Аннотация. В статье рассмотрены актуальные проблемы влияния террористического акта на психику человека и выделены рациональные пути предупреждения и преодоления его негативных тенденций. Обоснованы особенности протекания посттравматических расстройств у людей, которые находились в условиях воздействия террористической угрозы; разработки инновационной системы создания и распространения информационного контента, направленного на формирование у людей осведомленности о конструктивном поведении в условиях террористического акта и проведения мероприятий по минимизации его последствий.

Ключевые слова: террористический акт, психика, посттравматические стрессовые расстройства, психическое здоровье, психологическая готовность, стресс, стрессоустойчивость.

Abstract. The article contains analysis of the urgent issues concerning terrorist act impact on human psychics and singles out rational ways to prevent and overcome its harmful tendencies. Peculiarities of the post-traumatic mental disorders of people who came under the impact of the terrorist threat are motivated; innovative system of creating and spreading the information content intended to form people's awareness of the constructive behavior under terrorist act circumstances and measures to minimize its consequences have been worked out.

Key words: terrorist act, psychics, post-traumatic stress disorder, mental health, psychological readiness, stress, stress resistance.

УДК 351.746.1

МІТЕНКО Ольга Василівна

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми. На нинішньому етапі світової історії все більше зростає роль інформаційної сфери життя суспільства, під якою варто розуміти сукупність інформації, інформаційної інфраструктури, суб'єктів інформаційних правовідносин та системи їх регулювання у зазначеній сфері. У свою чергу, інформаційна сфера здійснює вагомий вплив на стан політичної, економічної, оборонної та інших складових національної безпеки України. Для українського суспільства питання забезпечення національної безпеки стоять особливо гостро, що пояснюється бойовими діями на Сході держави та агресією з боку Російської Федерації, веденням останньою інформаційної війни проти України, а відтак питання забезпечення національної безпеки залежить від забезпечення інформаційної безпеки як її складової.

Аналіз останніх досліджень і публікацій. Окремі питання, пов'язані з дослідженням інформаційної безпеки, знайшли відображення в працях вітчизняних вчених: наприклад, М. Дмитренко висвітлив проблеми інформаційної безпеки України в умовах глобальної інформатизації, М. Гуцалюк займався вивченням загальних концепцій захисту інформації, А. Гуз більш детально розглядав питання історії захисту інформації, А. Ліпінська досліджувала інформаційні ресурси в їх загальному розумінні та ступінь їх захищеності на сьогодні.

На нашу думку, питання інформаційної безпеки як складової національної безпеки України досліджено недостатньо і потребує подальшого вивчення. Адже нині інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни. Це, в першу чергу, зумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизації і, як наслідок, – істотним зростанням впливу інформаційної сфери на життя нашого суспільства. Отже, **метою статті** є розгляд інформаційної безпеки як складової національної безпеки України.

Виклад основного матеріалу. Згідно із Законом України «Про національну безпеку України» від 21 червня 2018 року ***національна безпека*** – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. ***Загрози національній безпеці*** – явища, тенденції та чинники, що унеможливлюють чи ускладнюють або можуть унеможливлювати чи ускладнювати реалізацію національних інтересів та збереження національних цінностей України [13]. На сучасному етапі основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері є:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційну інформацію, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації, в тому числі й стосовно подій на Сході України [4].

Згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» суб'єктами відносин, пов'язаних із захистом інформації в системах, є власники інформації; власники систем; користувачі; уповноважений орган у сфері захисту інформації [11]. Об'єктом є правовідносини між суб'єктами (суспільні відносини), які визначаються за певними об'єктивно існуючими критеріями. В науковій та

