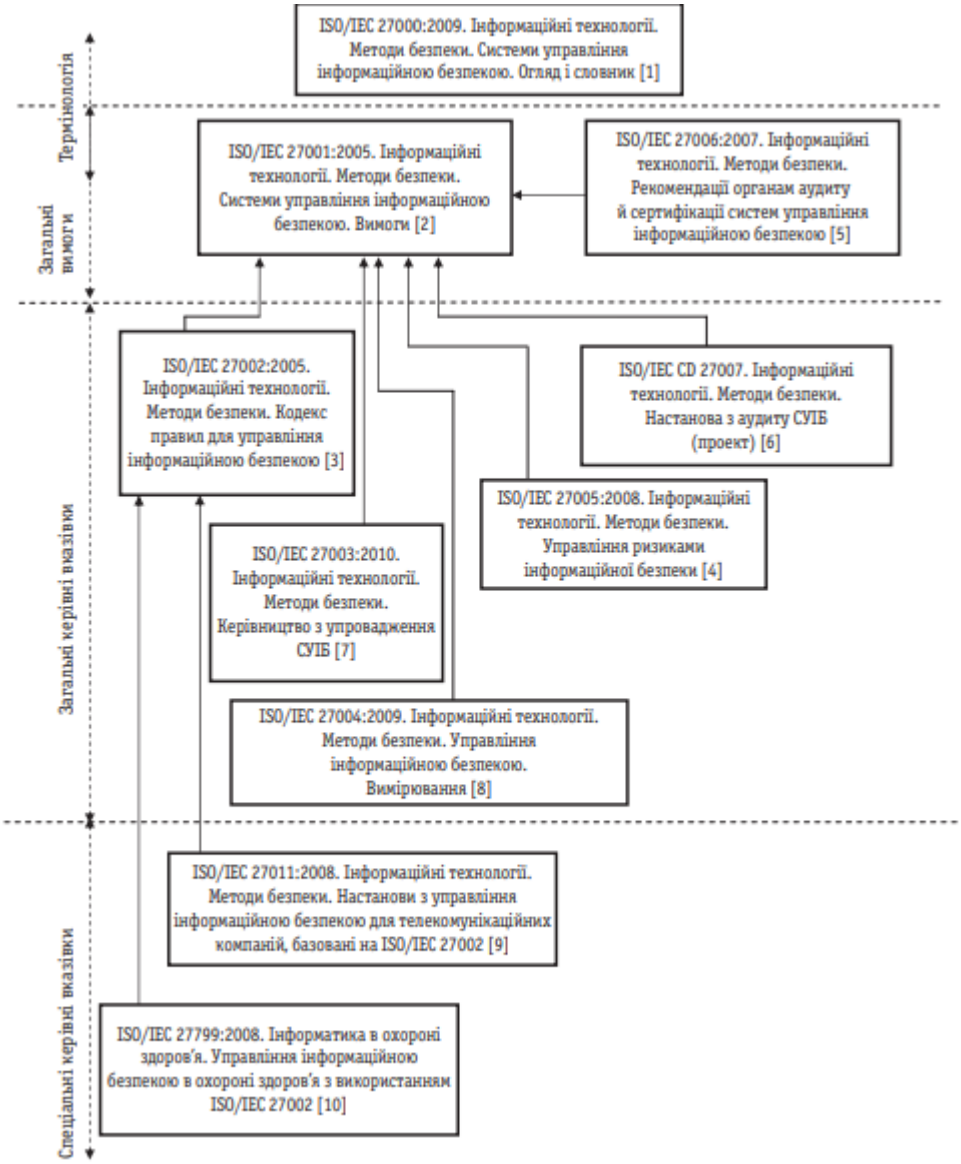

Рис. 2.2. Стандарти серії ISO/IEC 27000 стосовно СУІБ

Досягнення заданих цілей можливе за умови дотримання основних принципів:

- усвідомлення необхідності захисту інформації;
- визначення відповідальності за захист інформації;
- об'єднання зобов'язань стосовно управління та інтересів акціонерів;
- підвищення соціальних цінностей;
- оцінення ризику, яке визначає застосування відповідних засобів управління для досягнення прийнятних рівнів ризику;
- акцент на безпеку, що є істотним елементом інформаційних мереж і систем;

- активне запобігання та виявлення порушень захисту інформації;
- забезпечення всебічного підходу до управління захистом інформації;
- постійне переоцінення захисту інформації тавнесення необхідних змін.

Стандарти з управління інформаційною безпекою ISO 27 к дозволяють підприємствам та організаціям:

- оптимізувати вартість побудови та підтримання системи інформаційної безпеки; постійно відслідковувати та оцінювати ризики з урахуванням цілій бізнесу;
- ефективно виявляти найбільш критичні ризики та знижувати ймовірність їх реалізації;
- розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання;
- ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу;
- забезпечити розуміння питань інформаційної безпеки керівництвом та всіма працівниками банку;
- забезпечити підвищення репутації та ринкової привабливості банків;
- знизити ризики рейдерських та інших шкідливих атак тощо (рис. 2.3.).

Однак, наведені вище переваги не будуть досягнуті шляхом лише “формального” підходу до розроблення, впровадження та функціонування системи управління інформаційною безпекою, необхідно, щоб керівництво і працівники були теж зацікавлені в підвищенні рівня інформаційної безпеки.

Стандарт	Опис
1. Серія ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою»	
ISO/IEC 27000:2009	Визначення і основні принципи
ISO/IEC 27001:2005	Інформаційні технології — Методики безпеки — Системи менеджменту інформаційної безпеки — Вимоги (BS 7799-2:2005)
ISO/IEC 27002:2005	Інформаційні технології — Методики безпеки — Практичні правила управління інформаційною безпекою (попередній код ISO/IEC 17799:2005
ISO/IEC 27003:2010	Настанова з впровадження системи управління інформаційною безпекою
ISO/IEC 27005:2008	Інформаційні технології — Методики безпеки — Управління ризиками інформаційної безпеки (на основі стандарту BS 7799-3:2006)
ISO/IEC 27006:2007	Інформаційні технології — Методики безпеки — Вимоги до організацій, що провадять аудит і сертифікацію систем менеджменту інформаційної безпеки
ISO/IEC 27011:2008	Керівництво з менеджменту інформаційної безпеки для телекомунікацій
ISO/IEC 15408	Загальні критерії оцінки безпеки інформаційних технологій
2. Серія ISO 13335 «Міжнародні стандарти безпеки інформаційних технологій»	
ISO 13335-1:2004	Інформаційні технології — Керівництво по управлінню IT безпекою — Концепції і моделі для управління безпекою інформаційних і телекомунікаційних технологій
ISO 13335-3:1998	Інформаційні технології — Керівництво по управлінню IT безпекою — Методи управління IT безпекою
ISO 13335-4:2000	Інформаційні технології — Керівництво по управлінню IT безпекою — Вибір механізмів захисту
ISO 13335-5:2001	Інформаційні технології — Керівництво по управлінню IT безпекою — Керівництво по управлінню мережевою безпекою

