Mozol S. A. International and legal aspect of ensuring criminological safety

The international and legal aspect of ensuring criminological safety has been studied. Pondering on the state criminal policy as a logical continuation of the general policy of criminological safety, the author has concluded that the link between world law and order and security of both a separate state, and civilization in the whole. In this regard, international police cooperation has been considered as a direction of the state policy in the field of crime combating.

It has been proved that criminological safety is one of the obligatory attributes that ensure the normal functioning of a democratic state. The problems of criminological safety in Ukraine are quite acute, which is confirmed by modern criminal and legal statistics.

According to the integrated criterion the author has determined nowadays the urgent directions of international police cooperation in combating: international and internal terrorism; the seizure of hostages; illicit trafficking in narcotic drugs and psychotropic substances; illicit trafficking in chemical and nuclear materials; illicit trafficking in weapons and ammunition; illegal operations in the field of high technologies, first of all cybercrimes; international and national corruption; illegal banking operations (money laundering) and counterfeiting; theft and smuggling of cars; illegal human trafficking across the border; the trafficking of women and children for the purpose of their sexual exploitation; human trafficking for the purpose of transplantation of human organs.

It has been established that the priority of a particular direction of international police cooperation is determined by the international community or individual states, reflected in the international and legal, internal legal base and the relevant organizational structures of specific states, taking into account the public danger, the nature and prevalence of the crimes in question, and other circumstances (political situation, economic status, social development, religious orientation, formed traditions, etc.).

Keywords: safety, criminological safety, crime, international police cooperation, provision of criminological safety.

УДК 343.983.25

Ю. Ю. Нізовцев,
здобувач Національної академії Служби безпеки України (м. Київ)

Окремі питання упорядкування понятійно-термінологічного апарату у сфері кібербезпеки

Досліджено нормативні акти, що мають стосунок до кібербезпеки. Виявлено й проаналізовано неузгодженості та суперечності понятійно-термінологічного апарату кібербезпеки, запропоновано шляхи їх усунення.

Ключові слова: кібербезпека, понятійно-термінологічний апарат, уніфікація нормативних актів.

Постановка проблеми. Будь-яка важлива для функціонування держави сфера життєдіяльності потребує ефективного регулювання та захисту з боку держави. Особливо це стосується безпеки інформаційного

простору (кіберпростору) України, що перебуває під дією негативних чинників, які впливають як на стан кібербезпеки держави в цілому, так і на кібербезпеку та кіберзахист її окремих об'єктів. Зазвичай протидія таким загрозам вимагає злагодженої роботи багатьох державних інститутів, а ефективність цієї роботи, у свою чергу, значною мірою залежить від якості нормативної регламентації.

В Україні нормативно-правову основу функціонування інформаційно-телекомунікаційних систем, технічного захисту оброблюваної в них інформації та кримінальної відповідальності за несанкціоноване втручання в їх роботу становлять Конституція України, закони України та підзаконні нормативні акти. Слід зазначити, що деякі положення зазначених нормативних документів є неузгодженими між собою. Це, зокрема, ускладнює судово-експертне дослідження як шкідливих програмних засобів, так і ознак несанкціонованих втручань у роботу інформаційно-телекомунікаційних систем, учинених за допомогою зазначених програм.

Стан дослідження. Різним аспектам забезпечення кібербезпеки та протидії кіберзлочинності присвятили свої роботи Д. С. Азаров, П. Д. Біленчук, А. С. Білоусов, В. М. Бутузов, В. О. Вітюк, О. П. Войтович, В. Д. Гавловський, Ю. В. Гаврилін, В. О. Голубєв, С. М. Гусаров, В. А. Каплун, М. В. Карчевський, Н. С. Козак, В. В. Крилов, С. А. Кузьмін, А.А. Музика, Л. П. Паламарчук, Д. В. Пашнєв, Н. А. Розенфельд, М. В. Рудик, Л. М. Соловйов, Т. Л. Тропіна, В. С. Цимбалюк, О. М. Черкун, В. П. Шеломенцев та інші вчені. Однак, незважаючи на увагу до цієї теми, суперечності та неузгодженості в окремих положеннях відповідного понятійно-термінологічного апарату залишаються й досі.

