

УДК 35:172.4(477)

DOI 10.33244/2617-4154.3.2020.103-113

Т. В. Субіна,

к.ю.н.,

Університет ДФС України

e-mail: subinatv@ukr.net

ORCID ID 0000-0001-7806-7828

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОДИН З ВИДІВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У статті проаналізовано генезис наукових думок про сутність та понятійний апарат «інформаційної безпеки» та надано власне визначення інформаційної безпеки, а саме це – система унормованих методів, заходів, засобів, способів дотримання належного рівня охорони і захисту інформації з метою реалізації конституційних прав, свобод і законних інтересів людини та громадянина, суспільства і держави.

Особлива увага зверталася на аналіз нормативно-правового забезпечення інформаційної безпеки, а саме було розкрито, що інформаційна безпека є однією з видів національної безпеки та важливою самостійною сферою забезпечення національної безпеки.

Ключові слова: інформаційна безпека, національна безпека України, забезпечення інформаційної безпеки, захист інформації, інформаційна безпека як людини і громадянина, суспільства та держави.

Т. В. Субина. Информационная безопасность как один из видов национальной безопасности Украины

В статье проанализированы генезис научных мыслей о сути и понятийном аппарате «информационной безопасности» и предоставлено собственное определение информационной безопасности, а именно это – система нормированных методов, мероприятий, средств, способов соблюдения надлежащего уровня охраны и защиты информации с целью реализации конституционных прав, свобод и законных интересов человека и гражданина, общества и государства.

Особое внимание обращалось на анализ нормативно-правового обеспечения информационной безопасности, а именно было раскрыто, что информационная безопасность является одной из видов национальной безопасности и важной самостоятельной сферой обеспечения национальной безопасности.

Ключевые слова: информационная безопасность, национальная безопасность Украины, обеспечение информационной безопасности, защита информации, информационная безопасность как человека и гражданина, общества и государства.

Мета статті. За умов швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають питання інформаційної безпеки.

Унаслідок відсутності дієвої системи забезпечення інформаційної безпеки у національному інформаційному просторі України спостерігається ряд негативних явищ, які створюють реальні та потенційні загрози інформаційній безпеці людини і громадянина, суспільства та держави.

Постановка проблеми. Інформаційна безпека є невід’ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз, що являє собою сукупність інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки, надання всебічної державної підтримки національним виробникам інформаційного продукту та телекомунікаційного обладнання, створення нормативно-правових, фінансових та інших передумов, необхідних для їх успішної конкуренції на світовому та національному ринках інформаційних і телекомунікаційних послуг [1].

Актуальність цієї теми є безперечною, оскільки основним розвитком інформаційного суспільства є використання інформації інформаційно-телекомунікаційними технологіями в усіх сферах життя людської спільноти та забезпечення захисту інформації.

Аналіз останніх досліджень і публікацій. Основні теоретичні напрями досліджували такі відомі українські вчені, як: І. В. Арістова, О. М. Бандурка, О. О. Бандурка, К. І. Белякова, А. І. Берлач, В. М. Брижко, В. Д. Гавловський, В. О. Глушков, Р. А. Калюжний, Б. А. Кормич, О. В. Логінов, В. М. Росоловський, А. М. Новицький, О. В. Олійник, С. П. Ріппа, Л. В. Трофімова, Д. Я. Семир’янов, І. С. Стаценко-Сургучова, В. С. Цимбалюк, М. Я. Швець та інші.

Виклад основного матеріалу. Основною умовою для створення надійної системи захисту інформації на сьогодні є зміцнення самої української держави та її державних органів, відповідальних за забезпечення інформаційної безпеки. У зв’язку з цим є необхідність з вироблення системи протидії загрозам інформаційної безпеки, пошуку принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління загрозами та небезпеками.

Інформаційну безпеку можна розкрити як стан захищеності потреб особи, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз. Щодо національних інтересів, інформаційна безпека означає такий стан захищеності інформаційних ресурсів особи, суспільства й держави, який забезпечує реалізацію та прогресивний розвиток життєво важливих для них інтересів. Щодо можливих негативних впливів різних видів інформаційної безпеки, це – захищеність інформації та підтримуючої інфраструктури від випадкових чи навмисних природних або штучних впливів, які можуть заподіяти шкоду їхнім власникам або користувачам. Інформаційна безпека також означає рівень захищеності інформаційного середовища суспільства, який забезпечує його формування, використання та розвиток в інтересах громадян, організацій, держави і нейтралізації негативних наслідків інформатизації суспільства.

