Практичні аспекти економічної безпеки держави

УДК 323:351

Островий Олексій Володимирович
здобувач кафедри управління персоналом та економіки підприємства
Донецький державний університет управління
Островой Алексей Владимирович
соискатель кафедры управления персоналом и экономики предприятия
Донецкий государственный университет управления
Ostrovoy Alexey
Applicant at the
Department of Personnel Management and Enterprise Economics
Donetsk State University of Management

ІНСТРУМЕНТИ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ
ИНСТРУМЕНТЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ
INSTRUMENTS OF THE STATE POLICY TO ENSURE KIBERNETIC SECURITY

Анотація. *В статті обґрунтовано доцільність незалежного аудиту, а також пов'язаних з ним процесів стандартизації та сертифікації як складових національної системи кібербезпеки України та інструментів формування ефективної державної політики в сфері кіберзахисту.*

Сформовано поняття аудиту в сфері інформаційної безпеки та визначено його об'єкти.

З метою підвищення ефективності аудиту та пов'язаних з ним процесів, виокремлено різні групи оцінки об'єктів системи інформаційної

безпеки в залежності від періоду, за який проводиться аналіз, оцінивши їх стан в минулому, теперішньому та майбутньому часі. Виокремлено основні види аудиту: галузевий аудит, аудит на відповідність вимогам конкретного стандарту і відповідної сертифікації та аудит кібербезпеки. Сфокусовано увагу на аудиті кібербезпеки.

Запропоновано методику проведення аудиту кібербезпеки підприємства (організації) за основними модулями.

В результаті проведеного дослідження визначено проблеми здійснення аудиту в сфері кібербезпеки. Акцентовано увагу на особливостях державної політики щодо стандартизації технічного захисту інформації, визначено основні недоліки. Досліджено сучасні напрацювання в сфері міжнародної стандартизації управління інформаційною безпекою. Проаналізовано особливості державної політики в сфері стандартизації кіберзбезпеки, яку сформовано у ряді країн світу у відповідь на зростаючий рівень кіберзагроз.

Актуалізовано формування комплексної галузевої системи кібербезпеки, яка зорієнтована на міжнародні норми та досвід. Сформовано рекомендації щодо здійснення аудиту в сфері інформаційної безпеки та розвитку державної політики стандартизації та сертифікації.

Ключові слова: *державна політика, інформаційна безпека, кібербезпека, аудит, сертифікація, стандартизація.*

Аннотация. *В статье обоснована целесообразность независимого аудита, а также связанных с ним процессов стандартизации и сертификации как составляющих национальной системы кибербезопасности Украины и инструментов формирования эффективной государственной политики в сфере киберзащиты.*

Сформировано понятие аудита в сфере информационной безопасности и определены его объекты.

С целью повышения эффективности аудита и связанных с ним процессов, выделены различные группы оценки объектов системы информационной безопасности в зависимости от периода, за который производится анализ, оценив их состояние в прошлом, настоящем и будущем времени. Выделены основные виды аудита: отраслевой аудит, аудит на соответствие требованиям конкретного стандарта и соответствующей сертификации и аудит кибербезопасности. Сфокусировано внимание на аудите кибербезопасности.

Предложена методика проведения аудита кибербезопасности предприятия (организации) по основным модулям.

В результате проведенного исследования определены проблемы аудита в сфере кибербезопасности. Акцентировано внимание на особенностях государственной политики по стандартизации технической защиты информации, определены основные недостатки. Исследованы современные наработки в сфере международной стандартизации управления информационной безопасностью. Проанализированы особенности государственной политики в сфере стандартизации киберзбезопасности, сформированной в ряде стран мира в ответ на растущий уровень киберугроз.

Актуализировано формирование комплексной отраслевой системы кибербезопасности, ориентированной на международные нормы и опыт. Сформированы рекомендации по аудиту в сфере информационной безопасности и развития государственной политики стандартизации и сертификации.

