УДК 519.217.2+338+331

С. Л. Волков, к.т.н., **Н. Ф. Казакова,** д.т.н., **Ю. В. Щербина,** к.т.н.

Одеська державна академія технічного регулювання та якості, м. Одеса

СУЧАСНІ ПРОБЛЕМИ БЕЗПЕКИ КІБЕРНЕТИЧНОГО ПРОСТОРУ

У статті розглянуто проблеми сучасного стану кібернетичного простору. Проаналізовано проблеми, що виникають при використанні відкритого Internet-середовища зловмисниками та можливі шляхи удосконалення методології побудови систем кібернетичного захисту. Розглянуто структуру стандарту ISO/IEC 27032:2012 і визначення у ньому кібернетичного простору та основних суміжних із ним понять. Зроблено висновок про необхідність пошуку нової, більш досконалої моделі захисту та методології оцінки інформаційної безпеки а також способів побудови адекватних загрозам систем захисту.

Ключові слова: *стандарти інформаційної безпеки, нормативно-правові документи, політика безпеки, управління ризиками, інформаційна безпека, інформаційний захист, кібернетична безпека, кіберпростір, кібернетична зброя, кіберзлочинність, Internet-простір, автоматизація управління, управління безпекою, стейкхолдер.*

S. L. Volkov, PhD, **N. F. Kazakova,** DSc, **Yu. V. Shcherbina,** PhD

CURRENT PROBLEMS OF THE CYBERNETIC SPACE SECURITY

The article deals with the problems of information security in modern cyberspace. The problems arising from the use of an open Internet environment by hackers are analyzed, taking into account the introduction of such modern intelligent technologies as "embedded systems", "smart cities", "big data", expert systems and decision-making support systems, as well as intelligent infrastructure management systems. The evolution of the international regulatory framework defining information security principles is considered. Prerequisites for the emergence and implementation of information concepts such as cyberspace and cybersecurity, as well as related concepts, have been analyzed and described in terms of information security. An analysis of the structure of the ISO / IEC 27032: 2012 standard is given, in which the formal definition of the new terminology is presented and the main subjects of information relations responsible for security are identified. Based on the analysis, it was shown that the reasons for the complexity of creating modern information protection systems are the increasing complexity of software and hardware of modern telecommunications systems and a significant expansion of the range of information services provided to users in the Internet environment. It is noted that the emergence of intelligent automation technology requires finding a new set of protection functions and means to ensure its security. The problems in the existing national regulatory framework governing the issues of information security are identified, and the conclusion is drawn on the need to improve it. It justifies the need to search for a new, more advanced protection model and methodology for assessing threats and information security, as well as tools for building protection systems that are adequate to modern threats.

Keywords: *information security standards, regulatory documents, security policy, risk management, information security, information protection, cyber security, cyberspace, cyberweapon, cybercrime, Internet space, management automation, security management, stakeholder.*

С. Л. Волков, к.т.н., **Н. Ф. Казакова,** д.т.н., **Ю. В. Щербина,** к.т.н.

СОВРЕМЕННЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ КИБЕРНЕТИЧЕСКОГО ПРОСТРАНСТВА

В статье рассмотрены проблемы текущего состояния кибернетического пространства. Проанализированы проблемы, возникающие при использовании открытого Internet-пространства злоумышленниками и возможные пути совершенствования методологии построения систем киберзащиты. Рассмотрена структура стандарта ISO/IEC 27032:2012 и определения в нем кибернетического пространства, а также, основных смежных понятий. В результате получены выводы о необ-

ходимости совершенствования модели защиты и методологии оценки защищенности, а также способов построения адекватных угрозам систем защиты.

Ключевые слова: *стандарты информационной безопасности, нормативно-правовые документы, политика безопасности, управление рисками, информационная безопасность, информационная защита, кибернетическая безопасность, киберпространство, кибернетическое оружие, киберпреступность, Internet-пространство, автоматизация управления, управление безопасностью, стейкхолдер.*

DOI 10.32684/2412-5288-2018-2-13-6-12

Вступ

Інформатизація усіх сфер життєдіяльності суспільства приводить до суттєвого розширення середовища експлуатації систем автоматизованого управління інформаційними і технологічними процесами. Удосконалення інформаційних технологій, що забезпечують створення нових видів послуг у Internet-середовищі, разом із позитивними сторонами, має і негативні наслідки.