спеціальній літературі до об'єктів інформаційної безпеки відносять інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізм забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни. Відтак соціальними об'єктами інформаційної безпеки є: особа (її права та свободи в інформаційній сфері), суспільство (його духовні цінності, засади солідарної діяльності), держава (її конституційний лад, суверенітет). Технічними об'єктами інформаційної безпеки є інформаційні ресурси, інформаційна інфраструктура, інформаційні технології. Система забезпечення інформаційної безпеки України – це організована державою сукупність суб'єктів (державних органів, посадових осіб, громадських організацій, окремих громадян), об'єднаних цілями та завданнями захисту національних інтересів України в інформаційній сфері, які здійснюють узгоджену діяльність у межах законодавства України. Суб'єкти забезпечення інформаційної безпеки – це Верховна Рада України, Конституційний Суд, суди загальної юрисдикції, Кабінет Міністрів України та місцеві державні адміністрації, Державний комітет зв'язку та інформатизації України, Прокуратура України, Міністерство внутрішніх справ України, Служба безпеки України.

Указом Президента України «Про заходи щодо забезпечення інформаційної безпеки держави» від 18 вересня 2002 року № 836/2002 з метою підвищення рівня захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, забезпечення інформаційної безпеки держави утворено Державний центр інформаційних та телекомунікаційних систем у складі Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, який здійснює методичне керівництво та координує діяльність державних органів, пов'язану із запобіганням, виявленням, реагуванням та усуненням наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, надає, у разі потреби, допомогу цим органам у здійсненні заходів із попередження порушення цілісності, доступності та конфіденційності зазначених ресурсів [1].

Органи виконавчої влади з метою захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах визначають перелік інформаційних та телекомунікаційних систем, які містять державні інформаційні ресурси та погоджують його з Департаментом; здійснюють, згідно з вимогами нормативно-правових актів з питань захисту інформації, під методичним керівництвом Департаменту заходи щодо захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, у тому числі підключених до глобальних мереж передавання даних; збирають, узагальнюють та аналізують інформацію про вчинення несанкціонованих дій і здійснюють заходи щодо усунення їх наслідків; невідкладно (протягом доби) інформують Департамент про спробу вчинення чи власне вчинення несанкціонованих дій; надають на запит Департаменту

інформацію про технічні та програмні засоби, що використовуються для надання мережних послуг, а також про зміни у способах або видах підключення до глобальних мереж передавання даних; здійснюють разом з Департаментом оцінку рівня захищеності державних інформаційних ресурсів на всіх етапах життєвого циклу інформаційних та телекомунікаційних систем під час створення або удосконалення комплексних систем захисту інформації відповідно до вимог нормативно-правових актів із питань захисту інформації; оновлюють за рекомендацією Департаменту антивірусні програмні засоби, використовуючи при цьому лише ті з них, які пройшли експертизу в Департаменті. Координаційним органом з питань національної безпеки, у тому числі й інформаційної, є Рада національної безпеки і оборони України, яка координує і контролює діяльність органів виконавчої влади у сфері національної безпеки й оборони.

Відповідно до інтересів забезпечення національної безпеки і ступеня цінності для держави, а також правових, економічних та інших інтересів користувачів, за режимом доступу інформація поділяється на ***відкриту інформацію***, тобто загальнодоступну, яку можна знайти у вільному доступі, та ***інформацію з обмеженим доступом***, яка містить відомості, що становлять той чи інший вид таємниці і підлягають захисту як з боку держави, так і відповідних користувачів. Порядок обігу інформації з обмеженим доступом регулює ст. 30 Закону України «Про інформацію» [10].

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну. ***Конфіденційною*** є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку, відповідно до передбачених нею умов, а також в інших випадках визначених законом. До ***таємної інформації*** належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Віднесення інформації до такої, що становить державну таємницю, і доступ до неї громадян здійснюється відповідно до Закону України «Про державну таємницю» від 21 січня 1994 року [12]. Стаття 8 зазначеного закону визначає інформацію, що може бути віднесена до державної таємниці. У цій самій статті відзначено, що забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

В контексті розгляду поняття «інформаційної безпеки», беручи до уваги події на Сході нашої держави, варто зосередити увагу на явищі ***«інформаційної війни»***, формах та методах її ведення. «Інформаційна війна» – специфічний вид протиборства, не пов'язаний із традиційними військовими діями, який проводиться в особливій

