УДК 342.9
DOI https://doi.org/10.32840/pdu.2-1.14

О. В. Дикий
кандидат юридичних наук, доцент,
в.о. декана факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

М. О. Флюнт
юрист компанії Hosting.ua

СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: КОМПАРАТИВНЕ ДОСЛІДЖЕННЯ

Стаття є комплексним дослідженням основних міжнародних стандартів інформаційної безпеки серії 27000х, що можуть бути застосовані організаціями усіх рівнів у будь-яких сферах діяльності.

Однією з передумов створення системи стандартів інформаційної безпеки є відсутність єдиної теорії захищених систем, що є в достатній мірі універсальною в різних предметних галузях (як в державному, так і в комерційному секторі).

У дослідженні визначено термін «інформаційна безпека» та вказано основні компоненти інформаційної безпеки комп'ютерних систем, якими є конфіденційність, можливість застосування та цілісність. Крім того, розкрито поняття «система управління інформаційною безпекою» та обґрунтовано необхідність створення системи стандартів для її функціонування. Зазначено, що розроблені стандарти є керівними положеннями під час забезпечення захисту інформації в кіберпросторі.

Міжнародні стандарти класифіковано за функціональним призначенням та розділено на чотири групи:

– стандарти для огляду і введення в термінологію;

– стандарти, які визначають обов'язкові вимоги до системи управління інформаційною безпекою;

– стандарти, що визначають вимоги і рекомендації для аудиту системи управління інформаційною безпекою;

– стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення системи управління інформаційною безпекою.

У дослідженні описано суть, завдання, переваги та недоліки найбільш поширених у використанні стандартів, зокрема ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27035.

Визначено, що превагами застосування Міжнародних стандартів ISO 27000х є: забезпечення безперервності, мінімізація ризиків, забезпечення комплексного та централізованого контролю рівня захисту інформації, забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів інформаційно-комунікаційних систем та мереж, зниження витрат на інформаційну безпеку.

У статті розкрито значення міжнародної стандартизації у сфері інформаційної безпеки на розвиток внутрішньодержавних та локальних вимог і правил. Перелічено основні документи в галузі технічного захисту інформації та акредитовані і впроваджені міжнародні стандарти, що застосовуються в Україні.

Ключові слова: *інформаційна безпека, система управління інформаційною безпекою, міжнародний стандарт, інциденти в області інформаційної безпеки.*

Постановка проблеми. На сучасному етапі розвитку суспільства, пов'язаного з масовим використанням інформаційних технологій і створенням єдиного інформаційного простору, в рамках якого відбувається накопичення, обробка, зберігання та обмін інформацією, проблеми інформаційної безпеки набувають першочергового

© Дикий О. В., Флюнт М. О., 2019

значення в усіх сферах суспільної і державної діяльності [1, с. 5].

Так, за наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки. Таким чином, інформаційна безпека комп'ютерних систем, яка є невіддільною частиною кібербезпеки, є необхідною умовою розвитку інформаційного суспільства.

Суцільна комп'ютеризація, стрімке поширення у глобальному вимірі інформаційних і телекомунікаційних мереж та техніко-технологічного розвитку зумовлюють необхідність вирішення ряду питань щодо захисту персональної та конфіденційної інформації, вдосконалення механізмів захисту та забезпечення інформаційної безпеки та посилення заходів кібербезпеки.

Аналіз останніх досліджень і публікацій. Питання, пов'язані з дослідженням міжнародних стандартів інформаційної безпеки, досліджувалися такими вітчизняними і зарубіжними науковцями, як Д.С. Бірюков, В.Л. Бурячко, В.М. Бутузов, В.Д. Гавловський, М.В. Гуцалюк, Д.В. Дубов, В.В. Петров, О.В. Орлов, О.Д. Довгань, В.П. Шеломенцев та інші.