Ключевые слова: *государственная политика, информационная безопасность, кибербезопасность, аудит, сертификация, стандартизация.*

Summary. *The article substantiates the feasibility of an independent audit, as well as related standardization and certification processes as part of the national cyber security system of Ukraine, and tools for the formation of an effective state policy in the field of cyber defense.*

The concept of audit in the field of information security has been formed and its objects have been defined.

In order to improve the efficiency of the audit and related processes, various groups for evaluating information security objects have been allocated, depending on the period for which the analysis has been made, assessing their condition in the past, present and future tense. The main types of audit (industry audit, audit for compliance with the requirements of a particular standard and relevant certification and cyber security audit) have been highlighted. Focus on cybersecurity audit has been made.

Methodology for conducting an audit of the enterprise (organization) cybersecurity for the main modules has been proposed.

As a result of the study, audit problems in the field of cyber security have been identified. The attention has been focused on the peculiarities of the state policy on the standardization of technical information protection, the main drawbacks have been identified. Modern developments in the field of international standardization for information security management have been researched. The features of the state policy in the field of cyber-security standardization, formed in a number of countries in response to the growing level of cyber threats, have been analyzed.

The formation of an integrated industry-wide cybersecurity system focused on international norms and experience has been updated. Recommendations for the audit in the field of information security and state policy standardization and certification development have been formed.

Key words: *state policy, information security, cybersecurity, auditing, certification, standardization.*

Постановка проблеми. Аналіз основних статистичних показників, які характеризують рівень використання інформаційно-комунікаційних технологій на підприємствах та в організаціях України, дозволив констатувати зростання кількості комп'ютерної техніки, підвищення доступу до мережі Інтернет та збільшення рівня використання інформаційно-комунікаційних технологій в своїй діяльності.

Але запровадження сучасних цифрових технологій створило не лише передумови для розвитку підприємств та національної економіки в цілому, але й спричинило посилення вразливості в комп'ютерних мережах, підвищення ризику виникнення кіберінцидентів та зростання рівня злочинності в сфері інформаційно-комунікаційних технологій.

Так, темп зростання кількості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за 2014-2017 роки склав 480,8%. За 8 місяців 2018 року цей показник вже перевищив рівень 2016 року на 117,9 % [1, с. 157].

Така ситуація потребує аналізу ситуації та формування обґрунтованої дієвої державної політики, яка спрямована на забезпечення інформаційної безпеки та використовує відповідні сучасні інструменти, що, в свою чергу, актуалізує проблеми аудиту, стандартизації та сертифікації в цій сфері.

Аналіз останніх досліджень і публікацій. Значний вклад у розвиток основних аспектів забезпечення інформаційної безпеки знайшли відображення у працях Л.Гнатюка [2], І. Діордіци [3], Д. Дубова [4], В. Ліпкана [5], В. Шеломенцева [6] та інших.

Однак в умовах формування ефективної державної політики в сфері кіберзахисту, питання незалежного аудиту та пов'язаних з ним проблем стандартизації та сертифікації потребують більш глибокого наукового

вивчення. Це дозволить забезпечити належний рівень кібербезпеки, як однієї зі складових національної безпеки.

Формулювання цілей статті. Метою статті є формування інструментів державної політики забезпечення кібернетичної безпеки.

Виклад основного матеріалу. Стандартизація та сертифікація інформаційної безпеки, гармонізація з міжнародними стандартами, здійснення незалежного аудиту в цій сфері є інструментами державної політики та складовими національної системи кібербезпеки України, яка знаходиться на етапі формування.

Враховуючи тематику дослідження, вважаємо за доцільне визначитися з поняттям аудиту в сфері інформаційної безпеки.

Пропонуємо під аудитом розуміти процес, під час якого компетентна, незалежна особа оцінює кількісну інформацію, яка стосується діяльності певної системи інформаційної безпеки з метою формування висновків про відповідність цієї інформації встановленим критеріям та розробки заходів щодо виправлення викритих недоліків і попередження загроз.

До об’єктів аудиту в сфері інформаційної безпеки слід віднести окремі і взаємопов’язані управлінські, організаційні, інформаційні та інші форми функціонування відповідної системи, що визначаються, стан яких може бути оцінено кількісно та якісно.

