УДК 004.056.5

В'ячеслав Володимирович Овсянніков *(канд. техн. наук)*
Святослав Володимирович Дехтяр
Світлана Анатолівна Паламарчук
Юлія Олександрівна Черниш
Олександр Віталійович Шемендюк

Військовий інститут телекомунікацій та інформатизації, Київ, Україна

АНАЛІЗ НОРМАТИВНО-ПРАВОВИХ ТА ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ АСПЕКТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Враховуючи світові тенденції інформатизації сучасного суспільства, стрімкий розвиток інформаційних технологій та інтенсивне впровадження інформаційно-телекомунікаційних систем в усі сфери життєдіяльності держави і суспільства, постає необхідність в окресленні поняття та змісту інформаційної безпеки і системи її забезпечення.

В статі проаналізовано вимоги нормативно-правових актів України та міжнародних стандартів ISO/IEC щодо забезпечення інформаційної безпеки, приведена сутність основних понять та змісту інформаційної безпеки.

В рамках стандартів міжнародного та національного рівнів щодо інформаційної безпеки визначаються вимоги до захисту інформації (її властивостей). В англомовних стандартах, це класична модель CIA (конфіденційності – confidentiality, цілісності – integrity, доступності – availability), щодо забезпечення вимог конфіденційності, цілісності та доступності інформації. Окремо виноситься вимога спостереженості.

В міжнародних стандартах особлива увага також приділяється системі управління інформаційною безпекою.

Ключові слова: *інформаційна безпека; загрози інформаційній безпеці; загрози кібербезпеці та безпеці інформаційних ресурсів; стандарти ISO/IEC; стратегія національної безпеки.*

Вступ

Згідно до норми ч. 1, ст. 17 Конституції України [1] забезпечення інформаційної безпеки (ІБ) є однією з найважливіших функцій держави, для виконання якої створюються відповідні системи захисту інформації (технічного, криптографічного, кібернетичного, стеганографічного захисту тощо) та управління безпекою. У Законі України "Про основи національної безпеки України" [2] йдеться "про основні сфери національної безпеки", серед яких виокремлюється інформаційна. В Стратегії національної безпеки України [3] визначаються актуальні загрози національній безпеці, серед яких: загрози інформаційній безпеці; кібербезпеці та безпеці інформаційних ресурсів; безпеці критичної інфраструктури та основні напрями державної політики національної безпеки України і шляхи її забезпечення.

Постановка проблеми. Своєрідні властивості інформаційної безпеки та особливості її складових, шляхи їх забезпечення все частіше стають актуальними напрямами досліджень в різних науках (гуманітарних, правових, технічних, тощо) та всіх сферах життєдіяльності держави і суспільства. Свої корективи в дослідження привносить постійне вдосконалення законодавчої бази у сфері безпеки та оборони, основу якого формують вимоги сьогодення.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень та публікацій з питань забезпечення інформаційної безпеки відмічені В.В. Богданов, В.П. Горбулін, С.Д. Гусарєв, Г.В. Іващенко, В.М. Карташов, М.Б. Левицька, В.М. Лопатін та ін.

Метою статті є аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки, як складової національної безпеки України.

Виклад основного матеріалу дослідження

Поняття інформаційної безпеки залежно від області його використання розглядається у декількох ракурсах.

В широкому розумінні, інформаційна безпека (ІБ) – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

В інформаційному праві інформаційна безпека – це одна зі сторін розгляду інформаційних

відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

В залежності від виду загроз інформаційну безпеку можна розглядати як забезпечення стану захищеності:

особистості, суспільства, держави від впливу неякісної інформації;

інформації та інформаційних ресурсів організації від неправомірного впливу сторонніх осіб;

інформаційних прав і свобод людини і громадянина.

Інформаційна безпека особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи і т.ін.) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і т.ін.) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Інформаційна безпека організації – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Слід відмітити, що в Україні досі не прийнято закону, який би визначав Концепцію інформаційної безпеки, і відповідно єдиний план, єдину державну позицію чи стратегію розвитку інформаційної галузі, а отже і забезпечення інформаційної безпеки.