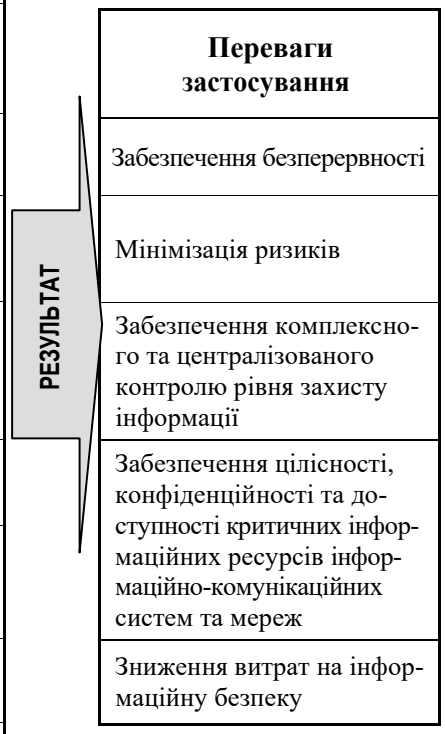

Рис. 2.3. Переваги застосування міжнародних стандартів серії ISO 27к.

Можна виділити 4 види груп стандартів, присвячених СУІБ:

• Стандарти для огляду і введення в термінологію

• Стандарти, які визначають обов'язкові вимоги до СУІБ

• Стандарти, що визначають вимоги і рекомендації для аудиту СУІБ

• Стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення СУІБ.

Стандарти для огляду і введення в термінологію:

ISO / IEC 27000 2009 - Інформаційні технології. Засоби забезпечення безпеки. Системи менеджменту інформаційної безпеки. Огляд і словник

Даний стандарт забезпечує визначення основної термінології, яка використовується в стандартах з інформаційної безпеки. У кожному стандарті є і додаткові терміни. В даний момент розробляється нова версія стандарту ISO 27000.

Стандарти, які визначають обов'язкові вимоги до СУІБ:

ISO / IEC 27001: 2005 - Інформаційні технології. Методи і засоби забезпечення безпеки. Системи менеджменту інформаційної безпеки. вимоги

Це основний стандарт групи. Він визначає вимоги до розробки, впровадження, підтримки і поліпшення систем менеджменту інформаційної безпеки.

Стандарти, що визначають вимоги і рекомендації для аудиту СУІБ:

ISO / IEC 27006: 2011 - Інформаційні технології. Засоби забезпечення безпеки. Вимоги для органів, що виконують аудит та сертифікацію систем менеджменту інформаційної безпеки

Цей стандарт розширює вимог стандарту ISO 17021 спеціально для органів, які проводять аудит і сертифікацію СУІБ

ISO / IEC 27007: 2011 - Інформаційні технології. Засоби забезпечення безпеки. Настанови для аудиту систем менеджменту інформаційної безпеки.

Стандарт ISO 27007 пропонує рекомендації з проведення аудитів СУІБ з боку сертифікаційних організацій. Він корисний для аудиторів цих організацій.

ISO / IEC TR 27008: 2011 - Інформаційні технології. Методи забезпечення безпеки - Керівництво для аудиторів щодо заходів і засобів забезпечення інформаційної безпеки

Даний стандарт, як і ISO 27007 є додатковим стандартом до ISO 19011: 2011 спеціально для СУІБ. Він спеціалізований для аудиту коштів управління інформаційною безпекою в організації

Стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення СУІБ:

ISO / IEC 27002: 2005 - Інформаційні технології. Засоби забезпечення. Звід практики для менеджменту інформаційної безпеки

Найпопулярніший стандарт групи після ISO 27001. Він дає відмінні вказівки для розробки, впровадження, підтримки і вдосконалення СУІБ. Його можна назвати «Біблією» для консультантів.

ISO / IEC 27003: 2010 рік - Інформаційні технології. Керівництво по здійсненню системи менеджменту інформаційної безпеки

Стандарт дає вказівки і методику для процесів розробки і впровадження СУІБ.

ISO / IEC 27004 2009 - Інформаційні технології. Засоби забезпечення безпеки. Вимірювання менеджменту інформаційної безпеки

Стандарт є керівництвом для вибору, проектування, управління і поліпшення засобів і методів вимірювання ефективності та результативності системи

ISO / IEC 27005: 2011 - Інформаційні технології. Методи захисту. Менеджмент ризиків інформаційної безпеки.

Цей стандарт є одним з найважливіших в групі. Незважаючи на те, що він тільки вказівний, а не обов'язковий стандарт, його призначення полягає в тому, що управління ризиками - один з найважливіших процесів для інформаційної безпеки.

ISO / IEC 27011: 2010 рік - Інформаційні технології. Засоби забезпечення безпеки. Настанови щодо менеджменту інформаційної безпеки для телекомунікацій на основі ISO / IEC 27002

Це спеціалізоване керівництво по СУІБ в телекомунікаційних організаціях.

ISO / IEC 27031: 2011 - Інформаційні технології - Методи забезпечення захисту - Керівництво для готовності інформаційних і комунікаційних технологій щодо забезпечення безперервності бізнесу.

Стандарт - керівництво щодо забезпечення безперервності бізнесу в ІКТ

ISO / IEC 27033-1 2009 - Інформаційні технології - Методи забезпечення захисту - Мережева безпека - Част 1 - Огляд і поняття

Перший з групи спеціалізованих стандартів в галузі забезпечення інформаційної безпеки мережевої інфраструктури

ISO / IEC 27033-3: 2010 рік - Інформаційні технології - Методи забезпечення захисту - Мережева безпека - Част 3 - Мережеві сценарії - Загрози, методи проектування та управління питаннями

Інший стандарт з групи спеціалізованих стандартів в галузі забезпечення інформаційної безпеки мережевої інфраструктури - з практичним значенням.

ISO / IEC 27034-1: 2011 - Інформаційні технології - Методи забезпечення захисту - Безпека додатків - Част 1: Огляд та поняття

Перший з іншої групи спеціалізованих стандартів в галузі забезпечення інформаційної безпеки прикладного програмного забезпечення.

ISO / IEC 27035: 2011 - Інформаційні технології - Методи забезпечення захисту - Управління інцидентами з інформаційної безпеки

Один з цінних стандартів в групі з практичною цінністю в галузі управління інцидентами з інформаційної безпекою

ISO 27799 2008 - Інформатика в охороні здоров'я. Менеджмент безпеки інформації за стандартом ISO / IEC 27002

Це спеціалізоване керівництво по СУІБ в охороні здоров'я.

ISO / IEC 24762 2008 - Інформаційні технології - Методи забезпечення захисту - Рекомендації по послугах для аварійного відновлення інформаційних і комунікаційних технологій

Стандарт має цінність з точки зору практичних рекомендацій щодо забезпечення аварійного відновлення ІКТ

Група стандартів ISO 27000 отримала дуже серйозний розвиток в останні роки. В даний час в різних стадіях підготовки знаходяться ще 25 нових стандартів, які забезпечать необхідну допомогу при розробці, впровадженні, підтримці і поліпшенні СУІБ.