сфері – інформаційній. Серед нових найбільш важливих засобів «інформаційної війни» сьогодні називають різні математичні, програмні засоби типу «вірусів» і «закладок», засоби дистанційного витирання інформації, що записана на магнітних носіях, генераторами електромагнітних імпульсів, засоби неконтрольованого включення у закриті інформаційні мережі та ін. У більш вузькому розумінні словосполучення «інформаційна війна» стає одним із різновидів бойових дій – інформаційних, або важливою фазою безпосередньої підготовки до них. Найважливішими складовими концепції «Інформаційна війна» є: введення супротивника в оману, психологічні операції, електронна війна і вогневе знищення, які проводяться в комплексі з глибокою і всебічною розвідкою як для дезорганізації системи управління противника, так і для захисту власної системи управління в ході бойових дій. При цьому інформація, що циркулює в системі управління, розглядається як високопріоритетний об'єкт впливу і захисту, зниження або підвищення достовірності. Якісно новий рівень сучасних інформаційних технологій дозволяє ефективно проводити інформаційні операції, які є складовими інформаційних війн, у глобальних масштабах з метою формування в потрібному руслі та контролю над масовою свідомістю населення. За допомогою інформаційної зброї вирішуються типові завдання: маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни супротивника з метою створення політичної напруженості та хаосу; дестабілізація політичних відносин між партіями, об'єднаннями і рухами з метою провокації конфліктів, розпалювання недовіри, підозрілості, загострення політичної боротьби, провокації репресій проти опозиції, провокації взаємознищення; зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень; дезінформація населення про роботу державних органів, підрив їх авторитету, дискредитація органів управління; провокація соціальних, політичних, національних і релігійних заворушень; ініціація страйків, масового безладдя й інших акцій економічного протесту; підрив міжнародного авторитету держави, його співробітництва з іншими країнами; завдання збитків життєво важливим інтересам держави в політичній, економічній, оборонній і в інших сферах [4].

Варто зауважити, що ведення інформаційної війни за своєю суттю нічим не відрізняється від ведення відкритих бойових дій. Однак інформаційна війна дозволяє противнику досягти своєї цілі, не використовуючи бойову зброю та, до прикладу, захопити частину території з діючою інфраструктурою. Згадаємо лише політику Гітлера у Судетській області у Чехословаччині. Знайшовши «благородну» офіційну причину – жахливі умови життя етнічних німців, утиски з боку уряду, – провівши активну пропаганду серед місцевого населення, гітлерівський уряд фактично захопив частину Чехословаччини, до того ж зробив це не докладаючи особливих зусиль. Такий механізм повторила Російська Федерація в АР Крим,

що призвело до анексії української території шляхом прихованого військового втручання та подальшого проведення сумнівного референдуму.

Важливим заходом у сучасних умовах є забезпечення інформаційно-психологічної безпеки України. Основними заходами щодо реалізації державної політики в цьому напрямі мають стати:

1) оцінка стану інформаційно-психологічної безпеки в країні;

2) виявлення джерел внутрішніх і зовнішніх загроз інформаційно-психологічної безпеки громадян, визначення пріоритетних напрямів відвертання, парирування і нейтралізації цих загроз;

3) удосконалення нормативно-правової бази забезпечення інформаційно-психологічної безпеки громадян України;

4) координація діяльності органів державної влади й інших органів, на яких покладено завдання забезпечення інформаційно-психологічної безпеки громадян України;

5) контроль діяльності органів державної влади і органів місцевого самоврядування, що беруть участь у вирішенні завдань забезпечення інформаційно-психологічної безпеки громадян України;

6) організація розробки державних і регіональних програм забезпечення інформаційно-психологічної безпеки громадян і координація робіт щодо їх реалізації;

7) здійснення міжнародної співпраці у сфері забезпечення інформаційно-психологічної безпеки громадян, представлення інтересів України у відповідних міжнародних організаціях.