Перша проблема полягає у підвищенні структурної складності програмного та апаратного забезпечення інформаційно-телекомунікаційних систем, що приводить до зниження їх надійності. Об'єднання у загальну систему великої кількості високонадійних компонентів не робить автоматично усю систему також високонадійною. Зазвичай загальна надійність навпаки, знижується. Це особливо небезпечно для систем технологічного управління енергопостачанням, транспортом та подібними великими системами. Зазвичай ціна помилки у таких системах надзвичайно велика.

Зростання масштабів об'єктів управління викликає зростання складності алгоритмів управління, що, у свою чергу, приводить до надмірного навантаження на персонал, який бере участь в управлінні. Одним із варіантів вирішення зазначених питань, на думку експертів може стати подальше впровадження інтелектуальних систем автоматизованого управління [1]. Тобто перекладання більшої кількості управлінських рішень на обчислювальну техніку.

Наступна проблема полягає у розширенні можливостей скоєння злочинів в інформаційному середовищі. Розширення спектру послуг, що надають користувачам сучасні інформаційно-телекомунікаційні системи, приводить до появи нових уразливостей у системах захисту, на основі яких будуються нові сценарії комп'ютерних атак, а це, у свою чергу, спрощує організацію і здійснення злочинів у державній, виробничій та соціальній сферах із використанням можливостей Інтернет-середовища.

З метою адекватного реагування на підвищення ризиків у більшості країн світу приймається велика кількість відповідних законів і підзаконних актів, пов'язаних з організацією боротьби із протиправними діями у сфері державної безпеки та соціального життя. Однак, вони більшою мірою призначені для регулювання соціальних відносин між суб'єктами інформаційних процесів, що протікають у сучасному Internet-середовищі і не торкаються технічної сторони проблеми.

Нові виклики у сфері інформаційної безпеки випливають із того, що глобалізація суспільного життя, виробництва і бізнесу створює нові напрями діяльності як у легальній, так і кримінальній сферах. Наприклад, наприкінці нульових років хакерство перейшло на комерційну основу, так само як торгівля зброєю або наркотиками. І кіберпростір тільки полегшує діяльність у таких протиправних сферах.

Таким чином, нові проблеми сучасного Інтернет-середовища пов'язані не стільки із уразливістю автоматизованих систем, скільки намаганням використати сучасні інформаційно-телекомунікаційні системи та їх нові можливості для досягнення зловмисних цілей. Все це привело до того, що у міжнародних нормативних документах поряд з поняттями інформаційна безпека та інформаційний простір набули поширення такі терміни як кібербезпека та кіберпростір. Це, у свою чергу, вимагає розуміння суті цих понять і відповідної адаптації національної законодавчої та нормативної бази до сучасних вимог захисту.

Аналіз останніх досліджень і публікацій

Поява перших цивільних автоматизованих інформаційних систем у середині 70-х років минулого сторіччя одразу привела до публічної дискусії про забезпечення недоторканності інформаційних ресурсів, що зберігаються, обробляються і передаються у таких системах. Результатом дискусії став документ під назвою «Критерії оцінки захищених комп'ютерних систем» [2], опублікований у 1985 році міністерством оборони США. В ньому були викладені основні засади створення захищених систем, визначена відповідна термінологія і, головне, надана шкала для оцінки рівня захищеності комп'ютерних систем. Цей документ був розрахований на закриті сис-

теми, що не мають фізичного виходу у зовнішній інформаційний простір.

На початку 90-х років з'явились доступні персональні комп'ютери з уніфікованою операційною системою і це привело до появи відкритого мережного простору. Організація на основі колективної відкритої обчислювальної мережі розподіленого обчислювального процесу, у свою чергу, викликала розширення кола інформаційних послуг, що надаються користувачам. Проблеми захисту таких мереж вирішувались на основі національного законодавства окремих країн. Спочатку у країнах Заходу таких як США, Канада та Європейських країнах з'явились відповідні національні документи, що визначали критерії оцінки захисту інформаційних технологій [3-5]. Наприкінці 1999 року у світ вийшли «Загальні критерії», зараз відомі та прийняті в Україні як ДСТУ ISO/IEC 15408:2017 [6]. Ці, та інші, пов'язані із ними, документи, визначали термінологію та основні засади захисту інформації у відкритому мережному просторі. Їх метою стало регулювання правових відносин між замовниками і розробниками захищених інформаційних технологій. Вони були націлені на вирішення технічних питань захисту. Тобто, крім термінології вони визначали які функції захисту і від яких загроз мають використовуватись, як має бути побудований профіль захисту і як забезпечити необхідний рівень довіри до системи захисту.