Аналізуючи класифікацію об'єктів та предметів різних аспектів інформаційної безпеки, необхідно відзначити одну особливість, властиву цілому ряду країн, в тому числі й Україні, а саме те, що більшість відповідних ідей і концепцій будуються не на об'єктно-цільовій базі, а на базі "загроз та інтересів". При цьому, ключову роль у проведенні політики інформаційної безпеки, особливо "силових" її векторів, повинна відігравати держава.

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонічного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства.

Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають відповідні повноваження, у відповідності із законодавством. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави.

Основними завданнями такої системи є:

виявлення і прогнозування дестабілізуючих факторів та інформаційних загроз інформаційних життєво важливим інтересам особистості, суспільства та держави;

здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;

створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Сутність основних понять та змісту інформаційної безпеки і системи її забезпечення приведена на рис. 1.

Нормативно-правову основу для забезпечення ІБ (безпеки інформаційних ресурсів) складає система документів, до якої входять: Конституція України; закони України ("Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про Основні засади розвитку інформаційного суспільства в Україні", "Про основи національної безпеки України"); нормативно-правові акти Президента і Кабінету Міністрів України (Стратегія національної безпеки, Доктрина інформаційної безпеки України, Концепція технічного захисту інформації в Україні, Положення про технічний захист інформації в Україні); міжнародні та державні стандарти, які визначають взаємовідносини між різними міністерствами, відомствами та іншими державними установами в частині забезпечення інформаційної безпеки; нормативні документи системи технічного захисту інформації (НД ТЗІ); відомчі нормативні документи в рамках їх відповідальності.

Рівні нормативно-правового забезпечення ІБ представлено на рис. 2.

Основу державного рівня нормативно-правового забезпечення інформаційної безпеки складають Закони України, Укази Президента, Постанови Кабінету Міністрів України та ін., вимоги яких є обов'язковими для виконання на всіх рівнях.

Згідно Закону України "Про захист інформації в ІТС" [4] інформація, яка є власністю держави повинна оброблятися із застосуванням комплексних систем захисту інформації з підтвердженою відповідністю (за результатами державної експертизи).

При проектуванні захищених інформаційно-телекомунікаційних систем важливо чітко

визначити, яким вимогам вони повинні відповідати, перелік основних показників якості, методику контролю та оцінки їх ефективності. На сьогодні, ця задача може бути вирішена за допомогою спеціально розроблених нормативних документів, які отримали назву стандартів інформаційної безпеки (СІБ).

В рамках стандартів міжнародного (стандарти ISO) та національного рівнів (ДСТУ, НД ТЗІ) щодо інформаційної безпеки визначаються вимоги до захисту інформації, або її властивостей. В англомовних стандартах, це класична модель CIA, щодо забезпечення вимог конфіденційності, цілісності та доступності інформації.

Окремо виноситься вимога спостереженості (accountability).

Вимога конфіденційності висувається до інформації, всі інші – як до інформації так і до системи в цілому.

З метою цільового застосування (як механізму захисту так і попередження) стандартів ІБ в рамках даної моделі в ІТС також розглядаються три складові: апаратне забезпечення (hardware); програмне забезпечення (software); комунікаційна складова (communication), які представлено на рис. 3.