Зазначені науковці зробили значний внесок в розвиток теоретичних вчень та досліджень у сфері інформаційної безпеки, однак окремі аспекти захисту інформації в кіберпросторі все ж залишилися малодослідженими.

Метою статті є компаративне дослідження міжнародних стандартів інформаційної безпеки.

Виклад основного матеріалу. В умовах швидких темпів впровадження комп'ютеризації у всі сфери діяльності суспільства, з метою забезпечення інформаційної безпеки в кіберпросторі постала необхідність створення єдиної та загальної системи стандартів інформаційної безпеки, що гарантували б її ефективність та універсальність, адже на цей час не існує єдиної теорії захищених систем, до того ж універсальної в різних предметних областях (як в державному, так і в комерційному секторі.

Так, перші напрацювання в цій сфері були наслідком роботи окремих національних та міжнародних форумів, зокрема, Стенфордських консорціумів з досліджень питань інформаційної безпеки та політики у 1990-х роках. На сучасному етапі розробкою міжнародних стандартів займаються Міжнародна організація з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). В області інформаційних технологій, ISO і IEC організований спільний технічний комітет, ISO/IEC JTC1, основним завданням якого є підготовка Міжнародних стандартів інформаційної безпеки.

Розроблені стандарти є керівними положеннями під час забезпечення захисту інформації в кіберпросторі. Таким чином, система кібербезпеки, яка базується на міжнародних стандартах інформаційної безпеки, надзвичайно важлива у сучасному цифровому світі, а система управління інформаційною безпекою (далі – СУІБ) є однією з основних категорій цієї сфери. Так, СУІБ становить собою частину загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки (далі – ІБ) [2]. Остання включає в себе три основні компоненти: конфіденційність, можливість застосування і цілісність.

У найбільш буденному розумінні ІБ визначають як «захищеність інформації і підтримуючої інфраструктури від випадкових або умисних впливів природного або штучного характеру, що мають своїм наслідком завдання шкоди власникам або користувачам інформації і підтримувальній інфраструктурі» [1, С. 9]. Водночас у більш широкому розумінні, ІБ – це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [1, с. 12–13].

Так, ІБ забезпечується застосуванням та управлінням відповідними заходами

забезпечення безпеки, які охоплюють широкий діапазон загроз з метою гарантування стійкого успіху бізнесу і мінімізації впливу інцидентів інформаційної безпеки. Таким чином, інформаційна безпека досягається за допомогою виконання відповідного набору засобів управління, сформованого в ході обраного процесу менеджменту ризику і керованого через СУІБ, включаючи політики, процеси, процедури, організаційні структури, програмне та технічне забезпечення для захисту виявлених інформаційних активів. Ці засоби управління повинні бути визначені, впроваджені, а також контролюватися, аналізуватися і поліпшуватися, щоб гарантувати досягнення встановленого рівня інформаційної безпеки і бізнес-цілей [3].

Сімейство міжнародних стандартів управління безпекою 2700х активно розвивається та призначене для забезпечення ІБ організації. Крім того, воно включає стандарти, що визначають вимоги до СУІБ, систему управління ризиками, метрики і вимірювання ефективності механізмів контролю, а також керівництво по впровадженню.

Стандарти СУІБ включають стандарти, які: визначають вимоги до СУІБ, а також до тих, хто сертифікує такі системи; забезпечують безпосередню підтримку, містять докладні рекомендації і/або інтерпретацію загального процесу розробки, впровадження, забезпечення працездатності та поліпшення СУІБ; містять керівництва по СУІБ для конкретних галузей; містять вказівки з оцінки відповідності для СУІБ. Водночас терміни та визначення, що використовуються в цій стандартизації, включають в себе найбільш використовувані в сімействі стандартів СМІБ терміни та визначення; не містять всіх термінів і визначень, що застосовуються в стандартах СУІБ; не обмежують сімейство стандартів на СУІБ у визначенні нових термінів [4].