Інформаційна безпека розглядається у трьох основних аспектах:

1) захист інформації;

2) контроль за національним інформаційним простором;
3) достатнє інформаційне забезпечення державних і недержавних органів, громадських, приватних організацій [2].

Інформаційна безпека виступає як система, що здійснює безпосередній вплив на фінансовий стан і фінансову безпеку держави, динаміку економічного зростання, фінансові пропорції і фінансову рівновагу. У загальному вигляді управління системою забезпечення фінансової безпеки повинне включати два рівні ухвалення рішень: державний і регіональний, а також відповідні механізми забезпечення фінансової безпеки: політичні, правові, адміністративні й економічні. Для кожного з рівнів мають бути визначені відповідні повноваження щодо ухвалення рішень: на державному рівні, наприклад, управління зовнішніми і внутрішніми чинниками, що несуть загрозу, а на регіональному – в основному внутрішніми чинниками.

Також інформаційну безпеку можна розглядати як стан захищеності інформації та інформаційного середовища від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної збитку суб'єктам інформаційних відносин (зокрема, власникам і користувачам інформації). Захистом інформації є комплекс заходів, які спрямовані на забезпечення інформаційної безпеки. Найпоширеніша модель інформаційної безпеки базується на забезпеченні трьох властивостей інформації: конфіденційність, цілісність і доступність. Під конфіденційністю інформації потрібно розуміти те, що з нею може ознайомитися тільки обмежене коло осіб, встановлене її власником. У випадку, коли доступ до інформації отримує неуповноважена особа, відбувається її втрата.

Щодо цілісності інформації, то вона визначається її здатністю зберігатися в неспотвореному вигляді. Неправомірні і не передбачені власником зміни інформації призводять до втрати цілісності. Доступність інформації визначається здатністю системи надавати своєчасний безперешкодний доступ до інформації суб'єкту, що володіє відповідними повноваженнями. Знищення або блокування інформації (в результаті помилки або навмисної дії) призводить до втрати доступності, яка є важливим атрибутом функціонування інформаційних систем, орієнтованих на обслуговування клієнтів. Крім перерахованих трьох властивостей, додатково виділяють ще дві властивості, важливі для інформаційної безпеки: автентичність й апелювання. Автентичністю є можливість достовірно встановити автора повідомлення, а до апелювання належить можливість довести, що автором є саме ця людина і ніхто інший. Найбільш важливі вимоги безпеки, що повинні бути реалізовані в системах, наприклад в електронному документообігу, є:

- аутентифікація та авторизація – перевірка заявленої ідентичності та надання права доступу;
- цілісність – підтримка цілісності даних і виявлення змін;
- конфіденційність – дані не можуть бути передані стороннім особам або системам;
- незаперечність – версифікатор може отримати докази, що підтверджують цілісність та походження даних;
- погодження – отримання, облік, відстеження інформованої згоди пацієнта на доступ до його медичних даних;
- аудит – усі дії повинні бути записані у хронологічному порядку.

Інші вимоги щодо засобів захисту інформації поділяються на дві групи: внутрішні, а саме запобігання загроз, що виходять з внутрішніх джерел, та зовнішні, що

включають запобігання загроз, що виходять ззовні. До систем захисту інформації, що забезпечують безпеку фінансової установи, відносять такі засоби захисту: фізичні, законодавчі, організаційні, програмно-технічні. Фізичні засоби захисту засновані на створенні фізичних перешкод для зловмисника, які перегороджують йому шлях до інформації (сувора система пропуску на територію і в приміщення з апаратурою або з носіями інформації). До законодавчих засобів захисту належать законодавчі акти, які регламентують правила використання й обробки інформації обмеженого доступу і встановлюють кримінальну відповідальність за порушення цих правил. Під організаційним розуміється захист інформації шляхом регулювання доступу до всіх ресурсів системи (технічним засобам, система безпеки телекомунікацій та зв'язку, програмним елементам тощо) [3].

Захист інформації в системі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [4].