Щодо питань організації захисту і управління ним, то вони вперше були викладені у стандарті BS 7799, виданому Британським інститутом стандартів (British Standards Institution – BSI) під назвою «Практичні правила управління інформаційною безпекою» у 1995 році. У 2000 році ISO/IEC JTC 1/SC 27, на базі британського стандарту BS 7799, розробив міжнародний стандарт з менеджменту безпеки ISO/IEC 17799. Згодом, у різні роки виходили міжнародні стандарти серії ISO/IEC 27000, що визначають модель управління безпекою, яка включає функції управління безпекою. По відношенню до них експерти різних країн досягли згоди на основі накопиченого досвіду. Сукупність цих стандартів визначають вимоги до систем управління інформаційною безпекою, управління ризиками, метрики та вимірювання, а також керівництво по втіленню.

Сьогодні інформаційне Інтернет-середовище надає користувачам надзвичайно широкий спектр послуг, починаючи із забезпечення документообігу і до автоматизації управління складними, розподіленими у просторі технічними системами.

Зважаючи на великі якісні зміни, що відбулися у загальному інформаційному просторі і нові проблеми у питаннях захисту, ISO/IEC оприлюднило новий міжнародний стандарт ISO/IEC 27032:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови із кібербезпеки» [7]. Цим стандартом було визначено такі поняття як кіберпростір та кібербезпека і надано їх тлумачення.

Підставами до введення нової термінології стало інтенсивне впровадження сучасних обчислювальних та телекомунікаційних технологій у сферу виробництва та соціального і суспільного життя людей. Мініатюризація обчислювальних пристроїв та збільшення їх обчислювальних можливостей дозволили підняти на якісно новий рівень автоматизацію управління складними виробничими процесами. Тобто це наслідки технічного прогресу у галузі інформаційно-телекомунікаційних систем.

Ще однією причиною суттєвих змін в інформаційному просторі є активне впровадження інтелектуальних технологій управління із використанням систем штучного інтелекту у всі сфери життєдіяльності, особливо для оптимізації функціонування інфраструктури складних систем. До складу таких систем слід віднести технології роботи із «великими даними», експертні системи, системи підтримки прийняття рішень і, так звані, «вбудовані системи» [8]. Під вбудованими розуміються системи управління, які розміщуються безпосередньо у виконавчих пристроях, що приводить до поступового стирання межі між об'єктами і органами управління. Передбачається, що на основі таких вбудованих систем у майбутньому будуть створені «розумні будинки» і навіть «розумні міста» [9].

Сьогодні не існує загальної сталої теорії побудови таких систем. Виробники створюють їх на основі власного досвіду і це не дозволяє визначити загальні підходи до їх захисту. Цей висновок випливає із того, що «Загальні критерії» ДСТУ ISO/IEC 15408:2017 [6] орієнтовані на захист відкритих систем, побудованих на основі стеку протоколів TCP/IP. Саме вразливості цих протоколів є основою переважної більшості мережних атак на інформаційні ресурси. Стандарт ISO 27032:2012 [7], яким було визначено якісні зміни у Internet-просторі, у питаннях конкретних методик управління ризиками посилається на інші відомі стандарти серії ISO 27000, які не враховують цих змін.

Мета та основні завдання досліджень

Враховуючи вище зазначене, метою дослідження є пошук напрямів удосконалення державної нормативно-правової бази, яка могла б стати основою для створення систем захисту, що від-

повідають сучасним вимогам.

Виклад основного матеріалу

Стандарт ISO 27032:2012 [7] визначає кіберпростір як комплексне віртуальне середовище, що виникає у процесі взаємодії людей, програмного забезпечення та Internet-послуг, які підтримуються міжнародними розподіленими фізичними інформаційно-телекомунікаційними технологіями та мережами зв'язку.

Необхідність перегляду основних поглядів на захист інформаційних процесів викликана новими проблемами у Internet-просторі, які нагадують про себе дедалі частіше.

Зловмисники і злочинні організації у різних країнах світу регулярно виконують масовані атаки на державні департаменти, фінансові установи та міністерства. Ефективність реагування на такі атаки сьогодні визнається недостатньою. Саме через це у розвинених країнах Заходу захист від подібних кібернетичних атак було оголошено пріоритетним завданням.