Метою статті є виявлення суперечностей та неузгодженостей понятійно-термінологічного апарату кібербезпеки й вироблення на підставі їх аналізу рекомендацій щодо уніфікації окремих положень указаного апарату.

Виклад основного матеріалу. Як уже згадувалося, в Україні існує низка нормативних актів, які визначають основні терміни, що застосовуються у сфері використання інформаційно-телекомунікаційних систем, регулюють відносини у цій сфері, а також установлюють відповідальність за відповідні злочини. Разом із тим автор виявив певні суперечності та неузгодженості понятійно-термінологічного апарату.

По-перше, декілька ключових законодавчих актів, які мають безпосередній стосунок до захисту інформації та протидії кіберзлочинності, містять дещо різні терміни, під якими розуміються технічні засоби обробки та передачі інформації, а саме:

– електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку (ст. 361 КК України [1]);

– інформаційна (автоматизована), телекомунікаційна та інформаційно-телекомунікаційна системи (закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2]);

– технологічна та комунікаційна системи (закон України «Про основні засади забезпечення кібербезпеки України» [3]).

Щоб уникнути неоднозначності під час застосування вказаних термінів, у тому числі під час проведення судових експертиз, слід дослідити, як ці терміни корелюються між собою: які з них мають однакове значення, які поглинають інші тощо.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» дає таке визначення: інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Уже в самому визначенні терміни «автоматизована» та «інформаційна» вживаються як рівнозначні.

Державний стандарт України 2226-93 [4] визначає, що машина обчислювальна цифрова електронна (ЕОМ) – сукупність технічних засобів та системного програмного забезпечення, яка створює можливість проведення оброблення інформації та отримання результату в необхідній формі. Комп'ютер – електронна цифрова обчислювальна машина. По-перше, ДСТУ підтверджує правильність уживання термінів «електронно-обчислювальна машина» (ЕОМ) та «комп'ютер» як рівнозначних. По-друге, виходячи з визначення, ЕОМ та «інформаційна система» також є рівнозначними, оскільки в обох випадках йдеться про сукупність технічних і програмних засобів, призначених для обробки інформації.

Відповідно до закону України «Про основні засади забезпечення кібербезпеки України» система управління технологічними процесами (далі – технологічна система) – це автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включно з промисловим, електронним, комунікаційним обладнанням та іншими технічними та технологічними засобами) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передання даних. Отже, фактично технологічна система є різновидом інформаційної (автоматизованої) системи, спеціалізованої для управління технологічними процесами.

Оскільки закон України «Про телекомунікації» [5] визначив термін «електрозв'язок» як рівнозначний терміну «телекомунікації», мережа електрозв'язку це ні що інше, як телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням. Разом із тим телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання,

випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [2]. Таким чином, і телекомунікаційна мережа, і телекомунікаційна система призначені для передавання інформації. Відмінність полягає у тому, що телекомунікаційна мережа – комплекс технічних засобів, а телекомунікаційна система – сукупність технічних і програмних засобів. Тобто, телекомунікаційна мережа є складовою частиною телекомунікаційної системи.

Інформаційно-телекомунікаційна система – сукупність інформаційних і телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [2]. Слід зазначити, що інформаційно-телекомунікаційними системами є не лише великі розподілені обчислювальні системи, що складаються з великої кількості об'єднаних мережею окремих комп'ютерів. Фактично більшість сучасних комп'ютерів можна віднести до інформаційно-телекомунікаційних систем, оскільки будь-який комп'ютер призначається для оброблення інформації, і більшість із них має у своєму складі мережевий інтерфейс та програмні засоби для взаємодії з мережею, до якої їх під'єднано. Це саме стосується і смартфонів, які, до речі, мають другу, менш розповсюджену назву – кишеньковий персональний комп'ютер (скорочено – КПК).