Слід зазначити, що з метою підвищення ефективності аудиту та пов’язаних з ним процесів, представляється доцільним виокремлення різних груп оцінки об’єктів системи інформаційної безпеки в залежності від періоду, за який проводиться аналіз, оцінивши їх стан у часі (рис.1).

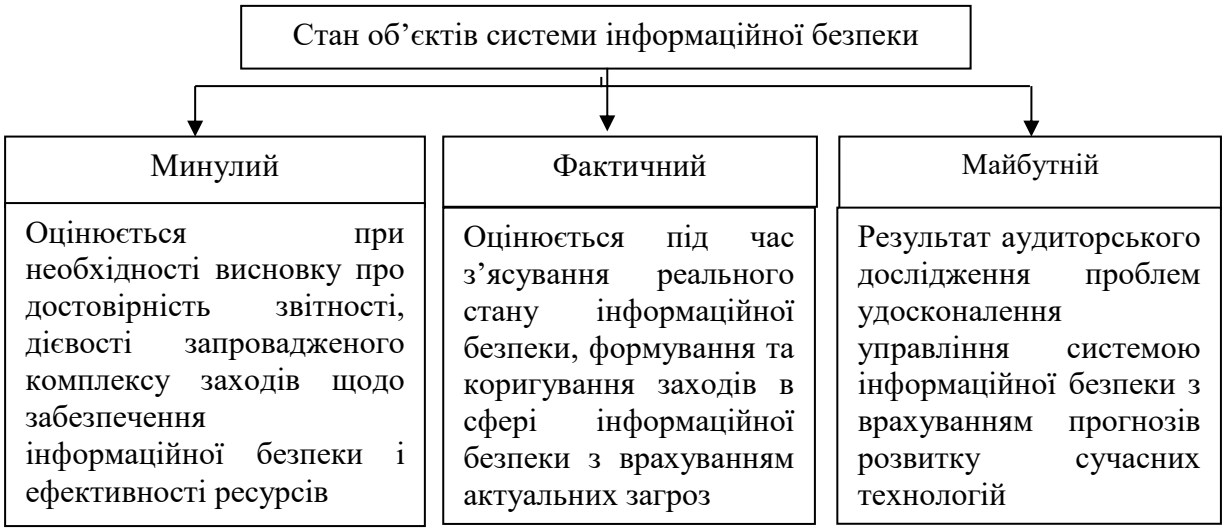

Рис. 1. Групи оцінки об'єктів системи інформаційної безпеки в залежності від часу

Джерело: сформовано автором

Звертаючи увагу на аудит в сфері інформаційної безпеки, слід виокремити такі його основні види: галузевий аудит, аудит на відповідність вимогам конкретного стандарту і відповідної сертифікації та аудит кібербезпеки (рис. 2).

Рис. 2. Основні види аудиту в сфері інформаційної безпеки

Джерело: сформовано автором

Однак, слід вказати на той факт, що перші два види аудиту суворо обмежені певною галуззю та сферою дії (охопленням) конкретного стандарту і не можуть відображати повної картини захищеності організації.

Аудит кібербезпеки є набагато ширшим та являє собою комплексну оцінку ступеню захищеності організації, яка складається з певних модулів,

що виконуються цілком, або вибірково, в залежності від поставленої цілі, здійснюється перевірка відповідності регуляторним нормам, оцінка безпеки роботи з контрагентами та за результатами якої формуються рекомендації практичного і методичного характеру.

Методика проведення аудиту кібербезпеки підприємства (організації) за основними модулями наведена у табл.1.