Зважаючи на те, що кіберпростір, не дивлячись на його «віртуальність», має конкретну матеріальну основу, яка складається із апаратної частини мереж зв'язку і обчислювальних пристроїв, добре спланована атака може спровокувати економічний колапс, паралізувати оборонні структури, або значно знизити ефективність управління державними органами.

Проблемним питанням на сьогодні залишається захист від апаратних закладок на етапі виробництва і постачання апаратури. У випадках, коли йдеться про використання апаратних засобів для критично важливих інформаційних систем, таких, наприклад, як управління елементами державної інфраструктури, супроводження її розроблення, виготовлення і впровадження у робочі системи має відбуватись у режимі посиленого контролю їх якості та надійності.

Пошук ефективних шляхів вирішення проблем безпеки в усіх провідних країнах світу відбувається за підтримки та під керуванням вищих державний інституцій. Кіберпростір розглядається як новий театр воєнних дій. Відповідно, постає питання доцільності та залежності від використання у державному секторі програмно-апаратного забезпечення виробників, афільованих із країнами, які можуть вважатись ймовірним супротивником.

Розширенню напрямів злочинної діяльності сприяє відкритість Internet-простору. Саме намагання приєднати до Internet-мережі більшу частину обчислювальних пристроїв, задіяних в організації документообігу або у виконанні технологічних процесів просто робить їх вразливими. Має місце тенденція, коли ймовірні втрати від реалізації загроз дедалі більше будуть перевищувати ефект від інформаційних послуг, що надає використання кіберпростору.

Є цілком очевидним, що у майбутньому проблема розподілення доступу мусить піднятися на якісно новий рівень. Великі комерційні об'єднання створюють для власних потреб закриті корпоративні приватні мережі. Постійно розвиваються технології екранування локального інформаційного середовища та VPN-технології. Але все це робиться на основі того самого стеку протоколів TCP/IP, що дає можливість при певних зусиллях долати сучасні системи захисту на програмно-апаратному рівні.

Можна стверджувати, що вже у недалекому майбутньому, для управління критично важливими автоматизованими системами, доведеться створювати локальні закриті мережі, побудовані із використанням унікальних протоколів із унеможливленням втручання із боку відкритого глобального кіберпростору. Це, насамперед, стосується управління військовим озброєнням, атомними електростанціями та іншими складними системами, де наслідки від незаконного втручання можуть бути критичними.

На основі досліджень, проведених британською компанією NCC Group за 2018 рік, було зроблено висновки про те, що у майбутньому боротьба із кіберзлочинністю буде організована на глобальному рівні, через те, що кількість атак, як із внутрішніх, так і зовнішніх джерел, буде тільки зростати. Одною із причин таких очікувань називається намагання багатьох країн в умовах економічних війн вдаватися до використання злочинних способів здобування необхідних ресурсів [12].

Стає цілком очевидним, що виникнення нових проблем у кібернетичному просторі є цілком закономірним результатом еволюційного розвитку світового інформаційного простору, рушійною силою якого є розвиток інформаційно-телекомунікаційних систем, обчислювальної техніки та інформаційних технологій. Якщо два десятиріччя тому головними проблемами були збереження конфіденційності та цілісності даних, а також забезпечення надійності функціонування інформаційних систем, то сьогодні мова іде про кібернетичну війну і кібернетичну зброю. Цілями злочинців стають повалення правлячих режимів, виведення із ладу елементів життєво важливої інфраструктури або здійснення терористичних актів. Для протидії таким негативним явищам необхідно сформулювати нові задачі захисту. Для цього шляхом відповідних досліджень слід виявити, за рахунок яких нових властивостей Internet-простору здійснюються ті або

інші злочинні дії і знайти відповідні засоби захисту для загроз кожного виду. Усе це має бути визначено на рівні державної нормативно-правової бази.

Міжнародний стандарт ISO/IEC 27032:2012 [7], визначає:

– поняття кіберпростору та кібербезпеки;

– активи кіберпростору;

– зацікавлені сторони;

– загрози;

– рекомендації щодо управління ризиками.

При цьому, пріоритетом кібербезпеки стає координація взаємодії між суб'єктами, які формують кібернетичний простір, і на них покладається відповідальність за усунення ризиків від реалізації кіберзагроз.