Відповідно до закону України «Про основні засади забезпечення кібербезпеки України» системи електронних комунікацій (далі – комунікаційні системи) – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включно з пасивними мережевими елементами, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережами мобільного, супутникового зв'язку й електричними кабельними мережами в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), серед іншого засоби та пристрої зв'язку, комп'ютери й інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передавання даних. З одного боку, виходячи з цього визначення, комунікаційні системи є різновидом телекомунікаційних систем, а саме тією їх частиною, що має доступ до мережі Інтернет та/або інших глобальних мереж передавання даних (тобто крім тих, що мають доступ лише до локальних мереж). Разом із тим у визначенні зазначено, що одним із різновидів комунікаційних систем є інформаційно-телекомунікаційні системи. Виникає суперечність: чи то комунікаційні системи є частиною телекомунікаційних і, відповідно, інформаційно-телекомунікаційних систем, чи навпаки, інформаційно-телекомунікаційні системи є частиною (різновидом) комунікаційних систем. На погляд автора, це пов'язано з тим, що на сьогодні спостерігається глибока інтеграція інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Крім того, різні інформаційно-телекомунікаційні системи мають різну спеціалізацію. Зокрема, певні з них створено спеціально для забезпечення роботи саме телекомунікаційних (комунікаційних) систем.

Виходячи з викладеного, автор вважає, що найбільш універсальним є термін «інформаційно-телекомунікаційні системи». Він охоплює всі зазначені вище системи та ін.: інформаційні/автоматизовані та технологічні системи, електронно-обчислювальні машини (комп'ютери) та комп'ютерні мережі, мережі електрозв'язку, телекомунікаційні та комунікаційні системи. Ураховуючи розглянуте вище розмаїття фактично рівнозначних понять, на думку автора, доцільно переглянути та уніфікувати чинне законодавство із застосуванням єдиного терміна «інформаційно-телекомунікаційні системи». Це дозволить уникнути неоднозначностей у тлумаченні тих чи інших понять і спростить розуміння різних нормативних актів, що стосуються однієї спільної або кількох суміжних сфер регулювання. Далі тут буде застосовуватися саме термін «інформаційно-телекомунікаційні системи» у зазначеному вище універсальному значенні.

Ще одне проблемне питання стосується терміна «шкідливий програмний засіб». Як уже зазначалося вище, стаття 361 Кримінального кодексу України передбачає кримінальне покарання за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. На додаток до цього стаття 361-1 Кримінального кодексу України передбачає кримінальне покарання за створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

На думку автора, якщо синтезувати визначення несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку та визначення шкідливих програмних засобів, що містяться, відповідно, у ст. 361 та 361-1 Кримінального кодексу України [1], можна запропонувати таке визначення: шкідливі програмні засоби – це програмні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, яке може призвести до витоку, втрати, підроблення, блокування інформації, спотворення процесу оброблення інформації або до порушення встановленого порядку її маршрутизації [6].

Разом із цим низка інших нормативних документів містить визначення окремих різновидів програмного забезпечення, яке за багатьма

ознаками може вважатися шкідливим, без указівки на співвідношення цих визначень із визначенням загального поняття «шкідливий програмний засіб», поданим у КК України. Зокрема, ДСТУ 3396.2-97 визначає такі поняття, як «комп'ютерний вірус» та «програмна закладка», а НД ТЗІ 1.1-003-99 визначає більш широке коло понять, а саме «комп'ютерний вірус», «програмна закладка», «люк» і «троянський кінь».

ДСТУ 3396.2-97 визначає поняття «комп'ютерний вірус» як програму, що «розмножується та поширюється самочинно», і додає у примітці, що він може порушувати цілісність інформації, програмне забезпечення та/або режим роботи обчислювальної техніки, а програмна закладка – це потай впроваджена програма, яка створює загрозу для інформації, що міститься у комп'ютері.