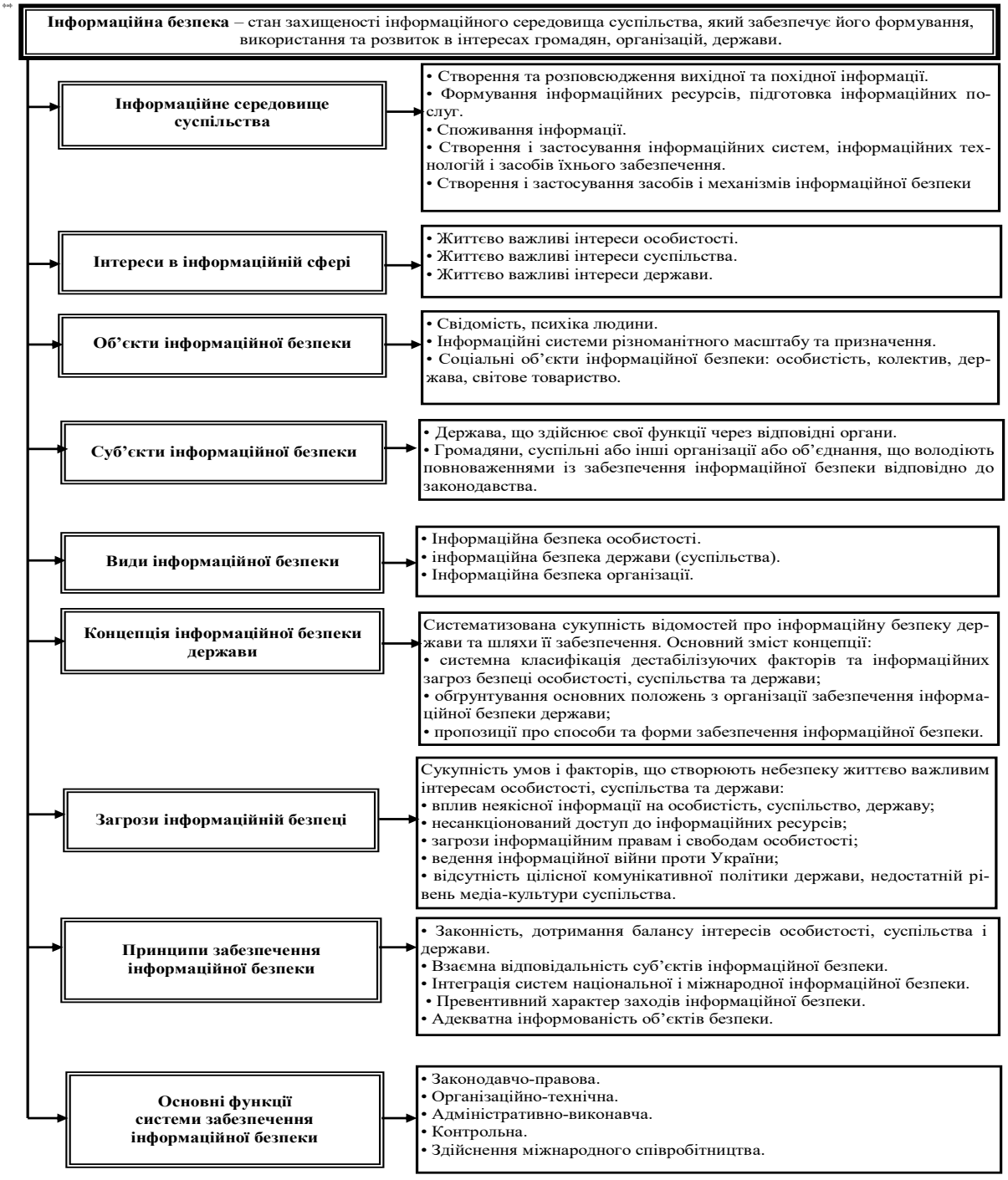

Рис. 1. Основні поняття та зміст інформаційної безпеки

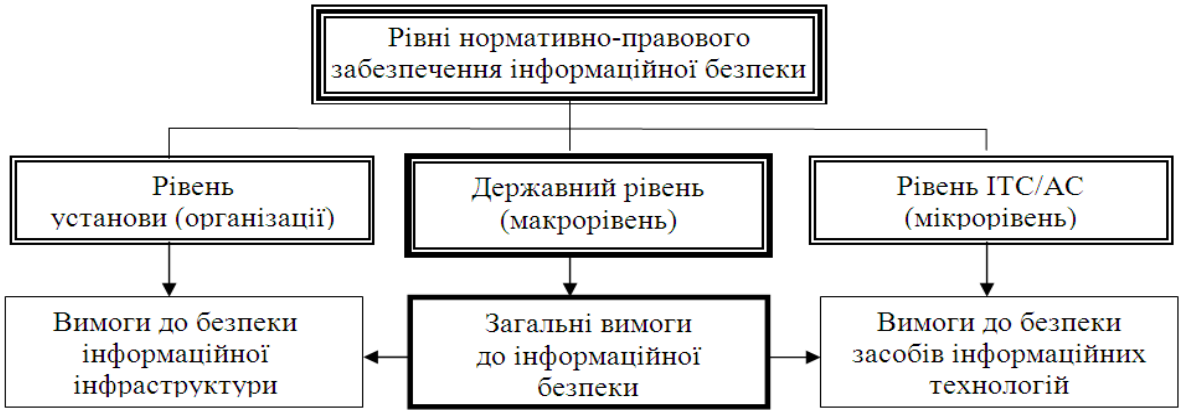

Рис. 2. Рівні нормативно-правового забезпечення інформаційної безпеки

.