Таблиця 1

Методика проведення аудиту кібербезпеки

№	Модуль	Мета	Процедура	Результат
1	Аудит бізнес-процесів та організаційної структури	обґрунтування розвитку кібербезпеки не як витратної	Знайомство з організацією, її структурою управління. Оцінка	Розуміння процесів діяльності, формування переліку критично важливих

Продовження табл. 1

		складової, а як частини розвитку	ризиків	процесів і більш небезпечних ризиків.
2	Аудит процесів управління і забезпечення кібербезпеки	Підготовка до активної роботи і ефективного реагування в разі кіберінцидентів або під час кібератаки.	У сучасній компанії сфера дії кібербезпеки розподілена між підрозділами, які безпосередньо та опосередковано впливають на рівень захисту, що потребує оцінки ефективності процесів управління кібербезпекою і взаємодії між елементами	Формування карти розвитку існуючих і впровадження нових процесів, які повинні забезпечити необхідний рівень кіберзахисту бізнесу.
3	Оцінка технічної захищеності (сканування і тестування на проникнення)	Періодична незалежна оцінка: зовнішнє і внутрішнє сканування для визначення вразливостей, тестування на проникнення ззовні і зсередини компанії.	Тестування на проникнення «наосліп» (Blackbox), аудит засобів безпеки і налаштувань, «біле» тестування на проникнення (Whitebox) з усіма конфігураціями і доступами на руках.	Результати етапу будуть цікаві технічним підрозділам і фахівцям, які матимуть практичну користь з рекомендацій, складених консультантами і «білими» хакерами
4	Оцінка стійкості	Перевірка стійкості компанії	Залежно від специфіки проекту	Результат багато в чому залежить не від

	організації до соціальної інженерії	до елементів соціальної інженерії: фішинг та вішинг	проводяться масові або персоналізовані фішингові розсилки, які фокусуються на конкретних співробітників компанії	налаштувань технічних засобів безпеки, а від підготовки співробітників компанії до таких дій з боку зловмисників.
5	Аудит «тіньових» інформаційних технологій	Виявлення технічних пристроїв, які не належать до розряду корпоративних	виявлення несанкціонованих програмних і апаратних продуктів в компанії, які можуть або використовуються зловмисниками	Уникнення хаосу з точки зору контролю за умов запровадження концепції «принеси свій пристрій»
6	Аудит безпеки процесів аутсорсингу	Оцінка ризиків співробітництва зі сторонніми компаніями	Перевірка існуючих контрагентів та умов роботи з ними, процесу залучення нових виконавців до роботи з компанією	Управління ризиками співробітництва зі сторонніми компаніями

Джерело: розроблено автором

Однак, в контексті дослідження аудиту в сфері кібербезпеки, слід вказати на ряд проблем, які потребують уваги. Серед основних з них слід виокремити такі:

необхідність прийняття відповідних нормативних документів, які спрямовані на формування та практичну реалізацію інституту незалежних аудиторів;

унормування порядку та методики здійснення аудиту кібербезпеки, що обумовлено його здійсненням, згідно з Законом «Про основні засади забезпечення кібербезпеки України», на основі міжнародних стандартів. Однак, в положеннях цього документу відсутні посилання на Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», в статті 8 якого визначено, що «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» [7].

У цьому контексті слід погодитись з Л.С. Гнатюком [2], який звертає увагу на той факт, що під дію цієї норми потрапляють практично всі об'єкти критичної інформаційної інфраструктури, значна кількість яких знаходиться в недержавному секторі (наприклад, в енергетиці, транспортній системі, телеком-індустрії, фармацевтиці тощо).

Однак, Комплексна система захисту інформації (КСЗІ), яка базується на вітчизняному стандарті КСЗІ НД ТЗІ 2.5- 004-99, а також вимога її обов'язкового застосування на об'єктах часто критикується як спеціалістами, так і представниками сфери бізнесу [8; 9; 10].

Зазначимо, що в Україні в сфері державної стандартизації технічного захисту інформації діє єдина серія нормативних документів (виключенням є лише банківський сектор), де основним є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [11], розроблений на основі Канадських критеріїв безпеки комп'ютерних систем, з урахуванням прийнятих у 2005 році міжнародних «Загальних критеріїв» (ISO 15408), що є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

Однак, критерієм захищеності інформації в цьому документі виступає відповідність архітектури та параметрів програмно-апаратних засобів об'єкта чіткому регламенту – КСЗІ, що відрізняє його від серії ISO/IEC 27000, яка концентрується, переважно, на менеджменті інформаційної безпеки і є найпоширенішою в світі.