Відповідно до НД ТЗІ 1.1-003-99 комп'ютерний вірус – програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування комп'ютерної системи та/або зумовити порушення політики безпеки. Програмна закладка – потай впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу комплексу засобів захисту та/або порушення політики безпеки. Люк – залишені розробником недокументовані функції, використання яких дозволяє оминути механізми захисту. Троянський кінь – програма, яка, будучи авторизованим процесом, окрім виконання документованих функцій, здатна здійснювати дії, приховані від особи авторизованого користувача, в інтересах розробника цієї програми.

На думку автора, впорядкування згаданих вище термінів з приведенням до єдиної системи значно полегшить роботу, зокрема, судових експертів, які зможуть використовувати ознаки всіх розглянутих різновидів шкідливих програм під час проведення експертиз потенційно шкідливого програмного забезпечення.

Також існує неузгодженість понять «виток» та «витік». Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» містить поняття «виток інформації» – результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Разом із тим ДСТУ 3396.2-97 визначає поняття «витік інформації» – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання. Семантично випливає, що ці поняття є тотожними. Разом із тим у низці випадків можуть виникнути певні непорозуміння. Отже, на думку автора, було б доцільно узгодити зазначені поняття.

Також, на думку автора, варто дослідити співвідношення значень таких термінів:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України [2]);

– втручання у дані (ст. 4 Конвенції про кіберзлочинність [7]);
– втручання у систему (ст. 5 Конвенції про кіберзлочинність [7]);
– атака (НД ТЗІ 1.1-003-99 [8]);
– кібератака (ст. 1 закону України «Про основні засади забезпечення кібербезпеки України» [3]).

Відповідно до закону України «Про основні засади забезпечення кібербезпеки України» кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включно з інформаційно-комунікаційними технологіями, програмними, програмно-апаратними засобами, іншими технічними та технологічними засобами й обладнанням), спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [3]. На думку автора, це визначення є найбільш точним та ємним.

Далі розглянемо, як це визначення корелює з іншими.

Стаття 361 КК України передбачає кримінальну відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації [1]. Ураховуючи умисну форму вини [9, с. 1038], можна сформулювати таке визначення.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – це умисні дії, спрямовані на досягнення однієї або сукупності таких цілей: витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації (зрозуміло, що кримінальна відповідальність настає лише у випадку успішного досягнення мети).

НД ТЗІ 1.1-003-99 визначає, що конфіденційність інформації – її властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом [8]. Разом із цим витік інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї [2]. Отже, як бачимо, згаданий у ст. 361 КК України витік інформації є рівнозначним

порушенню конфіденційності у законі України «Про основні засади забезпечення кібербезпеки України».

Відповідно до ДСТУ 3396.2-97 порушення цілісності інформації – це спотворення інформації, її руйнування або знищення [10]. Отже, порушення цілісності охоплює втрату та підробку інформації, а також спотворення процесу її обробки. Цей само ДСТУ визначає, що блокування інформації – це унеможливлення санкціонованого доступу до неї; або, інакше кажучи, блокування – це порушення доступності.

Якщо дещо скоротити, комунікаційні системи – це системи передавання, комутації або маршрутизації, обладнання та інші ресурси, що забезпечують електронні комунікації [3]. У разі штатного режиму функціонування ці системи забезпечують належну маршрутизацію інформації. Натомість «порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних … систем» призводить до «порушення встановленого порядку її маршрутизації».

Таким чином, на думку автора, термін «кібератака» є рівнозначним терміну «втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». Відмінність полягає лише у санкціонованості. Санкціонована кібератака (санкціоноване втручання) може мати місце, наприклад, у разі тестування системи технічного захисту інформації.

НД ТЗІ 1.1-003-99 визначає, що атака – це спроба реалізації загрози [8]. ДСТУ 3396.2-97 зазначає такі загрози інформації: витік, можливість блокування чи порушення цілісності інформації [10]. Отже, атака – це дії, метою яких є порушення конфіденційності (витік), доступності (блокування) та цілісності інформації. Таким чином, термін «атака» у визначенні НД ТЗІ 1.1-003-99 цілком поглинається терміном «кібератака» у визначенні закону України «Про основні засади забезпечення кібербезпеки України».

Конвенція про кіберзлочинність [7] визначає таке.