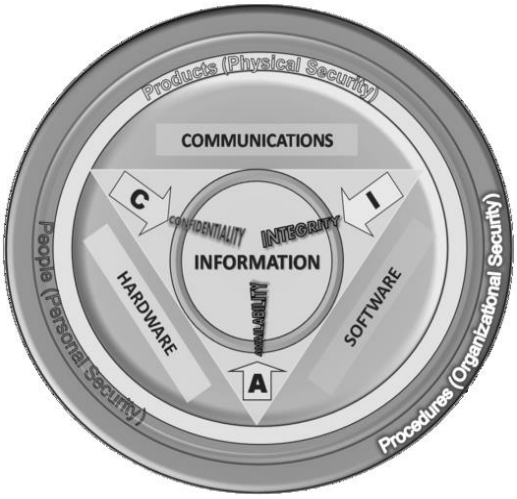

Рис. 3. Модель інформаційної безпеки в ІТС

Відповідно до СІБ, захищеною, вважається ІТС, яка відповідає встановленим вимогам і гарантіям щодо забезпечення конфіденційності, цілісності, доступності та спостережності інформаційних активів.

Інформаційна безпека представляє собою проблему високої складності. Забезпечення інформаційної безпеки потребує комплексного підходу до розробки засобів захисту як на організаційному, так і на технічному рівні, тобто таке управління, що забезпечує механізм, який дозволяє реалізувати інформаційну безпеку.

Управління інформаційною безпекою (англ. information security management) – частина загальної системи менеджменту (управління), метою якого є забезпечення конфіденційності, цілісності та доступності інформаційних активів (документів, носіїв, додатків, інформаційних систем, знань персоналу тощо). Це безперервний процес реалізації політики безпеки підприємства на постійній основі, а також її постійного оновлення.

Система управління інформаційною безпекою – СУІБ (англ. information security management system, ISMS) – частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Міжнародна стандартизація складових системи управління інформаційною безпекою формує три напрямки розвитку в даній сфері:

сімейство стандартів „Методи забезпечення безпеки" – ISO/IEC 27000-ISO/IEC 27037;

сімейство стандартів „Методи та засоби забезпечення безпеки" – ISO/IEC 15408 („Загальні критерії", 3 частини), ISO/IEC 13335 (5 частин), ISO/IEC 18045;

сімейство стандартів „Управління та аудиту інформаційних технологій" (CobIT, ITSM, ITIL та ін.).

Серед зазначеного, окреме місце займає система міжнародних стандартів щодо управління ІБ – адже для установ, організацій, підприємств, які провадять діяльність в межах України достатньо впровадження КСЗІ та отримання Атестату відповідності вимогам нормативних документів системи технічного захисту інформації України.

Стандарти управління інформаційною безпекою – це модель системи менеджменту, яка визначає загальну організацію, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т. ін. в контексті інформаційної безпеки. У процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої скорочення матеріальних втрат, зв'язаних з порушенням інформаційної безпеки, забезпечення не тільки надійного захисту інформації, але також організація ефективного доступу до даних та нормальна робота з ними.

Для установ, організацій, підприємств, які провадять діяльність на міжнародному рівні, важливою умовою підвищення ефективності цієї діяльності є наявність Сертифікату відповідності міжнародним стандартам серії ISO/IEC 27001 (оцінки і управління інформаційною безпекою) „Інформаційні технології – Засоби забезпечення безпеки", що ґрунтуються на авторитетних

британських стандартах BS 17799 (з 2000 р. признаних міжнародними під назвою "International Standart ISO/IEC 17799. Information technology – Code of practice for information security management".