Недосконалість чинного інформаційного законодавства та фінансову слабкість більшості українських ЗМІ використовують розвідувальні органи іноземних держав, закордонні неурядові організації, фінансово-політичні клани, радикально налаштовані політичні сили для проникнення в інформаційний простір держави. Зокрема, використовуючи можливості українського медіа-простору, іноземні держави здійснюють інформаційну політику у вигідному для них руслі (проведення широкомасштабних PR-акцій, стажування українських журналістів, поширення друкованої продукції тощо). Фіксуються непоодинокі спроби використати окремих радикально налаштованих осіб з метою дестабілізації суспільно-політичної обстановки, розпалювання сепаратистських настроїв, національної та релігійної ворожнечі. Відсутність механізмів державного контролю за розповсюдженням інформації через інтернет-сайти спричиняє стрімке збільшення обсягу повідомлень суспільно-політичного змісту (анонімних, достовірність яких викликає сумніви, провокативного і відверто протиправного характеру), які дублюються традиційними вітчизняними ЗМІ з посиланням на Інтернет.

До основних загроз інформаційній безпеці держави слід віднести посилення технологічної залежності від іноземних країн в інформаційній сфері України та витіснення з національного ринку засобів інформатизації і телекомунікації вітчизняного виробництва. Використовуючи впливові політичні та бізнесові зв'язки, представники закордонних компаній

впроваджують у державні установи телекомунікаційні і комп'ютерні обладнання іноземного виробництва з недокументованими функціями, чим створюють умови для віддаленого несанкціонованого доступу до інформації, що циркулює в інформаційно-телекомунікаційних системах та комп'ютерних мережах органів державної влади й місцевого самоврядування. В основному цей процес відбувається за рахунок кредитів міжнародних фінансових організацій та в рамках міжнародної технічної допомоги, що супроводжується усуненням від участі у тендерах на постачання комп'ютерного й телекомунікаційного обладнання конкурентоспроможних вітчизняних компаній. Таким чином, створюються реальні передумови для технічного проникнення до державних інформаційних ресурсів.

Новою тенденцією, яка створює передумови до реалізації загроз інформаційній безпеці держави, є активізація діяльності іноземних суб'єктів господарювання щодо запровадження програмного забезпечення для систем електронного документообігу за наявності достатньої кількості вітчизняних підприємств-розробників та постачальників аналогічної продукції. Окремі властивості зазначених програмних продуктів свідчать про можливу наявність недокументованих функцій. Аналіз процесів, що відбуваються в інформаційній сфері, свідчить про існування передумов до порушення сталого функціонування системи управління державою та збройними силами в особливий період. Стабільно високий інтерес закордонних бізнесових кіл щодо придбання контрольних пакетів акцій провідних вітчизняних компаній у сфері мобільного зв'язку, інформаційно-телекомунікаційних послуг та національних мереж передачі даних. Унаслідок цього може виникнути ситуація, при якій іноземні держави зможуть використовувати свій мережевий простір на шкоду інтересам України.

Глобалізація відкритих комп'ютерних і телекомунікаційних мереж, швидке зростання світового ринку інформаційних технологій, продуктів і послуг, формування міжнародного інформаційного простору створюють передумови для порушення традиційних механізмів забезпечення геополітичної цілісності держав, здійснюють серйозний вплив на суспільство. Саме тому зростає значення міжнародно-правових механізмів регулювання інформаційної сфери. Нові тенденції необхідно враховувати під час визначення напрямів реалізації державної політики в частині розвитку інформаційного законодавства та його окремих напрямків.