На нашу думку, найбільш повним за змістом є визначення О. Голобуцького та О. Шевчука, які пропонують розглядати інформаційну безпеку як сукупність трьох основних складових: конфіденційність, цілісність і доступність. Як уже вище зазначалося, конфіденційність належить до захисту вразливої інформації від несанкціонованого доступу. Цілісність означає захист точності та повноти інформації і програмного забезпечення. Доступність – це забезпечення доступності інформації й основних послуг для користувача в потрібний для нього час [5, с. 139].

Поділяємо думку В. Шамрая, який наголошує, що зростання незахищених інформаційних процесів може призвести до значних технологічних аварій, військових конфліктів і поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів. Проте чим вищий рівень інтелектуалізації та інформатизації суспільства, тим більш важливою стає надійна інформаційна безпека, оскільки реалізація інтересів суспільства здебільшого здійснюється і за допомогою інформатизації. Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися кругозір і мораль як окремих осіб, так і суспільства у цілому, нав'язуватися чужі інтереси, мотиви, спосіб життя. На перший план виступає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки, виробленню механізмів протидії їм у всіх напрямках [6].

Стосовно сутності і поняття інформаційної безпеки О. Баранова розглядає як стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [7].

В. Лизанчук акцентує свою увагу на визначенні А. Задворного, який зазначив, що «завдання інформаційної безпеки» – це створення системи протидії інформаційним загрозам і захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави [8].

В. Петрик дає таке визначення інформаційної безпеки: це – стан захищеності об'єкта (особистого суспільства, держави, інформаційно-технічної інфраструктури), при якому досягається його нормальне функціонування незалежно від наявності внутрішніх і зовнішніх інформаційних впливів [9, с. 160–161].

О. Олійник, О. Соснін, Л. Шаманський визначають інформаційну безпеку України як комплекс системи превентивних заходів з наданням гарантій захисту життєво важливих інтересів особистості, суспільству й державі від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного і незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захисту від маніпулювання інформацією і дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз [10].

В. Гриценко та інші науковці зазначають, що інформаційна безпека розглядається в Україні переважно в організаційно-управлінському та інженерно-технологічному аспектах [11, с. 185].

Л. Задорожня пропонує своє визначення інформаційної безпеки: з одного боку, як захист інформації і особливо як захист інформації з обмеженим доступом (зокрема, персональних даних), з іншого – як захист інформаційних систем, які фактично є засобом передачі інформації [12, с. 20].

Як свідчать дослідження, саме поняття «інформаційна безпека» формувалося упродовж п'ятдесяти останніх років, що відобразалося й у таких назвах:

- у 1960-х роках – «комп'ютерна безпека»;
- у 1970-х роках – «безпека даних» (захист інформації);
- у 1990-х роках проблема сформувалась у багаторівневу структуру та стала також включати конфіденційність, аутентифікацію, цілісність, управління доступом і контроль учасників взаємодії. Окремими дослідниками особлива увага зверталася і на «захист від інформації» [13].

1 травня 2014 року виконуючий обов'язки Президента України, голова Верховної Ради України О. Турчинов підписав Указ № 449/2014 про рішення РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [14].

На нашу думку, значною подією стало прийняття 2018 р. Закону України «Про національну безпеку України», яким визначено основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності. Зокрема, зазначено, що національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [15].

Відповідно до Закону України «Про Основні засади розвитку інформаційного суспільства в Україні 2007–2015 рр.» інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [16, с. 102].

У Законі України «Про телекомунікації» подано таке визначення інформаційної безпеки в телекомунікаційних мережах: це – здатність телекомунікаційних мереж

забезпечувати захист від знищення, перекручування, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації [17].

Відповідно до положень Доктрини інформаційної безпеки України є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Забезпечення інформаційної безпеки України ґрунтується на принципах:

- верховенства права, законності та пріоритету додержання прав і свобод людини і громадянина;
- своєчасності та адекватності заходів захисту національних інтересів України від зовнішніх і внутрішніх загроз в інформаційній сфері;
- невідворотності відповідальності за вчинення злочинів та правопорушень в інформаційній сфері і забезпечення відновлення порушених прав і законних інтересів, відшкодування збитків, шкоди, завданої цими злочинами;
- комплексності і безперервності заходів у сфері забезпечення інформаційної безпеки і захисту інформації;
- пріоритетності запобіжних заходів;
- взаємодії органів державної влади та чіткого розмежування їх повноважень у вирішенні питань забезпечення інформаційної безпеки; партнерства держави та приватного сектору у виробленні нових оптимальних рішень у сфері інформаційної безпеки та участі інституцій громадянського суспільства у забезпеченні інформаційної безпеки держави;
- дієвості, комплексності і постійності заходів із захисту інформації та інформаційних ресурсів в інформаційному просторі;
- пріоритетність національної інформаційної продукції;
- зниження рівня технічної анонімності з одночасним підвищенням захисту персональних даних [18].