Висновки до другого розділу

Ключову роль у стандартизації з управління інформаційною безпекою відіграють такі міжнародні організації, як Міжнародна організація по стандартизації, Міжнародна електротехнічна комісія та Міжнародний союз телекомунікації.

Встановлено, що основою для більшості стандартів стала так звана «Помаранчева книга», що встановлює базові вимоги щодо контролю комп'ютерної безпеки вбудованої в обчислювальну систему. Розробка і публікація «Помаранчевої книги» стали важливою ланкою в становленні теорії інформаційної безпеки. Такі базові поняття, як «політика безпеки», «монітор безпеки звернень» або «адміністратор безпеки» вперше у відкритій літературі з'явилися саме в «Помаранчевої книзі».

Розглянуто положення міжнародних стандартів серії ISO / IEC 27000, що включає стандарти з управління інформаційною безпекою, опубліковані спільно Міжнародною Організацією по Стандартизації (ISO) і Міжнародною Електротехнічною Комісією (IEC).

Умовно усі стандарти ISO / IEC 27000 можна поділити на такі групи: стандарти для огляду і введення в термінологію; стандарти, які визначають обов'язкові вимоги до СУІБ; стандарти, що визначають вимоги і рекомендації для аудиту СУІБ; стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення СУІБ.

Серія містить кращі практики і рекомендації в області інформаційної безпеки для створення, розвитку та підтримки СУІБ та визначає вимоги до СУІБ, управління ризиками, метрики і вимірювання, а також керівництво по впровадженню.

Розділ 3
ДОСЛІДЖЕННЯ ТА ВПРОВАДЖЕННЯ СТАНДАРТУ COBIT

3.1 Огляд стандарту COBIT

COBIT - підхід до управління інформаційними технологіями, створений асоціацією контролю і аудиту систем (Information Systems Audit and Control Association - ISACA) і інститутом керівництва IT (IT Governance Institute - ITGI) в 1992 році. Він надає менеджерам, аудиторам і IT користувачам набір затверджених метрик, процесів і кращих практик з метою допомогти їм в отриманні максимальної вигоди від використання інформаційних технологій і для розробки відповідного керівництва і контролю IT в компанії[35]. Перша редакція COBIT побачила світ в 1996 році.

Ключові галузі управління IT**:**

- Відповідність стратегії робить акцент на зв'язку між планами бізнесу та IT; виявленні, підтримки і контролі за ціннісним пропозицією IT; а також на відповідність IT та бізнес операцій.
- Корисність являє собою реалізацію ціннісного пропозиції, контроль за тим, щоб IT забезпечували певні стратегією переваги, зосередження на оптимізації витрат і підтвердження справжньої цінності IT.
- Управління ресурсами присвячено питанням, пов'язаним з управлінням критичними IT ресурсами, а саме, оптимізацією інвестицій та належного керівництва додатками, інформацією, інфраструктурою і персоналом. Ключові питання стосуються оптимізації знань та інфраструктури.
- Управління ризиками вимагає обізнаності вищого керівництва в області ризиків, чіткого розуміння корпоративного підходу в їх відношенні, відповідності вимогам прозорості щодо істотних ризиків, включення функції або системи управління ризиками в практику організації.

- Оцінка ефективності являє собою контроль за реалізацією стратегії, результатами проектів, використанням ресурсів, ефективністю процесів і сервісним обслуговуванням. Для цього застосовуються, зокрема, системи збалансованих показників, які перетворять стратегію в послідовність дій, результати яких вимірюються іншими, в порівнянні з бухгалтерським обліком, методами.

Концепція стандарту передбачає побудову механізмів управління IT виходячи з того, яка інформація необхідна для досягнення бізнес-цілей. При цьому інформація розглядається якрезультат використання IT ресурсів, управління якими здійснюється в рамках IT процесів . IT ресурси включають в себе додатки, інформацію (дані в будь-якій формі), інфраструктуру, персонал.

Для досягнення цілей бізнесу інформація повинна задовольняти певним критеріям, які в стандарті COBIT називають бізнес-вимогами до інформації. Виділяють наступні бізнес-вимоги до інформації або інформаційні критерії: ефективність, раціональність, конфіденційність, цілісність, доступність, відповідність нормам і надійність інформації. Механізми управління включають в себе політики, організаційні структури, процедури і регламенти. Завданням управління IT є формулювання бажаного результату або мети, які повинні бути досягнуті шляхом реалізації механізмів управління в рамках конкретного IT процесу.

Концептуальне ядро стандарту COBIT сформовано з 34 високорівневих процесів (які покривають близько 200 цілей контролю), згрупованих в 4 домена (сфери діяльності) [35]:

Планування і організація: включає стратегію і тактику, а також визначення способів найбільш ефективного використання IT для досягнення бізнес-цілей.Регламентовані процеси:

- PO1. Розробка стратегічного плану

- PO2. Визначення IT архітектури
- PO3. Визначення напрямків розвитку технологій
- PO4. Формалізація IT процесів, організації та взаємовідносин з бізнесом
- PO5. Управління інвестиціями в IT
- PO6. Узгоджене управління цілями і завданнями
- PO7. Управління IT персоналом
- PO8. Управління якістю
- PO9. Оцінка і управління ризиками IT
- PO10. Управління проектами

Придбання та впровадження: для реалізації IT стратегії потрібно ідентифікувати, розробити або придбати відповідні IT рішення, які повинні бути впроваджені і інтегровані в бізнес-процеси, а також внести зміни в інформаційні системи. Регламентовані процеси:

- AI1. Ідентифікація та вибір рішень по автоматизації
- AI2. Проектування і розробка додатків
- AI3. Проектування і підтримка технічної інфраструктури
- AI4. Забезпечення роботи і використання IC
- AI5. Закупівля IT ресурсів
- AI6. Управління змінами
- AI7. Установка і затвердження рішень і змін

Надання та підтримка: включає надання необхідних інформаційних служб, в тому числі забезпечення безпеки і безперервності бізнесу, навчання, а також обробку даних прикладними системами. Регламентовані процеси:

- DS1. Визначення та управління рівнями сервісу
- DS2. Управління сервісами підрядників
- DS3. Управління продуктивністю і потужністю
- DS4. Забезпечення безперервності сервісів
- DS5. Забезпечення безпеки систем

- DS6. Визначення і розподіл IT витрат
- DS7. Навчання користувачів
- DS8. Управління службою підтримки і інцидентами
- DS9. Управління конфігурацією
- DS10. Управління проблемами
- DS11. Управління даними
- DS12. Управління фізичним обладнанням
- DS13. Управління експлуатацією

Моніторинг та оцінка: якість і відповідність IT процесів вимогам контролю повинні оцінюватися на регулярній основі. Цей домен включає в себе нагляд з боку керівництва за процесами управління в організації, а також незалежний контроль з боку внутрішніх і зовнішніх аудиторів. Регламентовані процеси:

- ME1. Відстежувати й оцінювати продуктивність IT
- ME2. Відстежувати й оцінювати внутрішні контролі
- ME3. Гарантувати відповідність регулюючим вимогам
- ME4. Забезпечувати керівництво IT

Домени співвідносяться з традиційними сферами відповідальності IT: планування, впровадження, експлуатація та моніторинг. Така структура охоплює всі аспекти управління і використання IT. Виконання всіх 34 високорівневих процесів дозволяє гарантувати власнику бізнес-процесу, що система управління IT є адекватною завданням бізнесу.