«Стаття 4 – Втручання у дані

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це.

Стаття 5 – Втручання у систему

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це».

Виходячи з цього, можна сформулювати такі визначення.

Втручання у дані – це навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації без права на це.

Втручання у систему – це навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передання, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.

Як бачимо, в обох випадках йдеться про певні маніпуляції з комп'ютерною інформацією, оскільки навіть втручання у систему також здійснюється через вплив на інформацію, а точніше – через порушення двох основних її властивостей, які підлягають захисту [11]: доступності та цілісності.

Таким чином, найбільш ємним і точним терміном є «кібератака». Автор вважає доцільним уніфікувати розглянуті вище терміни в різних нормативних актах, застосувавши найоптимальніший з них – «кібератака», при цьому передбачивши кримінальну відповідальність за «несанкціоновані кібератаки».

Висновки. Можна констатувати, що частина нормативних документів, які стосуються забезпечення кібербезпеки в Україні, мають неузгоджений понятійний апарат. Приведення у відповідність цього апарату (зокрема з урахуванням пропозицій автора) дозволить уникнути неоднозначностей у тлумаченні тих чи інших термінів і спростить розуміння різних нормативних актів, що стосуються однієї спільної або кількох суміжних сфер регулювання.

Список бібліографічних посилань: **1.** Кримінальний кодекс України : закон України від 05.04.2001 № 2341-III // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 08.12.2017). **2.** Про захист інформації в інформаційно-телекомунікаційних системах : закон України від 05.07.1994 № 80/94-ВР // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 08.12.2017). **3.** Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/main/2163-19 (дата звернення: 08.12.2017). **4.** ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Київ, 1994. 92 с. **5.** Про телекомунікації : закон України від 18.11.2003 № 1280-IV // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення: 08.12.2017). **6.** Нізовцев Ю. Ю. Щодо нормативно-правового регулювання сфери протидії несанкціонованим втручанням в роботу інформаційно-телекомунікаційних систем. *Криміналістичний вісник.* 2017. № 1 (27). С. 54–61. **7.** Конвенція про кіберзлочинність : від 23.11.2001 : ратиф. Україною із застереженнями і заявами законом України від 07.09.2005 № 2824-IV // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 08.12.2017).

8. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : затв. наказом Департаменту спец. телекомунікац. систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. Київ, 1999. 30 с. **9.** Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 7-ме вид., перероб. та допов. Київ : Юрид. думка, 2010. 1288 с. **10.** ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Київ, 1998 р. 15 с. **11.** Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення. Київ, 2010. 708 с.

Надійшла до редколегії 12.12.2017

Низовцев Ю. Ю. Отдельные вопросы упорядочения понятийно-терминологического аппарата в области кибербезопасности

Исследованы нормативные акты, имеющие отношение к кибербезопасности. Выявлены и проанализированы несогласованности и противоречия понятийно-терминологического аппарата кибербезопасности, предложены пути их устранения.

Ключевые слова: кибербезопасность, понятийно-терминологический аппарат, унификация нормативных актов.

Nizovtsev Yu. Yu. Certain issues of regulating conceptual nomenclature in the field of cybersecurity

The author of the article researched the laws and by-laws of Ukraine related to cybersecurity. The inconsistencies and contradictions of the conceptual nomenclature of cybersecurity have been revealed. Information and telecommunication systems, cyberattacks, malicious programs and others are among these terms. The author has specially noticed the terms that relate to computer forensics. Having analyzed a number of terms and their definitions, the author came to the conclusion that they are actually equivalent or absorb each other. The presence of several different in sounding, but similar in meaning terms complicates the understanding of the normative act. Accordingly, there may be difficulties in applying it, including in the realizing forensic examinations. The author has suggested the most optimal ways, in his opinion, to eliminate the revealed contradictions and inconsistencies. Unification of the conceptual nomenclature, in the opinion of the author, will avoid confusion in understanding their meaning and will facilitate the application of normative acts.

Keywords: cybersecurity, conceptual nomenclature, unification of normative acts.