Згідно ISO/IEC 27001: 2005 побудова ефективної системи УІБ можлива при реалізації напрямків А5-А15 (Додаток А ISO/IEC 27001: 2005) наведених в таблиці 1.

Таблиця 1

Напрямки побудови СУІБ згідно ISO/IEC 27000

<table>
<tr><td colspan="4">А.5 Політика в області безпеки</td></tr>
<tr><td colspan="4">А.6 Організація системи безпеки</td></tr>
<tr><td colspan="4">А.7 Класифікація активів та управління</td></tr>
<tr><td>А.8 Безпека та персонал</td><td>А.9 Фізична та зовнішня безпека</td><td>А.10 Менеджмент комп'ютерів та мереж</td><td rowspan="2">А.12 Придбання, розробка й обслуговування інформаційної системи</td></tr>
<tr><td colspan="3">А.11 Управління доступом до системи</td></tr>
<tr><td colspan="4">А.13 Менеджмент інцидентів інформаційної безпеки</td></tr>
<tr><td colspan="4">А.14 Забезпечення безперервності бізнесу</td></tr>
<tr><td colspan="4">А.15 Відповідність законодавства</td></tr>
</table>

Структура стандарту дозволяє вибрати ті засоби управління, які мають відношення до конкретної організації або сфери відповідальності всередині організації.

У зв'язку з цим, виділяється ряд ключових елементів управління, що подаються як фундаментальні. При цьому, поряд з елементами управління для комп'ютерів та комп'ютерних мереж, стандарт приділяє велику увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам.

Безумовно, що не всі пункти стандарту можливо застосовувати в умовах кожної організації, тому в стандарті реалізовано підхід, при якому його використовують як деяке "меню", з якого слід вибирати елементи, для конкретних умов. Цей вибір здійснюється на основі оцінки ризику та ретельно обґрунтовується.

В залежності від конфіденційності інформації, яка зберігається, обробляється та передається в організації, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні організації, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови СУІБ. Можливі наступні варіанти:

досягнення необхідного рівня інформаційної безпеки за мінімальних затрат і допустимого рівня обмежень на технології зберігання, оброблення та передавання інформації у організації;

досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технології зберігання, оброблення та передавання інформації у організації;

досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технології зберігання, оброблення та передавання інформації у організації.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.

Взагалі перелік стандартів серії ISO/IEC 27000 включає близько 20-ти найменувань – від стандарту ISO/IEC 27001 (Системи управління інформаційною безпекою) до стандарту ISO/IEC 27037 (Настанови з ідентифікації, виявлення, збору та збереження цифрових доказів). Найбільш значимі з них, впровадження яких вже здійснюється або очікується найближчим часом, приведені в таблиці 2.

Таблиця 2

Перелік чинних та перспективних стандартів серії ISO/IEC 27000

Шифр стандарту	Найменування (призначення) стандарту
ISO/IEC 27000: 2009	Управління ІБ. Короткий огляд і словник
ISO/IEC 27001: 2005	Системи управління ІБ. Вимоги
ISO/IEC 27002: 2005	Звід практики для управління ІБ (*ISO/IEC 17799:2005*)
ISO/IEC 27003: 2010	Керівництво по реалізації системи управління ІБ
ISO/IEC 27004: 2009	Вимірювання в управлінні ІБ
ISO/IEC 27005: 2008	Ризик-менеджмент ІБ
ISO/IEC 27006: 2007	Вимоги до органів аудиту і сертифікації СУІБ
ISO/IEC 27007: 2011	Настанови щодо аудиту ІБ системи управління
ISO/IEC 27011: 2008	Настанови щодо управління ІБ для телекомунікацій
ISO/IEC 27031: 2011	Настанови щодо інформаційно-комунікаційних технологій. Готовність до безперервності бізнесу.

Названі стандарти отримали широке розповсюдження і послужили поштовхом для створення національних нормативних документів в галузі інформаційної безпеки в багатьох країнах світу. Так, в Російській Федерації Федеральним агентством по технічному регулюванню і

метрології, починаючи з 2005 року, в прийнятих державних стандартах наводяться відповідні посилання на стандарти серії ISO 27001-27006, а з 2006 р. вже діє стандарт ГОСТ Р ИСО/МЭК 27001 „Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

В Україні, в 2012 р. презентовано державний стандарт ДСТУ ISO/IEC 27001:2010 „Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Система управління інформаційною безпекою. Вимоги".