Відповідно до змісту Концепції національної програми інформатизації в інтерпретації В. Цимбалюка, інформаційна безпека – це комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для обробки та зберігання інформації обмеженого доступу; комплекс державних стандартів з документування, супроводження використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації та профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо [19, с. 88].

Це підтверджує потребу у створенні національної системи конфіденційного зв'язку, про що також зазначається в Концепції розвитку зв'язку в Україні до 2010 року, затвердженій Постановою Кабінету Міністрів України від 09.12.1999 № 2238 [20].

Інформаційна безпека України – це одна із видів національної безпеки, а її забезпечення – важлива функція держави, яка повинна забезпечити законодавче формування державної інформаційної політики, створення, відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об'єднаннями громадян, іншими суб'єктами права в Україні, гарантування свободи інформаційної діяльності та права доступу до інформації в національному інформаційному просторі України, всебічний розвиток

національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей державно-культурного життя народу України, створення та впровадження безпечних інформаційних технологій, захист прав власності всіх учасників інформаційної діяльності в національному просторі України, збереження права власності держави на стратегічні об'єкти інформаційної інфраструктури України, охорону державної таємниці, забезпечення інформаційної безпеки тощо [21].

Захист суверенітету й територіальної цілісності України, забезпечення її економічної та інформаційної безпеки визначаються у ст. 17 Конституції України як найважливіша функція держави, справа всього Українського народу [22].

Гарантування конституційних прав і свобод людини, громадянина та розвиток громадянського суспільства, його демократичних інститутів є основною метою функціонування системи національної інформаційної безпеки України, що підтримується шляхом проведення зваженої державної інформаційної політики відповідно до прийнятих в установленому порядку законодавства, доктрин, концепцій, стратегій, програм у політичній, економічній, військовій, екологічній, науково-технологічній та інших сферах, а також гарантована завдяки взаємозв'язаній і узгодженій діяльності всіх державних органів, громадян і їх об'єднань.

О. Баранова, розглядаючи проблему національної безпеки із системних позицій, стверджує, що інформаційна безпека посідає особливе місце з таких причин:

– по-перше, інформаційні відносини й процеси пронизують усі інші відносини, що існують у суспільстві, тому інформаційна безпека як один з елементів повинна входити в усі інші складові національної безпеки – зовнішньополітичну, військову, економічну, екологічну та інші;

– по-друге, в сучасних умовах, коли різні інформаційні технології і процеси, засоби обчислювальної техніки інтенсивно та в масовому порядку впроваджуються в багатьох сферах людської діяльності, питання інформаційної безпеки набуває самостійного суспільного значення;

– по-третє, система зовнішніх і внутрішніх загроз інформаційній безпеці має комплексний всеосяжний характер для всіх сфер діяльності людини, суспільства й держави [23, с. 134–135].

Отже, можна зазначити, що інформаційна безпека – це система унормованих методів, заходів, засобів, способів дотримання належного рівня охорони і захисту інформації з метою реалізації конституційних прав, свобод і законних інтересів людини і громадянина, суспільства та держави.

Забезпечення інформаційної безпеки доцільно:

– узгодити вже існуючі нормативно-правові акти у сфері забезпечення інформаційної безпеки шляхом їх систематизації;

– врегулювати положення щодо отримання та надання інформації;

– удосконалити нормативно-правову базу щодо забезпечення охорони, захисту та обігу інформації;

– розробити методичні рекомендації щодо нейтралізації вчинених протиправних дій відповідно до обігу інформації в мережі Інтернет.