Цілком слушною в цьому контексті є думка фахівців [2], які звертають увагу на той факт, що внутрішня структура і механізм впровадження концепції КСЗІ не відповідає вимогам сучасного

кіберзахисту, особливо це стосується недержавного сектору. Така ситуація обумовлена рядом недоліків, основні з яких відзначено на рис. 3.

Рис. 3. Основні недоліки Комплексної системи захисту інформації

Джерело: сформовано автором на основі [2; 9]

Відзначаючи основні недоліки вітчизняної КСЗІ, слід звернути увагу на сучасні напрацювання в сфері міжнародної стандартизації управління інформаційною безпекою, які застосовуються в розвинутих країнах, не мають вищевказаних вад та є відкритими для використання (табл.2).

Таблиця 2

Міжнародні стандарти кібербезпеки

Назва	Розробник	Характеристики	Результат
Серія міжнародних стандартів ISO/IEC 270009	Міжнародна організація з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC),	Модель (фреймворк) для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки як на загальному рівні (27001), так і в окремих секторах та галузях (фінанси,	Оптимізація процесів захисту інформаційних ресурсів і управління ризиками для них.

		транспорт, енергетика, охорона здоров'я, оператори зв'язку, хмарні обчислення, інфраструктурні проекти, аудит і сертифікація тощо). Постійно доповнюється новими документами	
National Institute of Standarts and Technology Cybersecurity Framework (NIST CSF)	Американський Інститут стандартів і технологій (для організацій приватного сектору США)	Відкритий, призначений виключно для добровільного використання. Достатньо «гнучкий» для адаптації в різних умовах/країнах, що зумовило його поширеність у світі. Уперше NIST CSF був випущений у 2014 році, є оновлені версії	комплекс методологій та рекомендацій щодо зниження IT-ризиків, а також запобігання, моніторингу і реагування на кібератаки.

Джерело: складено автором на основі [2; 12; 13]

Однак, зупиняючись на серії міжнародних стандартів ISO/IEC 27001 слід констатувати, що в якості державного стандарту в Україні визнано лише перший варіант ISO/IEC 27001, який застосовано в банківській сфері у вигляді вимог СОУ Н НБУ 65.1 СУІБ 1.0: 201010 (відповідно до закону «Про основні засади забезпечення кібербезпеки України» Національний банк України - один з суб'єктів національної системи кібербезпеки) [14]. Нажаль, в інших галузях ці стандарти поки не використовуються, що обумовлено рядом причин, основною з яких відзначається правова неврегульованість. Хоча міжнародні стандарти з інформаційної безпеки ISA 099 та IEC 62443 є спеціалізованими відкритими стандартами, пристосованими для використання на об'єктах критичної інфраструктури приватної форми власності.

Як свідчать результати аналізу зарубіжного досвіду, з метою недопущення недоброчесної конкуренції та монополізації регуляторної діяльності в цій сфері, практикується формування та використання альтернативних стандартів та моделей з кібербезпеки, призначених для різних галузей, що знаходяться у недержавному секторі.

Так, наприклад, в США, наряду з використанням приватними структурами NIST Cybersecurity Framework, в галузі енергетики діють стандарти NERC CIP [15], розроблені неприбутковою недержавною організацією Північноамериканською корпорацією з забезпечення надійності електросистем (North American Electric Reliability Corporation). Слід вказати, що ці стандарти рекомендовані до використання експертами київського відділення ISACA (Міжнародна професійна неприбуткова асоціація, орієнтована на IT-менеджмент) у вітчизняному паливно-енергетичному комплексі.

Дослідження європейського досвіду в контексті даного питання дозволило зазначити, що країни ЄС працюють над створенням на основі існуючого Європейського агентства з питань мережевої та інформаційної безпеки (ENISA) Агентства ЄС із кібербезпеки та запровадженням сучасної європейської системи сертифікації, яка здатна забезпечити безпеку цифрових продуктів та послуг [16].