Також Україні варто ініціювати міжнародні переговори з проблем забезпечення безпеки в інформаційній сфері. Зокрема, повинні бути досягнуті угоди з максимальною кількістю країн з питань координації діяльності у сфері боротьби з інформаційним тероризмом й інформаційним криміналом. Предметом переговорів повинен також стати правовий захист національних інформаційних ресурсів та інтелектуальної власності, а також авторських прав на матеріали, поширювані світовими відкритими мережами, в першу чергу, через Інтернет. Повинні бути вироблені узгоджені національні

та міжнародні правові норми, що встановлюють відповідальність за хакерство та інші комп'ютерні злочини, зловмисне проникнення в державні та корпоративні інформаційні мережі, порушення прав і законних інтересів громадян у процесі інформаційного обміну. Необхідно розглянути можливості контролю за поширенням у мережі Інтернет непристойної інформації і такої, що завдає шкоди суспільній моралі, містить недобросовісну рекламу, пропагує розпалювання війни, шахрайські операції тощо, які чинять негативний вплив на масову свідомість, фізичне, психічне і соціальне здоров'я людей.

Державна інформаційна політика сьогодні спрямована на забезпечення належних правових, економічних, внутрішньо- і зовнішньополітичних, організаційних та інших умов. Усі ці умови необхідні для: створення розвиненої та захищеної інформаційної інфраструктури України; розвитку міжнародного співробітництва в інформаційній сфері та утвердження України як країни з інформаційним суспільством; забезпечення безпеки інформаційної діяльності, життєво важливих інтересів особи, суспільства та держави в інформаційній сфері. Суттєвим для інформаційної політики будь-якої держави є дотримання балансу інтересів особистості, суспільства і держави. Держава повинна забезпечувати відкритість та поінформованість суспільства про діяльність її органів і суспільних інститутів в інформаційній сфері [2].

У нинішніх умовах для забезпечення безпеки національних інтересів в інформаційній сфері особливо важливою стає активізація діяльності суб'єктів стосовно інформаційної безпеки. Насамперед це стосується діяльності з питань захисту конституційних прав і свобод громадян, розвитку регіональних інформаційно-телекомунікаційних систем та забезпечення їх безпечного функціонування, формування регіональних відкритих інформаційних ресурсів та їх ефективного використання. Проблема забезпечення інформаційної безпеки України багато в чому зумовлена прогалинами в правовому регулюванні взаємодії органів виконавчої влади при вирішенні завдань забезпечення інформаційної безпеки. Для вирішення цієї проблеми вважається доцільним здійснити наступні заходи: створити ефективну багаторівневу державну систему забезпечення інформаційної безпеки, у якій будуть діяти єдині правові норми і механізми захисту інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури й інформаційних прав громадян, здійснюватиметься ефективна координація діяльності органів державної влади й управління; розробити механізм узгодження діяльності органів державної і місцевої влади в забезпеченні інформаційної безпеки; активізувати діяльність із формування державної політики в забезпеченні інформаційної безпеки регіонів, створенні необхідних для реалізації цієї політики організаційних структур і нормативної правової бази; зміцнювати взаємодію регіональних структур із державними органами виконавчої влади при вирішенні питань забезпечення інформаційної безпеки. Ще одна проблема,

що пов'язана з функціонуванням державної системи інформаційної безпеки України, – це забезпечення прозорості діяльності державних органів, що беруть участь у формуванні відкритих державних інформаційних ресурсів і здійсненні доступу до них громадян. Зараз відсутність такої інформації стає перешкодою для залучення внутрішніх і закордонних інвестицій, оскільки комерційні структури готові вкладати свої гроші в розвиток відкритих державних інформаційних ресурсів за умови, що ці гроші будуть використані за призначенням.