Висновки. З вищевикладеного можна зробити висновок, що інформаційна безпека є однією з видів національної безпеки. Водночас інформаційна безпека є важливою

самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки як людини і громадянина, суспільства та держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Доктрину інформаційної безпеки України Законодавство України: база даних / Верхов. Рада України. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025
2. Інформаційна безпека. URL: <http://ukr.vipreshebnik.ru/entsiklopediya/55-i/1943-informatsijna-bezpeka.html>
3. Інформаційна безпека фінансових установ. 2017. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/9896/Bernath-Lukavezka%20%20%20%20%202_2017-196.pdf?sequence=1
4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.
5. Голобуцький О. П. Електронний уряд. К., 2002. 173 с.
6. Шамрай В. О. Інформаційна безпека як складова національної безпеки України. URL: <http://www.crimeresearch.ru/library/Sh-amray.htm>
7. Інформаційна безпека України. Сутність та проблеми: матеріали круглого столу. URL: http://www.niurr.gov.ua/ukr/publishing/panorama3_4/kr_stil_a.htm
8. Лизанчук В. Свобода слова в контексті українського державотворення. URL: http://www.franko.lviv.ua/faculty/jur/Internet/PART-1_7.htm
9. Петрик В. Щодо визначення інформаційної безпеки та її різновидів. Форми та методи забезпечення інформаційної безпеки держави: збірник матеріалів Міжнародної науково-практичної конференції. К., 2008. С. 160–161.
10. Олійник О. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. URL: http://www.niss.gov.ua/book/Sosnin_2.htm
11. Гриценко В. Поступ України до інформаційного суспільства (організаційно-правовий аспект). *Науковий вісник Національної академії державної податкової служби України*. 2001. № 3 (13). С. 185.
12. Задорожня Л. До питання огляду законодавства в інформаційній сфері. 2004. № 3. С. 20.
13. Кашкін Д. Нормативно-правове забезпечення інформаційної безпеки України. URL: http://nc.ufeі.ukrsat.com/Kyrsi%202004/tezi/images_tezi/054_.htm
14. Заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ про рішення РНБО від 28 квітня 2014 року № 449/2014. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-14Про>
15. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2003. № 55. Ст. 241.
16. Про Основні засади розвитку інформаційного суспільства в Україні 2007–2015: Закон України від 09.01.2007 № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

17. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.
18. Про Доктрину інформаційної безпеки України. Законодавство України. *Відомості Верховної Ради України*. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025
19. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). *Підприємництво, господарство право*. 2004. № 3. С. 88.
20. Концепція розвитку зв'язку в Україні до 2010 року: Постанова Кабінету Міністрів України від 09.12.1999 № 2238. URL: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>
21. Шамрай В. О. Інформаційна безпека як складова національної безпеки України. URL: <http://www.crimeresearch.ru/library/Sh-amray.htm>
22. Конституція України від 1996 р. № 30. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
23. Баранов О. А. Інформаційне право України: Стан, проблеми, перспективи. 2005. 316 с.

REFERENCES

1. Pro Doktrynu informatsiinoi bezpeky Ukrainy Zakonodavstvo Ukrainy: baza danykh / Verkhov. Rada Ukrainy. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025
2. Informatsiina bezpeka. URL: <http://ukr.vipreshebnik.ru/entsiklopediya/55-i/1943-informatsijna-bezpeka.html>
3. Informatsiina bezpeka finansovykh ustanov. 2017. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/9896/Bernath-Lukavezka%20%20%20%20%202_2017-196.pdf?sequence=1
4. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh : Zakon Ukrainy vid 05.07.1994 № 80/94. *Vidomosti Verkhovnoi Rady*. 1994. № 31. St. 286.
5. Holobutskyi O. P. Elektronnyi uriad. K. 2002. 173 s.
6. Shamrai V. O. Informatsiina bezpeka yak skladova natsionalnoi bezpeky Ukrainy. URL: http://www.crime_research.ru/library/Sh-amray.htm
7. Informatsiina bezpeka Ukrainy. Sutnist ta problemy: materialy kruhloho stolu. URL: http://www.niurr.gov.ua/ukr/publishing/panorama3_4/kr_stil_a.htm
8. Lyzanchuk V. Svoboda slova v konteksti ukrainskoho derzhavotvorennia. URL: http://www.franko.lviv.ua/faculty/jur/Internet/PART-1_7.htm
9. Petryk V. Shchodo vyznachennia informatsiinoi bezpeky ta yii riznovydiv. Formy ta metody zabezpechennia informatsiinoi bezpeky derzhavy: zbirnyk materialiv mizhnarodnoi naukovo-praktychnoi konferentsii. K., 2008. S. 160–161.
10. Oliinyk O. Polityko-pravovi aspekty formuvannia informatsiinoho suspilstva suverennoi i nezaleznoi derzhavy. URL: http://www.niss.gov.ua/book/Sosnin_2.htm
11. Hrytsenko V. Postup Ukrainy do informatsiinoho suspilstva (orhanizatsiino-pravovy aspekt). *Naukovyi visnyk Natsionalnoi akademii derzhavnoi podatkovoi sluzhby Ukrainy*. 2001. № 3 (13). S. 185.