Зазначимо, що таке Агентство матиме постійний мандат та можливість надавати державам-членам ефективну допомогу та реагувати на кібератаки. А нові європейські сертифікати спрямовані на забезпечення кібербезпеки у сфері критичної інфраструктури (енергетичні та транспортні мережі). Прогнозується, що визнання цих сертифікатів державами-членами ЄС сприятиме зниженню адміністративних витрат та витрат окремих компаній.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Формування державної політики забезпечення кібербезпеки, адекватної сучасним загрозам, потребує розробки та використання сучасних інструментів, серед яких доцільно виокремити аудит, процеси стандартизації та сертифікації. Зазначимо, шо для національної економіки актуалізується формування комплексної галузевої системи кібербезпеки, яка зорієнтована на міжнародні норми та

досвід. Основні вітчизняні напрацювання у цьому напрямі пов'язані лише з певними практиками, які запроваджено окремими галузями та підприємствами різних форм власності.

У зв'язку з цим є необхідність у формуванні та вдосконаленні вже існуючої відповідної нормативної бази, спрямованої на забезпечення кібернетичної безпеки, що входить до основних задач і перспектив подальших досліджень.

Література

1. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні / М.О. Кравцова // Вісник Кримінологічної асоціації України. – 2018. – № 2(19) – С. 155-166.
2. Гнатюк С.Л. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні: [аналітична записка] / С.Л. Гнатюк. URL: http://www.niss.gov.ua/content/articles/files/kiberbezpek-d3e61.pdf
3. Діордіца І. Поняття та зміст кіберзлочинності / І. Діордіца. URL: http://goal-int.org/ponyattya-ta-zmistkiberzlochinnosti
4. Дубов Д. В. Стратегічні аспекти кібербезпеки України / Д. В. Дубов // Стратегічні пріоритети : [наук.-аналіт. щокварт. зб.] / Нац. ін-т стратег. дослідж. К. : НІСД, 2013. № 4 (29). С. 119–126.
5. Ліпкан В. Національна і міжнародна безпека у визначеннях та поняттях / Ліпкан В., Ліпкан О. Вид. 2-ге, доп. і перероб. К.: Текст, 2008. 400 с.
6. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 312-320.

7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5.07.1994 р. // Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
8. Грабовий А. Закон про кібербезпеку та Стратегія кібербезпеки України / А. Грабовий // Юрист & Закон. 2017. № 26. URL: http://uz.ligazakon.ua/ua/magazine_article/ EA010553
9. Янковский А. Що не так з проектом про кібербезпеку та як його вдосконалити / А. Янковский. URL: https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci
10. Бараш Л. Кибербезопасность в Украине. Дискуссия / Л. Бараш. URL: http://ko.com.ua/ kiberbezopasnost_v_ukraine_diskussiya_121089
11. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанціонованого доступу». URL: http://am-soft.ua/files/KSZI/2.5-004-99.pdf
12. ISO/IEC 27000 family - Information security management systems. URL: https://www.iso.org/isoiec-27001-information-security.html
13. NIST Releases Version 1.1 of its Popular Cybersecurity Framework. URL: https://www.nist.gov/cyberframework/draft-version-11
14. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD) Стандарт організації України. URL: https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf
15. CIP Standards. URL: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
16. В ЄС створять агентство із кібербезпеки та нові сертифікати для цифрових продуктів. URL: https://www.unian.ua/science/2143199-v-es-stvoryat-agentstvo-iz-kiberbezpeki-ta-novi-sertifikati-dlya-tsifrovih-produktiv.html