У стандарті COBIT детально описано цілі і принципи управління, об'єкти управління, чітко визначені всі IT процеси (для кожного процесу визначені входи і виходи, виконавці та відповідальні, а також об'єкти контролю та метрики) і вимоги до них, описаний можливий інструментарій (практики) для їх реалізації. В описі IT процесів також наведені практичні рекомендації з управління IT безпекою. COBIT застосовується для контролю і аудиту існуючої системи управління інформаційними технологіями, організації оперативного і

стратегічного управління IT, аналізу витрат на IT проекти та підтримку відповідної інфраструктури, відповідності вимогам стандартів і регулюючим організаціям, таких як SOX і COSO.

За допомогою використання стандарту COBIT керівники IT підрозділів перетворять завдання бізнесу в чіткі і зрозумілі плани розвитку IT. Основною перевагою стандарту COBIT є його повнота і виразні практичні рекомендації та інструменти, за допомогою яких можна побудувати систему управління інформаційними технологіями корпорації і, в тому числі, ефективну систему управління ризиками в IT. Таким чином, при використанні методології COBIT інформаційна система будується виходячи з вимог бізнесу і умов жорсткої економії ресурсів, а також ефективного використання цих ресурсів. Іншими словами, стандарт COBIT описує бізнес-орієнтований підхід до створення інформаційного середовища: IT розглядаються в вигляді інструменту бізнесу, а стандарт визначає принципи побудови та організації роботи IT департаменту.

3.1.1 Моделі зрілості

Управління IT - складова частина успіху в управлінні підприємством, яка гарантує раціональне і ефективне вдосконалення всіх взаємопов'язаних процесів підприємства. Управління IT надає основу, яка пов'язує IT-процеси, IT-ресурси і інформацію із стратегією та цілями установи, що дозволяє максимально ефективно використати інформацію, при цьому підвищивши капіталізацію і отримуючи конкурентоспроможні переваги.

Принципи управління створені для того, щоб допомогти керівнику IT відповісти на три стратегічних питання:

1. Чи існують зараз в організації інформаційні технології, при керуванні якими "задовольняються" всі інформаційні потреби організації?
2. Як організація забезпечує інфраструктуру та керує ризиками, наскільки організація залежить від цього?

3. З якими проблемами організація стикається при управлінні IT?

Щоб отримати відповіді на ці стратегічні питання необхідно безперервно відповідати на "тактичні" питання:

• Що є результатом IT-процесів?

• Що є рішенням проблем в IT?

• З чого складаються ці рішення?

• Чи будуть працювати ці рішення?

• Як їх реалізувати?

Для отримання відповідей на "тактичні" питання до принципів управління CobiT, включені такі розділи як моделі зрілості, критичні фактори успіху (КФУ), ключові індикатори цілі (КІЦ) і ключові показники результату (КПР), це доповнення дало змогу отримати якісно покращений підхід до питань управління IT, який відповідає потребам керівників в частині управління і контролю.

Моделі зрілості в стандарті CobiT призначаються для контролю над IT-процесами в установі. Вони базуються на визначені ступеню розвитку компанії від неіснуючої до оптимізованої (від 0-го до 5-го рівня моделі зрілості). Цей підхід був привнесений в CobiT з Моделей Зрілості, розроблених Інститутом проектування і розробки програмного забезпечення (Software Engineering Institute), створених для оцінки рівня зрілості розробки програмного забезпечення.

Моделі зрілості не підказують як поліпшити роботу компанії і не пояснюють, як працювати з персоналом, також немає готових посібників і по застосуванню моделей зрілості. Рекомендується для кожної компанії розробити подібне керівництво для свого бізнесу або запросити сторонніх консультантів для вирішення цього питання. Моделі зрілості призначені для організації ефективного управління. Вони визначають ключові дії, які

вказують, що треба зробити для досягнення необхідної якості і містять способи контролю над правильністю виконання ключових IT-процесів і методи їх коригування. Ключові дії детально описані в Керівництві на абстрактному рівні, а в процесі використання моделей зрілості компанія може вибрати довільний ступінь їх формалізації.

Шкала моделей зрілості[35]:

0. Система управління безпекою не створена. Повністю відсутні будь-які процеси управління IT. Організація не визнає факт існування проблем в IT, які треба вирішувати, а отже немає ніяких відомостей про проблеми.

1. Початок. Організація визнала існування проблем в управлінні IT та необхідність вирішувати їх. При цьому не створено ніяких стандартизованих рішень. Є випадкові рішення, прийняті кимось персонально або випадково. Підхід керівництва щодо вирішення проблем в IT хаотичний, визнання наявності проблем випадкове і непослідовне.

2. Повторення. Є загальне усвідомлення наявності проблем в управлінні IT. Показники діяльності та IT-процесів розвиваються, охоплюючи при цьому процеси планування, функціонування та моніторингу за IT. Дії з управління інформаційними технологіями описані та інтегровані в процес управління установою. Вибрані для покращення та/або контролю такі IT-процеси, які можуть вплинути на основні бізнес-процеси в підприємстві. Ефективно здійснюється планування і управління інвестиціями. Керівництво організації регламентувало заходи з управління IT і методи з управління та оцінки, але процес не було прийнято в установі. Вся відповідальність покладена на співробітників. Вони повинні контролювати процеси управління з використанням проектів та IT-процесів. Вибрано і впроваджено обмежені інструменти для відбору метрик управління, але їх не вдається використати в повному обсязі, бо є недоліки в оцінці їх функціональності.

3. Опис (Стандартизація). Необхідність діяти у відповідності до принципів управління ІТ усвідомлена керівництвом і впроваджується. У розвитку знаходиться базовий набір показників управління ІТ: є визначеним зв'язок між результатами та показниками продуктивності, він зафіксований та впроваджений в стратегічні процеси при плануванні та моніторингу. Процедури стандартизовані і задокументовані, проводиться навчання працівників щодо виконання цих процедур. Показники продуктивності всіх видів діяльності зафіксовано і їх значення відслідковуються, що в результаті призводить до підвищення ефективності функціонування всієї компанії. Процедури самі по собі не складні, вони являються формалізацією існуючої в компанії практики. Відповідальними за вивчення, виконання та використання стандартів покладено на робітників організації. Більшість процесів працюють відповідно до деяких основних метрик, і, як правило, контролюються окремими співробітниками, тому про деякі відхиленнях керівництво може не знати. Проте загальна звітність щодо виконання ключових процесів є доволі чіткою, і керівництво може заохочувати співробітників на основі оцінки ключових результатів.