Міжнародна стандартизація в галузі ІБ охоплює стандарти, котрі умовно поділяються на 4 групи: стандарти для огляду і введення в термінологію; стандарти, які визначають обов'язкові вимоги до СУІБ (система управління інформаційною безпекою); стандарти, що визначають вимоги і рекомендації для аудиту СУІБ; стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення СУІБ.

Так, до стандартів для огляду і введення в термінологію входить стандарт ISO/IEC 27000 «Інформаційні технології – Методи і засоби забезпечення безпеки – Система менеджменту інформаційної безпеки – Загальні відомості та словник», що містить загальні відомості про систему менеджменту ІБ та включає тлумачення відповідної термінології [5].

Стандарти, які визначають обов'язкові вимоги до СУІБ, включають в себе ряд стандартів: ISO/IEC 27001 «Інформаційна технологія – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги», що зібрав описи найкращих світових практик в області управління інформаційною безпекою.

Цей стандарт визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації, а також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації. Вимоги, наведені в ISO/IEC 27001, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи [6]. Крім того, документ встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений як модель для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки [7].

Щодо стандартів, що визначають вимоги і рекомендації для аудиту СУІБ, то до них належать: ISO/IEC 27006 «Інформаційні технології – Методи забезпечення безпеки – Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою», що розширює вимоги стандарту ISO 17021 спеціально для органів, які проводять аудит і сертифікацію СУІБ; ISO/IEC 27007 «Інформаційні технології – Методи забезпечення безпеки – Керівництво по

аудиту – Систем менеджменту інформаційної безпеки», що пропонує рекомендації з проведення аудитів СУІБ з боку сертифікаційних організацій. Він корисний для аудиторів цих організацій; ISO/IEC TR 27008 «Інформаційні технології – Методи забезпечення безпеки – Керівництво для аудиторів щодо механізмів контролю СУІБ», що є додатковим стандартом до ISO 19011: 2011спеціально для СУІБ. Він спеціалізований для аудиту коштів управління інформаційною безпекою в організації.

Найбільш об'ємною є група стандартів, що пропонують кращі практики впровадження, та вдосконалення СУІБ, до якої входять: ISO/IEC 27002 «Інформаційні технології – Методи забезпечення безпеки – Практичні правила управління інформаційною безпекою. Друга редакція 01.10.2013», що є найпопулярнішим стандартом групи після ISO 27001 та надає відмінні вказівки для розробки, впровадження, підтримки і вдосконалення СУІБ.

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

Організації всіх типів та розмірів (охоплюючи публічний та приватний сектор, комерційні та неприбуткові) збирають, обробляють, зберігають та передають інформацію в багатьох формах, включаючи електронну, фізичну та усну (наприклад, бесіди та презентації) [8].

ISO/IEC 27003 «Інформаційні технології – Методи забезпечення безпеки – Керівництво по впровадженню системи управління інформаційною безпекою», що дає вказівки і методику для процесів розробки і впровадження СУІБ. Метою зазначеного стандарту є надання допомоги під час реалізації СУІБ у межах організації відповідно до ISO/IEC 27001.

Варто зазначити, що у стандарті приведені рекомендації та роз'яснення, однак не визначено жодних вимог. Водночас ISO/IEC 27003 визначає фази планування проекту СУІБ та: призначений для використання у корпоративних системах, що впроваджують СУІБ; застосовується організаціями всіх типів і розмірів; фокусується на критичних аспектах, необхідних для успішного проектування та впровадження СУІБ; описує процес специфікації та проектування СУІБ з моменту початку проектування до подання планів впровадження системи; описує процес отримання затвердження з боку керівництва впровадження СУІБ; визначає проект впровадження СУІБ; забезпечує керівництво планом проекту СУІБ.