Модель кібернетичної безпеки, що визначає такі основні поняття як загрози, уразливості, ризики та зв'язок між ними, повністю відповідає моделі захисту, визначеній у ДСТУ ISO/IEC 15408:2017 [6], але у якості активів розглядаються в основному віртуальні гроші, аватари, хмарні технології, віртуальні розваги або інші віртуальні об'єкти, що складають предмет взаємодії між стейкхолдерами (зацікавленими особами).

Таксономія загроз у кіберпросторі надається за традиційною схемою, класифікація яких виконується за видами активів, зовнішніми або внутрішніми ознаками, цілями, порушниками, джерелами тощо. Фактично, стандарт виділяє в Internet-середовищі віртуальний сектор, що обмежується віртуальними діями над віртуальними об'єктами. Він орієнтований на керівників вищого рівня, на яких покладається відповідальність за вирішення проблем безпеки у кіберпросторі і визначає методологію управління кібербезпекою, виділяючи при цьому три напрями такого управління:

– рекомендації з оцінки і визначення ризиків;

– рекомендації вимог безпеки;

– рекомендації щодо забезпечення кібербезпеки провайдерів.

Рекомендації з оцінки і визначення ризиків викладені у відповідності до вимог ISO/IEC 27032:2012 [7], де основний наголос зроблено на відповідальності стейкхолдерів щодо звітності, інформованості і забезпечення узгодженості дій між споживачами послуг і провайдерами у разі виникнення інцидентів із питань безпеки.

Рекомендації споживачам послуг являють собою сукупність норм поведінки, визначених провайдером. Стандарт також надає керівні вказівки організаціям, що містять комплекс заходів щодо управління інформаційною безпекою. Як і в усіх суміжних стандартах засоби захисту пропонується визначати на основі аналізу ризиків, а у якості базових заходів націлених на вирішення задач захисту запропоновано:

– захист програмних додатків;

– захист серверів;

– захист споживачів;

– захист від атак засобами соціальної інженерії;

– підвищення рівня готовності.

Що стосується інформаційного обміну, то стандарт розділяє суб'єкти інформаційного обміну на тих, що надають або отримують інформацію. Організації, що надають інформацію відіграють первинну роль і визначають її класифікацію, рівні безпеки, форми можливого обміну та інше. Сторона, що отримує інформацію, виконує захищене оброблення інформації. Для реалізації і координації обміну інформацією рекомендується:

– мати політику безпеки;

– розробити методи і процедури обміну;

– визначити перелік суб'єктів обміну;

– розробити відповідні технічні рішення.

В цілому, положення стандарту ISO/IEC 27032:2012 [7] відповідають організаційно-технічним заходам, визначеним стандартами серії 27000 і посилаються на підходи до оцінки безпеки, що викладені у стандарті [10] та «Загальних критеріях» [6].

Цього року в Україні було прийнято і опубліковано у липні місяці підготовлений за участю працівників Спеціальної служби зв'язку та захисту інформації закон «Про основні засади забезпечення кібербезпеки України» [11].

В основу цього закону було закладено положення і вимоги стандартів серії ISO/IEC 27000.

Однак, слід зазначити, що по-перше, не зважаючи на те, що в Україні з 2017 року вже діють стандарти пакету в [6], необхідно створити цілий пакет нормативно-методичних документів, що деталізують їх використання у сучасних умовах України.

По-друге, в Україні на офіційному рівні не діє переважна більшість документів пакету серії 27000. Стандарт 27032:2012 [7] вказує лише основні засади організації кібербезпеки і удосконалює діяльність, спрямовану на управління інформаційним захистом в Internet-просторі. Очевидно, що потребують розробки додаткові стандарти, де буде деталізовано способи вирішення складових задач кібербезпеки.

Висновки

Сучасний стан розвитку глобального інформаційного середовища, побудованого на основі інформаційно-телекомунікаційних систем, не тільки надає широкі можливості користувачам, але й приводить до негативних наслідків. В умо-

вах існування кіберпростору стають реальними деякі види злочинів, від яких людство вважало себе надійно захищеними. Боротьба із ними потребує виконання додаткових досліджень і кардинального перегляду самої концепції оцінки безпеки та правил побудови систем захисту.

Поява стандарту ISO/IEC 27032:2012 [7] фактично вводить основні поняття і визначає основні засади організації захисту у нових умовах. Що ж стосується «Загальних критеріїв» ДСТУ ISO/IEC 15408:2017 [6], що визначають технічну сторону захисту, і які у першій редакції ISO були прийняті майже двадцять років тому, то питання про їх кардинальний перегляд поки що не ставиться.