4. Управління. Є повне розуміння проблем в управлінні ІТ на всіх рівнях компанії, постійно відбувається підвищення рівня кваліфікації співробітників. Угоди щодо рівня обслуговування визначено і вони підтримуються в актуальному стані. Є чітке розподілення відповідальності, встановлено рівень володіння процесами. В першу чергу покращення в процесах управління ІТ ґрунтуються на вимірюваних кількісних показниках. Є можливість керувати процедурами та метриками процесів, проводити вимірювання їх відповідності. Керівництвом організації визначено допустимі відхилення, за яких процеси мають продовжувати працювати. Процеси постійно вдосконалюються, їх результати відповідають "найкращим практикам". Формалізований порядок аналізу першопричин. Присутнє розуміння необхідності постійного

вдосконалення. Обмежено застосовуються передові технології, засновані на сучасній інфраструктурі і стандартних інструментах, які модифіковано. В бізнес-процеси залучаються всі необхідні IT-фахівці. Управління IT переростає в процес рівня усієї організації. Діяльність з управління IT інтегровано в процес керування організацією.

5. Оптимізація. В організації є глибоке розуміння того як управляти IT, вирішувати проблеми, а також шляхи розвитку. Комунікація та навчання підтримуються на високому рівні, за допомогою найсучасніших засобів. Як результат безперервного покращення, процеси відповідають моделям зрілості, які побудовано на підставі "кращих практик". Першопричини проблем і відхилень, що виникають ретельно аналізуються, і за результатами цього аналізу виконуються відповідні дії. Інформаційні технології інтегровано в бізнес-процеси, є повна їх автоматизація, яка надає можливість підвищувати якість та ефективність роботи організації.

3.1.2 Критичні фактори успіху

Критичні фактори успіху (КФУ) дають визначення найбільш важливим проблемам або діям керівництва і спрямовані на досягнення повного контролю над IT-процесами. КФУ мають бути керованими, з орієнтацією на успіх і мати опис того, як виконувати стратегічні, технічні, організаційні і процедурні дії щоб досягти успіху[36].

Як приклади критичних факторів успіху можна зазначити наступні:

- Дії з управління процесами в IT інтегровано в процеси управління організацією і стиль роботи керівництва;
- Управління IT зосереджується на цілях компанії: стратегічні ініціативи, технологій для забезпечення розвитку бізнесу, достатність ресурсів і задоволення бізнес-вимогам;
- Дії по управлінню процесами в IT чітко визначено, формалізовано і відбувається їх здійснення на основі потреб компанії з відповідною звітністю;

• Методики управління розроблено для підвищення продуктивності, досягнення оптимальності використання ресурсів і підвищення ефективності IT-процесів;

• Методи аудиту визначені таким чином, щоб уникнути збоїв і помилок в системі внутрішнього контролю;

• Можна спостерігати інтеграцію і розвиток взаємодії складних IT-процесів, наприклад, управління проблемами, змінами та конфігурацією;

• Засновано контрольний комітет, який призначає і спостерігає за незалежним аудитом, який приділяє пильну увагу IT при складанні планів аудиту, а також приймає до уваги результати досліджень сторонніх організацій і аудиторів.

3.1.3 Ключові індикатори цілі

Ключові індикатори цілі (КІЦ) описують комплекс вимірювань, які за фактом повідомляють керівництву, що IT-процес досяг пропонованих бізнес-вимог[36]. КІЦ виражаються в наступних термінах інформаційних критеріїв:

• Придатність інформації, яка необхідна для підтримки бізнесу;

• Ризики, пов'язані з відсутністю цілісності та конфіденційності;

• Рентабельність процесів і операцій;

• Підтверджена надійність, ефективність та узгодженість.

3.1.4 Ключові індикатори результату

Ключові індикатори результату(КІР) містять в собі опис комплексу дій, необхідних для того щоб визначити, наскільки IT-процеси можуть досягти поставлених цілей. КІР є основними індикаторами, які відображають імовірність досягнення поставленої мети. А також індикаторами, які вказують на адекватність способів, методів і навичок, використовуваних для досягнення результату[36].

Ключовими індикаторами результату (КІР), можуть бути:

• Підвищення рентабельності IT-процесів;

• Покращення роботи і планування дій з вдосконалення IT-процесів;

• Збільшення навантаження на інфраструктуру IT;

• Підвищення ступеня задоволеності користувачів (опитування користувачів та відстежування кількості скарг);

• Покращення взаємодії та комунікації між керівниками IT і керівництвом компанії

• Підвищення продуктивності робітників.

3.2. Методологія COBIT 5

COBIT 5 пропонує цілісну методологію, яка покликана допомогти у вирішенні завдання керівництва і управління IT на підприємстві. Простіше кажучи, COBIT 5 допомагає підприємствам досягти оптимальної цінності від IT, підтримуючи баланс між отриманням вигоди і оптимізацією ризиків і ресурсів. COBIT 5 дає можливість керувати і управляти IT в масштабах всього підприємства, як в областях функціональної відповідальності IT, так і бізнесу, а також дозволяє враховувати потреби в IT внутрішніх і зовнішніх зацікавлених сторін. Методологія COBIT 5 універсальна і буде корисна підприємствам будь-якого масштабу і сфери діяльності: комерційним, громадським і державним.

COBIT 5 заснований на п'яти принципах керівництва та управління IT на підприємстві[37]:

• Принцип 1: Відповідність потребам зацікавлених сторін. Підприємства існують для того, щоб створювати цінність для зацікавлених сторін, шляхом підтримання балансу між отриманням вигоди і оптимізацією ризиків і ресурсів. COBIT 5 описує всі необхідні процеси і інші фактори впливу, які підтримують створення бізнес-цінності за допомогою IT. Оскільки завдання, що стоять перед кожним підприємством, можуть бути різними, можна модифікувати модель COBIT 5 так, щоб ці рекомендації підходили до конкретного контексту даної організації. Зробити це можна за допомогою каскадування високорівневих

цілей підприємства до рівня керованих і конкретних IT-цілей і пов'язаних з ними процесів і практик.

• Принцип 2: Комплексний погляд на підприємство. COBIT 5 вбудовує керівництво IT в керівництво підприємством в цілому, тобто:

- Розглядає всі функції і процеси підприємства. COBIT 5 націлений не тільки на реалізацію «IT функції», але розглядає інформацію та пов'язані з нею технології як активи підприємства, якими слід управляти, як і будь-якими іншими активами.

- Виходить із того, що фактори впливу керівництва та управління, пов'язані з IT, працюють на всіх підприємстві і по всій ланцюжка створення цінності, і включають в себе всі внутрішні і зовнішні аспекти і ролі, які мають відношення до керівництва та управління IT.

• Принцип 3: Застосування єдиної інтегрованої методології. Існує безліч пов'язаних з IT склепінь знань і стандартів, присвячених окремим аспектам IT-діяльності. У COBIT 5 реалізовано відповідність цим зовнішнім склепіння і стандартам. Таким чином, методологія COBIT 5 забезпечує інтеграційний підхід для організації керівництва та управління IT на підприємстві.