Застосування міжнародного стандарту ISO/IEC 27003 дозволить: оптимізувати вартість побудови та підтримання ІБ; постійно відслідковувати та оцінювати ризики з урахуванням цілей бізнесу; ефективно виявляти найбільш критичні ризики та знижати ймовірність їх реалізації; розробити ефективну політику ІБ; ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу; забезпечити розуміння питань ІБ керівництвом та всіма працівниками підприємства, де впроваджується СУІБ; забезпечити підвищення репутації та ринкової привабливості підприємств.

ISO/IEC 27004 «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимірювання», що є керівництвом для вибору, проектування, управління і поліпшення засобів і методів вимірювання ефективності та результативності системи.

Цей Міжнародний стандарт надає вказівки щодо розробки та використання заходів та вимірювань з метою оцінки ефективності впровадженої СУІБ та елементів управління або груп контролю, визначених у ISO/IEC 27001. Так, документ включає політику, управління ризиками інформаційної безпеки, цілі контролю, контроль, процеси та процедури, підтримку процесу її перегляду, допомогу у визначенні чи потрібно змінювати або вдосконалювати будь-який із процесів чи

контроль СУІБ. Варто пам'ятати, що жодне вимірювання контролю не може гарантувати повну безпеку.

Реалізація цього підходу є програмою вимірювання інформаційної безпеки, яка допоможе керівництву у виявленні та оцінці невідповідних і неефективних процесів та засобів управління СУІБ та визначення пріоритетності дій, пов'язаних із вдосконаленням чи зміною цих процесів та/або контролю. Він також може допомогти в організації демонстрації відповідності ISO/IEC 27001 та надати додаткові докази для огляду керівництва та процесів управління ризиками інформаційної безпеки [9].

ISO/IEC 27005 «Інформаційні технології – Методи забезпечення безпеки – Управління ризиками інформаційної безпеки», що є одним з найважливіших в групі. Незважаючи на те, що це тільки рекомендаційний, а не обов'язковий стандарт, його призначення полягає в тому, що управління ризиками – один з найважливіших процесів для інформаційної безпеки.

Цей стандарт надає рекомендації щодо управління ризиками інформаційної безпеки в організації, зокрема, підтримуючи вимоги СУІБ відповідно до ISO/IEC 27001. Однак цей Міжнародний стандарт не передбачає конкретних методів управління ризиками ІБ. Організація повинна визначити свій підхід до управління ризиками, залежно, наприклад, від сфери застосування СУІБ, контексту управління ризиками чи галузевого сектору [10].

ISO/IEC 27011 «Інформаційні технології – Методи забезпечення безпеки – Керівництво з управління інформаційною безпекою для телекомунікацій ISO / IEC 27002», що є спеціалізованим керівництвом по СУІБ в телекомунікаційних організаціях. Суміжним до ISO/IEC 27011 є стандарт ISO/IEC 27031 «Інформаційні технології – Методи забезпечення безпеки – Керівництво по забезпеченню готовності інформаційних і комунікаційних технологій до їх використання для управління безперервністю бізнесу», що є стандартом-керівництвом щодо забезпечення безперервності бізнесу в інформаційних комунікаційних технологіях (ІКТ) та впровадження плану готовності послуг ІКТ, який забезпечить безперервність бізнесу під час збоїв. Так, у стандарті описані принципи забезпечення готовності ІКТ. У ньому наводяться основні методи і процедури визначення та опису всіх аспектів, таких як критерії ефективності, проектування та впровадження, що впливають на готовність ІКТ організації. Він також пропонує узгоджений і загальноприйнятий підхід до вимірювання характеристик, відповідних програмі забезпечення готовності ІКТ до забезпечення безперервності бізнесу.

Даний стандарт поширюється на всі події та інциденти (включаючи пов'язані з безпекою), які впливають на інфраструктуру і системи ІКТ. Він включає і доповнює практику обробки інцидентів в області інформаційної безпеки і управління ними, а також планування готовності і сервіси ІКТ [11].