Також, в якості галузевих, з березня 2011 р. прийняті два стандарти Національного банку України: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 „Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги" (ISO/IEC 27001: 2005, MOD); ГСТУ СУІБ 2.0/ISO/IEC 27002: 2010 „Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою" (ISO/IEC 27002: 2005, MOD).

Слід зазначити, що застосування ДСТУ ISO/IEC 27001 для банківських структур є обов'язковим, для структур з іншими видами діяльності – на власний розсуд. Окрім цього, для реалізації вимог СУІБ в Україні гармонізації потребують міжнародні стандарти ISO/IEC 27005: 2008 „Ризик-менеджмент ІБ" та ISO/IEC 27003:2010 „Керівництво по реалізації системи управління ІБ".

Перший надає структуру для визначення підходу до управління ризиками в залежності від області дії СУІБ, область застосування управління ризиками ІБ або сектора промисловості та процес оцінки інформаційних ризиків (ІР) (2 етапи):

аналіз ІР (ідентифікація і кількісна оцінка активів, загроз, існуючих засобів контролю, вразливостей і наслідків;

оцінювання ІР (управління ризиком на основі ітераційного підходу щодо його оцінки до отримання прийнятного значення).

Другий описує процес специфікації та проектування СУІБ з моменту початку проектування до подання планів впровадження системи. Метою стандарту є надання практичної допомоги при реалізації СУІБ у межах організації відповідно до ISO/IEC 27001: 2005. На основі стандарту ISO/IEC 27003: 2010 „Керівництво по реалізації системи управління ІБ" Департамент інформатизації Національного банку України розробив Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до галузевих стандартів Національного банку України з врахуванням особливостей банківської діяльності та вимог Національного банку України з питань ІБ.

Виходячи з загального призначення і практичної користі у встановленні контролю за інформаційною безпекою, на основі стандартів ISO/IEC 27001, 27002 та 27003 авторами розроблений алгоритм впровадження СУІБ при створенні (модернізації) комплексної системи захисту інформації (КСЗІ) в інформаційно-телекомунікаційній системі. Алгоритм включає 32 етапи – від усвідомлення цілей та вигод впровадження СУІБ до проведення аналізу СУІБ в АС з боку вищого керівництва і прийняття відповідного наказу про введення в дію СУІБ.

Також проведено порівняльний аналіз вимог нормативних документів системи технічного захисту інформації (т. з. НД ТЗІ), щодо створення КСЗІ в ІТС і вимог стандартів ISO/IEC 27001, 27002 і 27003, який свідчить про необхідність перегляду більше 10 вимог, прописаних в НД ТЗІ, пов'язаних з необхідністю ідентифікації активів, загроз, вразливостей, оцінкою та ранжуванням ризиків і проведенням аудиту.

Висновки й перспективи подальших досліджень

Загалом, питання ефективної реалізації будь-якого стандарту невід'ємне від його інструментальних можливостей, що дозволяє автоматизувати роботу, забезпечити гнучкість і адаптивність застосування різноманітних "паперових" методик. Найкращими можливостями в цьому плані володіє стандарт ISO/IEC 27002: 2005 (ISO 17799).

Виходячи з зазначеного, доцільно доповнити діючі та перспективні стандарти такими програмними продуктами як довідник з питань інформаційної безпеки, гіпертекстовий довідник з питань захисту інформації, керівництво для співробітників служби безпеки, різноманітні демонстраційні версії і презентації, зручною навігацією.