• Принцип 4: Забезпечення цілісності підходу. Ефективне і раціональне керівництво та управління IT на підприємстві вимагає цілісного підходу, з урахуванням багатьох взаємопов'язаних компонентів.

У COBIT 5 описаний набір факторів впливу, які забезпечують впровадження системи керівництва та управління IT на підприємстві. Фактори впливу - це сутності, які сприяють вирішенню завдань підприємства. Методологія COBIT 5 описує сім видів факторів впливу:

- Принципи, політики і підходи
- Процеси
- Організаційна структура
- Культура, етика і поведінку

- Інформація

- Послуги, інфраструктура і додатки

- Персонал, навички та компетенції

• Принцип 5: Поділ керівництва та управління. Методологія COBIT 5 проводить чітку межу між керівництвом і управлінням. Ці дві дисципліни включають в себе різні види діяльності, вимагають різних організаційних структур і служать різним цілям. У розумінні COBIT 5, різниця між керівництвом і управлінням полягає в наступному:

- Керівництво забезпечує впевненість в досягненні цілей підприємства, шляхом: збалансованої оцінки потреб зацікавлених сторін, існуючих умов і можливих варіантів; встановлення напрямку розвитку через пріоритизації і прийняття рішень; постійного моніторингу відповідності фактичної продуктивності і ступеня виконання вимог встановленим напрямку і цілям підприємства. У більшості випадків обов'язки по керівництву на підприємстві виконує рада директорів, очолюваний головою ради директорів. Деякі обов'язки можуть бути делеговані спеціальним організаційним одиницям відповідного рівня - особливо, у великих організаціях.

- Управління полягає в плануванні, побудові, виконанні та відстеження діяльності, в відповідно до напряму, заданим органом керівництва, для досягнення цілей підприємства. У більшості випадків, обов'язки з управління на підприємстві виконують виконавчі директора, очолювані генеральним директором (CEO). Разом ці принципи допомагають побудувати ефективну методологію керівництва та управління, оптимізує інвестиції в інформаційні технології для отримання вигоди зацікавленими сторонами.

Розповідаючи про керівництво і управління інформаційними і пов'язаними технологіями, методологія COBIT 5 розглядає підприємство комплексно, по всьому ланцюжку створення цінності. Це означає, що COBIT 5:

• Розглядає керівництво IT як невід'ємну частину керівництва підприємством в цілому. Тому пропонована в методології COBIT 5 система керівництва IT легко інтегрується в будь-яку систему керівництва. Методологія COBIT 5 враховує новітні віяння в корпоративному керівництві.

• Описує всі функції і процеси, необхідні для керівництва та управління інформаційними і пов'язаними технологіями на підприємстві, де б не проводилася обробка інформації. використовуючи такий широкий погляд на підприємство, методологія COBIT 5 може описувати всі внутрішні і зовнішні IT-послуги, а також внутрішні і зовнішні бізнес-процеси.

Методологія COBIT 5 пропонує цілісний і системний погляд на керівництво та управління інформаційними та пов'язаними технологіями на підприємстві, заснований на наборі факторів впливу. Фактори впливу є універсальними і застосовними на всіх етапах створення цінності, а це значить, що вони відносяться до всіх аспектів і особам, внутрішнім і зовнішнім, хто має відношення до керівництва інформаційними та пов'язаними технологіями на підприємстві, включаючи обов'язки і діяльність як IT-функцій, так і бізнес-підрозділів.

Інформація є одним з факторів впливу в методології COBIT. Модель, яка використовується в COBIT 5 для опису факторів впливу, дозволяє кожній зацікавленій стороні пред'явити повні і вичерпні вимоги до інформації та життєвому циклу обробки інформації, зв'язавши таким чином бізнес з його потребами в актуальної інформації в існуючому контексті з IT-функціями, що підтримують бізнес.

3.3. Приклад використання каскаду цілей COBIT 5

Складемо набір стратегічних цілей (Рис 3.1), найважливішою з яких є підвищення задоволеності клієнтів. тепер потрібно дізнатися, в яких областях управління IT найбільше затребувані заходи щодо вдосконалення. 'P' - означає прямий зв'язок, а 'S' - непрямий, тобто слабіший[37].

Вимір збалансованої карти показників	Мета підприємства	Зв`язок із завданнями керівництва		
		Отримання вигоди	Оптимізація ризиків	Оптимізація ресурсів
Фінанси	1. Віддача від інвестицій для зацікавлених сторін	P		S
	2.Портфель конкурентоспроможних товарів і послуг	P	P	S
	3.Керовані бізнес-ризики (захист активів)		P	S
	4.Відповідність зовнішнім законам і регулюючим нормам		P	
	5.Фінансова прозорість	P	S	S
Замовник	6.Клієнтоорієнтована сервісна культура	P		S
	7.Неперервність та доступність бізнес-послуг		P	
	8.Гнучка реакція на мінливі умови ведення бізнесу	P		S
	9.Прийняття стратегічних рішень на основі інформації	P	P	P
	10.Оптимізація витрат на надання послуг	P		P
Внутрішнє управління	11.Оптимізація функціональності бізнес-процесів	P		P
	12.Оптимізація витрат бізнес-процесів	P		P
	13.Управління програмами бізнес-змін	P	P	S
	14.Операційна продуктивність персоналу	P		P
	15.Дотримання внутрішніх політик		P	
Навчання і розвиток	16.Кваліфікований та мотивований персонал	S	P	P
	17.Культура довгострокових інновацій продуктів і бізнеса	P		

Рис. 3.1. Цілі підприємства згідно COBIT 5

Було вирішено, що найвищий пріоритет задоволеності клієнтів означає, що такі цілі підприємства є найважливішими:

• Клієнтоорієнтована сервісна культура

•Неперервність та доступність бізнес-послуг

• Гнучка реакція на мінливі умови ведення бізнесу

Після цього за допомогою каскаду цілей були виявлені IT-цілі, що відповідають цілям підприємства.

В якості найважливіших було обрано такі IT-цілі (всі відносини типу «P»):

• Відповідність між IT та бізнес стратегіями

• Управління бізнес-ризиками, пов'язаними з IT

• Надання IT-послуг відповідно до бізнес-вимог

• Гнучкість IT

• Безпека інформації, а також обробної її інфраструктури та додатків

• Доступність надійної та корисної інформації для прийняття рішень

• Знання, експертиза та ініціативність для здійснення бізнес-інновацій

Після перевірки цього списку було вирішено вважати перші 4 мети самими пріоритетними. На наступному кроці каскаду цілей ці IT-цілі передбачають ряд цілей факторів впливу, в число яких входять цілі процесів.

Пропонується зв'язок між IT-цілями і процесами COBIT 5. Таблиця дозволяє виявити найважливіші IT-процеси, підтримують досягнення IT-цілей, проте одних тільки процесів недостатньо. Інші фактори впливу, такі як культура, поведінка і етика, організаційні структури, навички та експертиза точно так само важливі і вимагають набору чітких цілей.