Також, з точки зору практичних рекомендацій щодо забезпечення аварійного відновлення ІКТ, доволі цікавим є стандарт ISO/IEC 24762 «Інформаційні технології – Методи забезпечення захисту – Рекомендації по послугам для аварійного відновлення інформаційних і комунікаційних технологій».

ISO/IEC 27033, що замінює відомий міжнародний стандарт мережевої безпеки ISO 18028. Так, стандарт включає в себе декілька частин, з яких найбільш вагомими є ISO/IEC 27033-1 «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Основні концепції управління мережевою безпекою», що є першим з групи спеціалізованих стандартів в галузі забезпечення інформаційної безпеки мережевої інфраструктури; та ISO / IEC 27033-3 «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Базові мережеві сценарії – загрози, методи проектування та механізми контролю», що має практичне значення [12].

ISO/IEC 27034-1 «Інформаційні технології – Методи забезпечення безпеки – Огляд та основні концепції в області забезпечення безпеки додатків», що є першим з іншої групи спеціалізованих стандартів в галузі забезпечення інформаційної

безпеки прикладного програмного забезпечення.

ISO/IEC 27035 «Інформаційні технології – Методи забезпечення безпеки – Управління інцидентами безпеки», що є одним з цінних стандартів в групі з практичною вартістю в галузі управління інцидентами з ІБ, адже стандарт є рекомендацією щодо виявлення, реєстрації та оцінки інформації, випадків порушення безпеки і уразливості.

Стандарт допомагає організації реагувати на інциденти порушення безпеки, включаючи відповідні заходи контролю для запобігання та скорочення, відновлення наслідків, і таким чином, вчитися і вдосконалювати свій загальний підхід. Крім того, стандарт може бути застосований до будь-якої організації, незалежно від розміру. Він охоплює діапазон інцидентів інформаційної безпеки, незалежно від того, чи є вони навмисними або аварійними, спричинені через технічні чи фізичні засоби

Інтеграція інцидентів ІБ системи управління має ряд переваг, зокрема: підвищення загальної інформаційної безпеки; зменшення негативного впливу на бізнес; зміцнення інцидентів ІБ, профілактика, визначення пріоритетів, докази; сприяння бюджетному і ресурсному обґрунтуванню; поліпшення оновлення інформаційної безпеки оцінки ризиків та управління результатами; забезпечення підвищення інформованості в безпеці інформації та матеріалів, навчальна програма; забезпечення взаємозв'язку інформаційної політики безпеки і загальної документації [13].

Перевагами застосування Міжнародних стандартів ISO 27000х є: забезпечення безперервності, мінімізація ризиків, забезпечення комплексного та централізованого контролю рівня захисту інформації, забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів інформаційно-комунікаційних систем та мереж, зниження витрат на інформаційну безпеку.

Окрім зазначених стандартів, до системи міжнародної стандартизації ІБ входить безліч документів, що містять рекомендації та вимоги до впровадження та функціонування СУІБ, які слугують основою для розроблення та прийняття внутрішньодержавних правил та інструкцій.

Так, в нашій державі було створено ряд нормативних документів в галузі технічного захисту інформації та державні стандарти України (ДСТУ) стосовно створення і функціонування СУІБ, зокрема [1, с. 15]: НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі; Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96; НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі; НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу; НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу; НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2; НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу; НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі; НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу; ГОСТ 34.602-89; НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Також в Україні акредитовано та впроваджено два галузеві міжнародні стандарти: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD) та ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформа-

ційною безпекою. (ISO/IEC 27002:2005, MOD).

Крім того, Департамент інформатизації Національного банку України розробив Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України (прийнятий 03 березня 2011 року). Ці Методичні рекомендації щодо впровадження СУІБ розроблені на основі міжнародного стандарту ISO/IEC 27003: 2010 з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань ІБ [2].