12. Zadorozhnia L. Do pytannia ohliadu zakonodavstva v informatsiinii sferi. 2004. № 3. S. 20.
13. Kashkin D. Normatyvno-pravove zabezpechennia informatsiinoi bezpeky Ukrainy. URL: http://nc.ufeі.ukrsat.com/Kyrsi%202004/tezi/images_tezi/054_.htm
14. Zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy: Ukaz pro rishennia RNBO vid 28 kvitnia 2014 roku № 449/2014. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-14Pro>
15. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018 № 2469-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2003. № 55. St. 241.
16. Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini 2007–2015: Zakon Ukrainy vid 09.01.2007 № 537-V. Vidomosti Verkhovnoi Rady Ukrainy. 2007. № 12. St. 102.
17. Pro telekomunikatsii: Zakon Ukrainy vid 18.11.2003 № 1280-IV. Vidomosti Verkhovnoi Rady Ukrainy. 2004. № 12. St. 155.
18. Pro Doktrynu informatsiinoi bezpeky Ukrainy. Zakonodavstvo Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025
19. Tsybaliuk V. Informatsiina bezpeka pidpriemnytskoi diialnosti: vyznachennia sutnosti ta zmistu poniattia za umov vkhodzhennia Ukrainy do informatsiinoho suspilstva (hlobalnoi kibertsyvilizatsii). *Pidpriemnytstvo, hospodarstvo pravo*. 2004. № 3. S. 88.
20. Kontseptsiia rozvytku zviazku v Ukraini do 2010 roku: Postanova Kabinetu Ministriv Ukrainy vid 09.12.1999 № 2238. URL: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>
21. Shamrai V. O. Informatsiina bezpeka yak skladova natsionalnoi bezpeky Ukrainy. URL: http://www.crime_research.ru/library/Sh-amray.htm
22. Konstytutsiia Ukrainy vid 1996 r. № 30. Vidomosti Verkhovnoi Rady Ukrainy. 1996. № 30. St. 141.
23. Baranov O. A. Informatsiine pravo Ukrainy: Ctan, problemy, perspektyvy. 2005. 316 s.

T. Subina. Informational security as a kind of Ukrainian national security

This topic is undoubtedly actual because the main development of informational society is using the information by information and telecommunication technologies in all the spheres of human life and proving it's security.

Today the providing of informational security means strengthening of Ukrainian state itself and it's government agencies which are responsible for informational security providing. Thereby there is a necessity of making a system to resist informational security threats, searching principally new non-standard forms of organization, interaction, activity coordination and improving all the means which are aimed at the providing the process of threats and hazards management.

This article analyses the genesis of scientific opinions about the essence and concept of "informational security" and also there is a personal definition of informational security. That is a system of standardized methods, measures, means and ways to adhere the appropriate level of informational protection. All this is necessary to execute the constitutional rights, freedoms and legitimate interests of people and citizens, the society and the state.

A special attention was payed to the analysis of regulatory support of informational security. It was revealed that informational security is a kind of the national security and also it is an important independent sphere of the national security providence. So, development of Ukraine

as an independent, democratic, legal and economically stable state, is possible just on condition that an appropriate level of informational security for people, citizens, the society and the state will be provided.

The article reveals the principles and gives propositions for informational security of Ukraine. And exactly:

- to agree the regulations about the informational security providing by their systematization;*
- to settle provisions about the getting and giving the information;*
- to improve the regulatory framework as to the providing of security, defense and circulation of the information;*
- to develop guidelines about the neutralization of the committed illegal actions according to the circulation of information in the Internet.*

Key words: *informational security, national security of Ukraine, providing of the international security, defense of information, informational security of people, citizens, the society and the state.*

Стаття надійшла до редколегії 1 вересня 2020 року