Завершивши цю роботу, на підприємстві отримали набір чітких цілей для всіх факторів впливу, який дозволить досягти заявлених стратегічних цілей, а також набір відповідних їм метрик для вимірювання продуктивності.

Стверджується, що єдина структура з набором атрибутів дозволяє:

- працювати з усіма факторами впливу на єдиної, простої і структурованої основі;
- керувати комплексними взаємодіями;
- забезпечувати успішні результати роботи факторів впливу.

Начебто все слова зрозумілі, але ось що з них слід - тут у мене було більше питань, ніж відповідей. І лише недавно, на мій погляд, картинка в цілому склалася. У цій замітці я хочу поділитися тим, яку корисну інформацію можна витягти зі структури фактора впливу при вирішенні задачі проектування або розвитку процесу.

Візьмемо як приклад всім знайомий процес управління змінами.

Зацікавлені сторони

Хто є зацікавленими сторонами (ЗС) процесу управління змінами?

- Керівники різних рівнів аж до ради директорів: нездатність IT підтримати розвиток бізнесу може привести втрати конкурентних переваг і недоотриманого прибутку.

- Сервіс-менеджери, які відповідають за якість послуги, яким загрожує кожну зміну.
- Менеджери і учасники інших процесів, що обмінюються інформацією з процесом управління змінами, - в першу чергу, управління релізами, управління конфігураціями, управління інцидентами.
- Зацікавлені сторони бувають зовнішні і внутрішні, їх інтереси транслюються в бізнес-цілі, потім в IT-цілі і, нарешті, в цілі процесу.

Цілі

Список цілей всіх процесів і відповідних їм метрик сформульований в публікації COBIT 5 Enabling Processes, але, на жаль, без рознесення на пряме і контекстуальне якість, а тут, на мій погляд, є цікаві деталі.

Пряме якість - чи дає процес необхідні результати? Виходячи з призначення (з ITIL або COBIT), процес управління змінами повинен забезпечувати контроль змін таким чином, щоб досягалася користь (від змін) і мінімізувався негативний вплив (від змін). Метрики, що відображають пряме якість процесу, в «Керівництві по вимірюванню» і в ITIL Practitioner Guidance названі метриками результативності. Це - своєчасність реалізації змін; частка змін, що призвели до значних / повторюваним інцидентів; задоволеність споживачів послуг якістю реалізації змін. Так як призначення процесу універсально, не дуже мінливий і набір метрик, які повинні підтверджувати, що воно (призначення) реалізується. Це пряме якість.

Контекстуальное якість - адаптований процес до умов організації? Наскільки раціонально він організований? Якою ціною досягаються необхідні результати? Частка стандартних змін; частка екстрених змін; частка змін, які реалізуються з першого разу; частка змін, що проходять через CAB; частка

змін, що проходять через PIR - все це метрики раціональності, що відображають те, як організований процес. На відміну від якості прямого мети і відповідні їм метрики за якістю контекстуальному досить специфічні для організації, і залежать в першу чергу від зрілості системи менеджменту.

Доступність (тут «accessibility») і конфіденційність - все, кому належить, повинні мати доступ до документації і записів по процесу, системи автоматизації; для інших - доступ повинен бути обмежений / закритий. З огляду на корені COBIT і історично сильний крен в бік аудиту, пункт специфічний (бачиться, що його можна віднести до контекстуальному якості), але зрозумілий і важливий.

Хороші практики

Хороші практики - набір завдань, факторів успіху, досягнення яких необхідно для реалізації призначення процесу. Список хороших практик можна взяти з будь-якої загальнодоступної референтної моделі (COBIT, ITIL, ISO20000), або побудувати свою.

Список ключових практик BAI06 Manage Changes в COBIT 5 такий:

- Оцінка, визначення пріоритетів, авторизація запитів на зміни
- Управління екстреними змінами
- Відстеження статусу зміни і надання звітності
- Документування та закриття змін

І ось у нас з'являються метрики відповідності зовнішнім або внутрішнім вимогам: наявність / відсутність / повнота реалізації набору практик з референтної моделі.

Життєвий цикл

У COBIT5 наведено такий перелік станів життєвого циклу процесу: планування, придбання, побудова / придбання / створення / впровадження,

використання / експлуатація, оцінка / моніторинг, оновлення / утилізація. Думаю, цей список можна спростити без втрати сенсу до PDCA, за яким будуть ховатися такі справи, як:

- Постановка цілей процесу
- Створення / оновлення плану процесу
- Проведення вимірювань і підготовка звітності
- Проведення зустрічей з оцінки процесу
- Планування вдосконалення процесу

Всі ті справи, завдяки яким процес буде приносити користь не тільки зараз, але і в майбутньому. На відміну від хороших практик, які специфічні для кожного процесу, завдання з управління життєвим циклом універсальні. Повнота реалізації циклу Демінга фактично свідчить про те, на якому рівні зрілості перебуває процес - саме це перевіряється в таких підходах, як CMMI-SVC і (заснованих на ISO15504) COBIT PAM і TIPA (з рівня 2 і вище)

Висновки до третього розділу

У даному розділі розглянуто методологію ISACA - COBIT 5. Своє місце застосування методологія COBIT знайшла в багатьох країнах.

Управление компанией будь-яких масштабів і різних сфер діяльності вельми багатобічний і кропітка праця для груп керівників, що включає в себе підтримку корпоративного духу, структуроване взаємодія компонентів компанії, узгоджене професійне взаєморозуміння бізнес-співробітників та IT-співробітників, своєчасні прогнози ризиків і втрат, впровадження та моніторинг IT , підтримання висхідних трендів виробництва і прибутку тощо. В потоці

нових ідей щодо вдосконалення систем управління вельми важко вибрати най олее ефективний підхід, який враховував би організаційну структуру, місію та цінності компанії. Особливий напрямок, яке заслуговує на найбільшу увагу при управлінні компанії, є IT.

Важливу роль на світовій арені займає міжнародна асоціація IT ISACA (Information Systems Audit and Control Association). Асоціація фокусується на аудиті, безпеки та управлінні IT, а також надає різні сертифікації. Дана організація розробила безліч посібників, методологій і політик по грамотному управлінню і моніторингу IT в компанії з точки зору різних критеріїв - ризики, рівні зрілості процесів, цінностей підприємства.

Методологія COBIT 5 пропонує цілісний і системний погляд на керівництво та управління інформаційними та пов'язаними технологіями на підприємстві, заснований на наборі факторів впливу. Фактори впливу є універсальними і застосовними на всіх етапах створення цінності, а це значить, що вони відносяться до всіх аспектів і особам, внутрішнім і зовнішнім, хто має відношення до керівництва інформаційними та пов'язаними технологіями на підприємстві, включаючи обов'язки і діяльність як IT-функцій, так і бізнес-підрозділів.

ВИСНОВКИ

Правовий захист інформації забезпечується нормативно-правовими актами, сукупність яких за рівнем представляє ієрархічну систему від Конституції України, Законів України у сфері інформаційної безпеки та захисту інформації, підзаконних та нормативних актів до функціональних обов'язків і контрактів конкретного виконавця, які визначають перелік відомостей, що підлягає охороні, і заходи відповідальності за їх розголошення.