Висновки і пропозиції. Міжнародні стандарти інформаційної безпеки становлять собою розгалужену систему, що включає в себе як обов'язкові положення, так і положення-рекомендації щодо забезпечення ІБ, а розроблення нових стандартів є безперервним процесом, який реагує на щоразу нові виклики та інциденти ІБ, і спрямоване на проектування універсальної та надійної моделі захисту персональних даних та інформації, у тому числі й у кіберпросторі.

Сімейство міжнародних стандартів є не лише основою надійного механізму забезпечення ІБ, а й слугує орієнтиром для подальших розробок програм захисту СУІБ та забезпечення ІБ на локальних рівнях.

Список використаної літератури:

1. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. КІІВіП НУ «ОЮА», 2017. 128 с.
2. Стандарти ISO/IEC захистять від кіберзагроз. URL: http://csm.kiev.ua/index.php?option=com_content&view=article&id=3631%3A-isoiec---&catid=122%3A2015-09-15-07-01-23&lang=uk.
3. Застосування міжнародного стандарту ISO/IEC 27003: 2010 у практиці корпоративних систем України. URL: https://www.slideshare.net/VladislavChernish/isoiec-270032010.
4. ISO/IEC27000. URL: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2014.pdf.
5. Общие сведения о стандартах серии ISO 27000. URL: http://www.iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu.
6. ISO/IEC 27000. URL: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2014.pdf.
7. ДСТУ ISO/IEC 27001-2015. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf.
8. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки. URL: https://naurok.com.ua/keruvannya-mehanizmami-zahistu-mizhnarodni-standarti-informaciyno-bezpeki-104726.html.
9. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.
10. ISO/IEC 27004:2009(E). URL: http://www.klubok.net/Downloads-index-req-viewdownloaddetails-lid-425.html.
11. ISO/IEC 27005:2011(E). URL: http://www.klubok.net/Downloads-index-req-viewdownloaddetails-lid-421.html.
12. Вашему бизнесу угрожают хакеры? Стандарт ISO/IEC 27031:2011 предлагает решения. URL: http://www.klubok.net/article3.html.
13. ISO 27000 – группа стандартов по информационной безопасности. URL: http://www.klubok.net/article2543.html.
14. ISO/IEC 27035:2011. URL: http://www.klubok.net/article2523.html.

Dykyi O., Fliunt M. Information security standards: a comparative research. *The article is a comprehensive study of the major international information security standards of the 27000x series, which can be applied by organizations of all levels in all fields of activity.*

One of the prerequisites for creating a system of information security standards is the absence of a unified theory of secure systems, which is sufficiently universal in various subject areas (both in the public and commercial sectors).

The term «information security» was defined and the main components of information security of computer systems, which are confidentiality, application and integrity, was indicated. In addition, the concept of «information security management system» was

explained and was substantiated the need to create a system of standards for its operation. It is stated that the developed standards are the guiding principles in ensuring the protection of information in cyberspace.

International standards were classified by function and were divided into four groups: standards for review and introduction to terminology; standards defining mandatory requirements for the information security management system; standards defining requirements and recommendations for the audit of the information security management system; standards that offer best practices for implementing, developing, and improving information security management systems.

The study describes the nature, objectives, advantages and disadvantages of the most widely used standards, including ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27035.

It is determined that the advantages of the application of the International Standards ISO 27000x are: ensuring continuity, minimizing risks, providing comprehensive and centralized control of the level of protection of information, ensuring the integrity, confidentiality and accessibility of critical information resources of information and communication systems and networks, reducing the cost of information security.

It is determined that the advantages of the application of the International Standards ISO 27000x are: ensuring continuity, minimizing risks, providing comprehensive and centralized control of the level of protection of information, ensuring the integrity, confidentiality and accessibility of critical information resources of information and communication systems and networks, reducing the cost of information security.

The importance of international standardization in the field of information security for the development of national and local requirements and rules was revealed. The main documents in the field of technical protection of information were listed and accredited and implemented international standards applicable in Ukraine was indicated.

Key words: *information security, information security management system, international standard, information security incidents.*