References

1. Kravcova M.O. (2018) Suchasnyj stan i naprjamy protydiji kiberzlochynnosti v Ukrajini [The current state and directions of counteraction to cybercrime in Ukraine]. Visnyk Kryminologhichnoji asociaciji Ukrajiny [Bulletin of the Criminological Association of Ukraine], No.2 (19), pp. 155-166. (in Ukrainian).
2. Ghnatjuk S.L. Aktualjni pytannja rozvytku derzhavno-pryvatnoji vzajemodiji u sferi zabezpechennja kiberbezpeky v Ukrajini: analitychna zapyska [Topical issues of development of public-private interaction in the field of cyber security in Ukraine: analytical note]. Available at: http://www.niss.gov.ua/ content/articles/files/kiberbezpek-d3e61.pdf
3. Diordica I. Ponjattja ta zmist kiberzlochynnosti [The concept and content of cybercrime]. Available at: http://goal-int.org/ponyattya-ta-zmistkiberzlochinnosti.
4. Dubov D. V. (2013) Strateghichni aspekty kiberbezpeky Ukrajiny [Strategic Aspects of Cybersecurity in Ukraine]. Strateghichni priorytety : [nauk.-analit. shhokvart. zb.] [Strategic priorities: [scientific and analytical quarterly collection]]. K. : National Institute for Strategic Studies, No. 4 (29). – PP. 119-126. (in Ukrainian).
5. Lipkan V., Lipkan O. (2008) Nacionaljna i mizhnarodna bezpeka u vyznachennjakh ta ponjattjakh [National and international security in definitions and concepts]– Edition. 2nd. K. : Text, 400 p. (in Ukrainian).
6. Shelomencev V. P. (2012) Pravove zabezpechennja systemy kibernetychnoji bezpeky Ukrajiny ta osnovni naprjamy jiji udoskonalennja [Legal support of the system of cybernetic security of Ukraine and the main directions of its improvement]. Borotjba z orghanizovanoju zlochynnistju i korupcijeju (teorija i praktyka) [Fighting Organized Crime and Corruption (theory and practice)] No. 1. – PP. 312-320. (in Ukrainian).

7. Zakon Ukrajiny «Pro zakhyst informaciji v informacijno-telekomunikacijnykh systemakh» vid 5.07.1994 r [Law of Ukraine «On Protection of Information in Information and Telecommunication Systems» of July 5, 1994]. Vidomosti Verkhovnoji Rady Ukrajiny (VVR), 1994, N 31, st.286 [Bulletin of the Verkhovna Rada of Ukraine, 1994, No.31] Available at: https://zakon.rada.gov.ua/laws/show/80/94-вр
8. Ghrabovyj A. (2017) Zakon pro kiberbezpeku ta Strateghija kiberbezpeky Ukrajiny [Cybersecurity Act and Cybersecurity Strategy of Ukraine]. Juryst & Zakon [Lawyer & Law], No.26. Available at: http://uz. ligazakon.ua/ua/ magazine_article/EA010553
9. Jankovskyj A. (2017) Shho ne tak z proektom pro kiberbezpeku ta jak jogho vdoskonalyty [What's wrong with the cybersecurity project and how to improve it]. Available at: https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci
10. Barash L. Kyberbezopasnostj v Ukrayne. Dyskussyja [Cybersecurity in Ukraine. The discussion] Available at: http://ko.com.ua/ kiberbezopasnost_v_ukraine_diskussiya_121089
11. ND TZI 2.5-004-99 «Kryteriji ocinky zakhyshhenosti informaciji v komp'juternykh systemakh vid nesancionovanogho dostupu» [ND TZI 2.5-004-99 "Criteria for assessing information security in computer systems from unsanctioned access"] Available at: http://am-soft.ua/files/KSZI/2.5-004-99.pdf
12. ISO/IEC 27000 family - Information security management systems Available at: https://www.iso.org/isoiec-27001-information-security.html
13. NIST Releases Version 1.1 of its Popular Cybersecurity Framework Available at: https://www.nist.gov /cyberframework/draft-version-11
14. Metody zakhystu v bankivsjkij dijaljnosti systema upravlinnja informacijnoju bezpekoju. Vymoghy (ISO/IEC 27001:2005, MOD) Standart orghanizaciji Ukrajiny [Methods of protection in banking activity information security

management system. Requirements (ISO/IEC 27001:2005, MOD) The standard of organization of Ukraine] Available at: https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf

15. CIP Standards. Available at: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
16. V JeS stvorjatj aghentstvo iz kiberbezpeky ta novi sertyfikaty dlja cyfrovykh produktiv [The EU will create a cyber security agency and new certificates for digital products]. Available at: https://www.unian.ua/science/2143199-v-es-stvoryat-agentstvo-iz-kiberbezpeki-ta-novi-sertifikati-dlya-tsifrovih-produktiv.html