Були досліджені основні закони України, що регулюють правовий захист інформаційної безпеки. Технічний захист інформації регулюється нормативними документами технічного захисту інформації та призначений для забезпечення організаційними, інженерними та технічними заходами, методами і засобами конфіденційності, цілісності та доступності інформації, яка обробляється в ІТС, циркулює на підприємстві та становить державну та іншу встановлену законами таємницю.

Ключову роль у стандартизації з управління інформаційною безпекою відіграють такі міжнародні організації, як Міжнародна організація по стандартизації, Міжнародна електротехнічна комісія та Міжнародний союз телекомунікації.

Була розглянута «Помаранчева книга», яка стала основою для більшості сучасних стандартів інформаційної безпеки. Розглянуто положення міжнародних стандартів серії ISO / IEC 27000. Серія містить кращі практики і рекомендації в області інформаційної безпеки для створення, розвитку та підтримки СУІБ та визначає вимоги до СУІБ, управління ризиками, метрики і вимірювання, а також керівництво по впровадженню.

У стандарті COBIT детально описано цілі і принципи управління, об'єкти управління, чітко визначені всі IT процеси (для кожного процесу визначені входи і виходи, виконавці та відповідальні, а також об'єкти контролю та метрики) і вимоги до них, описаний можливий інструментарій (практики) для їх реалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Правовий захист інформаційної безпеки. [Електронний ресурс]. – Режим доступу: https://studopedia.org/12-73889.html.

2. Марущак А. «Захист інформації з обмеженим доступом та право на інформацію: проблеми правового регулювання». [Електронний ресурс]. – Режим доступу: http://pnzzi.kpi.ua/13/13_p108.pdf .

3. Закон України «Про інформацію». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12.

4. Закон України «Про доступ до публічної інформації». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17 .

5. Що таке публічна інформація, порядок її отримання. [Електронний ресурс]. – Режим доступу: https://www.msp.gov.ua/content/shcho-take-publichna-informaciya-poryadok-ii-otrimannya.html?PrintVersion .

6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». [Електронний ресурс]. – Режим доступу: https://zakon2.rada.gov.ua/laws/show/80/94-вр.

7. Закон України «Про державну таємницю». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12.

8. Закон України «Про основні засади забезпечення кібербезпеки України». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.

9. Жовницька Н. Основні засади забезпечення кібербезпеки України. [Електронний ресурс]. – Режим доступу: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-osnovnye-principy-obespecheniya-kiberbezopasnosti-ukrainy .

10. Закон України ««Про захист персональних даних»». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17 .

11. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі". [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074.

12. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. [Електронний ресурс]. – Режим доступу: http://webcache.googleusercontent.com/search?q=cache:mq79-OAQhRkJ:www.dsszzi.gov.ua/dsszzi/doccatalog/document%3Fid%3D106341+&cd=1&hl=uk&ct=clnk&gl=ua&client=opera .

13. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96. [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836 .

14. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу – [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

15. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

16. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiPpZrqgMHiAhVmw4sKHa-xAVEQFjAAegQIBRAC&url=http%3A%2F%2Fwww.dsszzi.gov.ua%2Fdsszzi%2Fdoccatalog%2Fdocument%3Fid%3D106344&usg=AOvVaw1FCWTVxvEo624Prh6aNeEh .

17. Захист інформації WEB-сторінки. [Електронний ресурс]. – Режим доступу: http://www.nics.com.ua/index.php/nashi-poslugi/115-zakhist-informatsiji-web-storinki

18. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в

автоматизованій системі. [Електронний ресурс]. – Режим доступу: https://studfiles.net/preview/4494505/page:7/

19. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/nd-tz-1.1-002-99.html

20. ГСТУ СУІБ 1.0/ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD). [Електронний ресурс]. – Режим доступу:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910

21. ГСТУ СУІБ 2.0/ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. [Електронний ресурс]. – Режим доступу: http://s-byte.com/useful/27002.pdf

22. Євсеєв С. "Управління інформаційною безпекою"- 2016 - [Електронний ресурс]. – Режим доступу: http://s-byte.com/useful/27002.pdf

23. Стандарти із захисту інформації. [Електронний ресурс]. – Режим доступу: https://studfiles.net/preview/3541381/page:4/

24. "Помаранчева книга". [Електронний ресурс]. – Режим доступу: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/oranzhevaja_kniga_tcsec/

25. Стандарт ISO / IEC 17799. [Електронний ресурс]. – Режим доступу: http://www.kmgep.kz/data/filedat/default/ISO_IEC_17799_2000_rus.pdf

26. Формування інформаційної безпеки на основі стандарту ISO / IEC 27001:2005. [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiZyKqKkMPiAhVNR5oKHV7BAjsQFjAAegQIABAC&url=http%3A%2F%2Firbisnbuv.gov.ua%2Fcgibin%2Firbis_nbuv%2Fcgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAGE_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF%2Fssia_2010_2_12.pdf&usg=AOvVaw2XzPhg42bLwZFZsP9clheM

27. ISO / IEC 2700 Інформаційні технології — Технології безпеки — Системи управління інформаційною безпекою. Керівництво. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/ISO/IEC_27003

28. ISO/IEC 27005:2008 Інформаційні технології — Методики безпеки — Управління ризиками інформаційної безпеки. [Електронний ресурс]. – Режим доступу: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf

29. ISO/IEC 27006:2015 «Інформаційні технології – Методи безпеки – Вимоги до органів, які здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки». [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/ISO/IEC_27006

30. ISO/IEC 27006:2015 «Інформаційні технології – Методи безпеки – Вимоги до органів, які здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки». [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66913

31. Загальні критерії – ISO / IEC 15408. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Common_Criteria

32. Стандарт ISO/IEC 15408. [Електронний ресурс]. – Режим доступу: https://studfiles.net/preview/6012701/page:28/

33. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки. [Електронний ресурс]. – Режим доступу: https://www.intuit.ru/studies/courses/563/419/lecture/9577?page=3

34. Безпека інформаційних систем. [Електронний ресурс]. – Режим доступу: https://pidruchniki.com/74227/informatika/bezpeka_informatsiynih_sistem

35. ISACA. «COBIT 5 по інформаційної безпеки». ISACA. США. 2012.ISBN: [978-1-60420-255-7].

36. COBIT 5: Бизнес-модель по руководству и управлению ИТ на предприятии. [Электронный ресурс] – Режим доступа: World Wide Web. – URL: http://www.wikiitil.ru/books/Cobit-5_frm_rus_0813.pdf/.

37. ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ МЕТОДОЛОГИИ COBIT НА РЕАЛЬНЫХ КОМПАНИЯХ. [Электронный ресурс] - Режим доступа: World Wide Web. – URL: https://sibac.info/studconf/tech/xlix/67486/.

38. Обзор стандарта COBIT. [Електронний ресурс] - Режим доступа: World Wide Web. – URL: https://www.itexpert.ru/rus/biblio/cobit/.