Висновки. Сучасний глобальний інформаційний простір не має меж і володіє надшвидкісними можливостями. Водночас він також потерпає від стрімко зростаючої кількості незаконних втручань, які спрямовуються проти безпеки особистості, держави в цілому, міжнародної стабільності. Активізація інформаційного обміну між країнами формує ставлення до захисту комунікаційних систем, як до невід'ємної складової національної безпеки кожного учасника такого процесу, спонукає об'єднувати зусилля для вироблення єдиних, узгоджених підходів до забезпечення конфіденційності інформаційних ресурсів, що є власністю держави. Ефективність системи державного управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає в умовах науково-технічного прогресу та переходу до постіндустріального суспільства загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні системи державного управління цими процесами призводять до непоправних збитків суспільству й державі. Все це визначає проблему формування організаційно-правових засад системи управління і захисту інформаційних ресурсів, як найактуальнішу і невідкладну. Стратегічно важливою залишається проблема координації правотворчого процесу щодо формування правових засад побудови, забезпечення функціонування і розвитку системи управління інформаційними ресурсами України, а також розвитку інформаційної інфраструктури країни. Щодо перспектив подальших розвідок. Останні події в нашій державі показали, наскільки влада є неготовою протистояти інформаційним війнам, оскільки питання інформаційної політики не розглядаються на достатньому рівні. Необхідно звернути увагу на здобутки в цій сфері зарубіжних країн і налагодити законодавчий процес в системі захисту стратегічних інформаційних ресурсів.

Список використаних джерел

1. Дмитренко М. Проблеми інформаційної безпеки України [Електронний ресурс] / М. Дмитренко. – Режим доступу : http://socialscience.com.ua/article/807 (дата звернення: 23.11.2018).

2. Логінов О. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління / О. Логінов // Науковий вісник Юридичної академії МВС України. – Київ, 2003. – Вип. 3. – 224 с.

3. Кормич Б. Інформаційна безпека: організаційно-правові основи : навчальний посібник / Б. Кормич. – Київ : Кондор, 2004. – 384 с.

4. Галамба М. Інформаційна безпека України: поняття, сутність та загрози [Електронний ресурс]. – Режим доступу : http://www.justinian.com.ua/article.php?id=2463 (дата звернення: 12.12.2018).

5. Актуальні проблеми інформаційної безпеки України : аналітична доповідь УЦЕПД // Національна безпека і оборона. – Київ, 2001. – № 1. – 224 с.

6. Виноградова Г. Інформаційне право : навчальний посібник / Г. Виноградова. – Київ : МАУП, 2011. – 144 с.

7. Василенко Д. Законодавство провідних країн світу в сфері захисту інформації [Електронний ресурс]. – Режим доступу : http://www.kdu.edu.ua/statti/2010-2-1(61)/128.PDF (дата звернення: 01.10.2018).

8. Парахонський Б. Стратегічні інтереси України в країнах Чорноморського регіону та проблеми національної безпеки / Б. Парахонський. – Київ : НІСД, 2001. – Вип. 7. – 134 с.

9. Черненко Т. Пріоритети державної інформаційної політики в умовах гібридної війни / Т. Черненко // Стратегічні пріоритети. – Миколаїв, 2015. – Вип. 4 (37). – С. 83–92.

10. Про інформацію : Закон України від 2 жовтня 1992 року № 2675-XII // Відомості Верховної Ради України. – 1992. – № 48. Ст. 650.

11. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 158.

12. Про державну таємницю : Закон України від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради України. – 1994. – № 19. – Ст. 98.

13. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII // Відомості Верховної Ради України. – 2018. – № 36. – Ст. 65.

Рецензенти:
кандидат юридичних наук, доцент
І. Манжул,
кандидат юридичних наук
Л. Глущенко

Аннотация. В статье исследовано понятие информационной безопасности, определено ее место в системе национальной безопасности Украины, рассмотрены основные элементы системы информационной безопасности. Проанализированы основные угрозы национальной безопасности в информационной сфере и мероприятия государственной политики для ее обеспечения. Очерчены ключевые проблемы функционирования и усовершенствования системы защиты информации на государственном уровне.

Ключевые слова: информационная безопасность, национальная безопасность, информация, информационная безопасность, угроза информационной безопасности.

Abstract. The article investigates the concept of information security, determines its place in the system of the national security of Ukraine, considers the main elements of the information security system. The main threats to national security in the information sphere as well as the measures of state policy concerning its provision are analyzed. The key problems in the operation and improvement of the information security system at the state level are outlined.

Key words: information security, national security, information, information resources, information security, threats to information security.