Намагання створити в Україні стратегію кібернетичної безпеки України у відповідь на нові виклики в інформаційному просторі, повинні розпочинатись із узгодження національної нормативно-правової бази з питань інформаційного захисту із вимогами відповідних міжнародних стандартів.

Список використаних джерел

1. Diagnosis and Fault Tolerant Control / M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki. – Berlin: Springer-Verlag, 2003.
2. Trusted Computer System Evaluation Criteria. US Department of Defense 5200.28-STD, 1993.
3. Federal Criteria for Information Technology Security. National Institute of Standards and Technology & National Security Agency. Version 1,0 December 1992.
4. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. – Department of Trade and Industry, London, 1991.
5. Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.
6. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT).
7. ISO/IEC 27032:2012 Information technology – Security techniques Guidelines for Cybersecurity. – 2012-07.
8. Edward A. Lee. Past, Present and Future of Cyber-Physical Systems: A Focus on Models. 2015 Feb 26. [Електронний ресурс] / Портал : https://www.ncbi.nlm.nih.gov/ – Режим доступу \www/ URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4435108/
9. Rodger Lea. Smart Cities: An Overview of the Technology Trends Driving Smart Cities. March 2017. – 16 С. [Електронний ресурс] / Портал : https://www.ieee.org/ – Режим доступу \www/ URL: https://www.ieee.org/content/dam/ieee-org/ieee-web/pdf/ieee-smart-cities-trend-paper-2017.pdf.
10. ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT (ISO/IEC 18045:2008, IDT).
11. Закон України Про основні засади забезпечення кібербезпеки України : Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 [Електронний ресурс] / Портал : rada.gov.ua. – Режим доступу \www/ URL: http://zakon5.rada.gov.ua/laws/show/287/2015. – Заголовок з екрану, доступ вільний, 8.07.2018.
12. A Cyber Year In Review. Dec, 2018. [Електронний ресурс] / Портал : https://www.nccgroup.trust/ Режим доступу \www/ URL: https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/december/a-cyber-year-in-review/?style=Cyber+Security – Заголовок з екрану, доступ вільний, 1.12.2018.

References

1. Diagnosis and Fault Tolerant Control / M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki. – Berlin: Springer-Verlag, 2003.
2. Trusted Computer System Evaluation Criteria. US Department of Defense 5200.28-STD, 1993.
3. Federal Criteria for Information Technology Security. National Institute of Standards and Technology & National Security Agency. Version 1,0 December 1992.
4. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. – Department of Trade and Industry, London, 1991.
5. Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.
6. DSTU ISO/IEC 15408-1:2017 Informatsiini tekhnolohii. Metody zakhystu. Kryterii otsinky. Chastyna 1. Vstup ta zahalna model [Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model] (ISO/IEC 15408-1:2009, IDT).
7. ISO/IEC 27032:2012 Information technology – Security techniques Guidelines for Cybersecurity. – 2012-07.
8. Edward A. Lee. Past, Present and Future of Cyber-Physical Systems: A Focus on Models. 2015 Feb 26. [Electronic resource] / Portal:

https://www.ncbi.nlm.nih.gov/ – Access mode \www/ URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4435108/

9. Rodger Lea. Smart Cities: An Overview of the Technology Trends Driving Smart Cities. March 2017. – 16 C. [Electronic resource] / Portal : https://www.ieee.org/ – Access mode \www/ URL: https://www.ieee.org/content/dam/ieee-org/ieee-web/pdf/ieee-smart-cities-trend-paper-2017.pdf

10. DSTU ISO/IEC 18045:2015 Informatsiini tekhnolohii. Metody zakhystu. Metodolohiia otsiniuvannia bezpeky IT [Information technology − Security techniques − Methodology for IT security evaluation] (ISO/IEC 18045:2008, IDT).

11. Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Vidomosti Verkhovnoi Rady (VVR) [On the basic principles of ensuring cybersecurity Ukraine], 2017, № 45, ст.403 [Electronic resource] / Portal: rada.gov.ua. – Access mode \www/ URL: http://zakon.rada.gov.ua/laws/show/2163-19, 8.07.2018.

12. A Cyber Year In Review. Dec, 2018. [Electronic resource] / Portal: https:// www.nccgroup.trust/ Access mode \www/ URL: https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/december/a-cyber-year-in-review/?style=Cyber+Security

Надійшла до редакції 10.12.2018