Література

1. Конституція України, 1996 / [Електронний ресурс] // – Режим доступу: http://zakon4. rada.gov.ua/laws/show/ 254к/96-вр – Назва з екрану. **2. Закон України** Про основи національної безпеки України**:** Закон від 2003 / [Електронний ресурс] // Верховна Рада України – Режим доступу: http://zakon4.rada.gov.ua/laws/show /964-15 - Назва з екрану. **3. Указ Президента України** Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ від 26.05.2015 / [Електронний ресурс] // РНБО – Режим доступу: №287/2015.http://zakon5.rada.gov.ua/laws/show/287/2015 – Назва з екрану. **4. Закон України** Про захист інформації в інформаційно-телекомунікаційних системах: Закон від 05.07.1994 № 81/94-ВР / [Електронний ресурс] // Верховна Рада України – Режим доступу: http://zakon5.rada.gov.ua/laws/show/80/94-вр/ed20111231 - Назва з екрану.

АНАЛИЗ НОРМАТИВНО-ПРАВОВЫХ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ АСПЕКТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вячеслав Владимирович Овсянников (канд. техн. наук)
Святослав Владимирович Дехтярь
Светлана Анатольевна Паламарчук
Юлия Александровна Черныш
Александр Витальевич Шемендюк

Военный институт телекоммуникаций и информатизации, Киев, Украина

Учитывая мировые тенденции информатизации современного общества, стремительное развитие информационных технологий и интенсивное внедрение информационно-телекоммуникационных систем во все сферы жизнедеятельности государства и общества, возникает необходимость в определении понятия и содержания информационной безопасности и системы ее обеспечения.

В статье проанализированы требования нормативно-правовых актов Украины и международных стандартов ISO/IEC по обеспечению информационной безопасности, приведена сущность основных понятий и содержания информационной безопасности.

В рамках стандартов международного и национального уровней по информационной безопасности определяются требования к защите информации (ее свойств). В англоязычных стандартах, это классическая модель СИА, по обеспечению требований конфиденциальности, целостности и доступности информации. Отдельно выносится требование наблюдаемости.

В международных стандартах особое внимание также уделяется системе управления информационной безопасностью.

Ключевые слова: *информационная безопасность; угрозы информационной безопасности; угрозы кибербезопасности и безопасности информационных ресурсов; стандарты ISO / IEC, стратегия национальной безопасности.*

ANALYSIS OF LEGAL, ORGANIZATIONAL AND TECHNICAL ASPECTS OF INFORMATION SECURITY

Viacheslav V. Ovsiannikov ***(Candidate of Technical Sciences)***
Sviatoslav V. Dekhtiar
Svitlana A. Palamarchuk
Yuliia O. Chernysh
Oleksandr V. Shemendiuk

Military Institute of Telecommunications and Information, Kyiv, Ukraine

Analysis of legal, organizational and technical aspects of information security given the global trends of informatization of modern society, the rapid development of information technology and intensive implementation of information and telecommunication systems in all spheres of state and society, there is a need for defining the concept and content of the information security system and its software.

The requirements of Ukraine legal acts and international information security standards ISO/IEC were analyzed. The nature of basic concepts and content of the information security was given.

In the framework of international and national standards for information security levels defined requirements for protection (of properties). In the English-language standards is a classic CIA model, to ensure the requirements of confidentiality, integrity and availability of information. Separately requirement imposed observability.

At international standards, special attention is also paid to information security management system.

Keywords: *information security; threats to information security; cyber security threats and information resources; Standards ISO / IEC, national security strategy.*

References

1. The Constitution of Ukraine (1996). [*Konstytutsiya Ukrayiny*], http://zakon4.rada.gov.ua/laws/show/254k/96-BP. **2. The Law** of Ukraine (2003) On National Security of Ukraine [*Pro osnovy natsional'noyi bezpeky Ukrayiny*], The Verkhovna Rada of Ukraine, http://zakon4.rada.gov.ua/laws/show/964-15. **3. Decree** of the President of Ukraine On the decision of the National Security and Defense Council of Ukraine on May 6, 2015 "On National Security Strategy of Ukraine" (2015) [*Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 6 travnya 2015 roku "Pro Stratehiyu natsional'noyi bezpeky Ukrayiny"*], NSDC, http: //zakon5.rada.gov.ua/laws/show/287/2015. **4. The Law** of Ukraine On protection of information in telecommunication systems (1994) [*Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh*], Verkhovna Rada of Ukraine, http://zakon5.rada.gov.ua/laws/show/80/94-VR/ed20,111,231.

Отримано: 11.10.2015 р.