УДК 352.07:351.86

Губар О.В.
Національна академія державного управління при Президентові України

ЗАХИСТ ІНФОРМАЦІЇ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ БІОЛОГІЧНОЇ БЕЗПЕКИ: ТЕОРЕТИЧНІ АСПЕКТИ

У статті проведено аналіз теоретичних аспектів захисту інформації суб'єктів забезпечення біологічної безпеки. Розглянуто основні загрози безпеці інформації з обмеженим доступом, розпорядниками якої є суб'єкти біологічної безпеки. Проаналізовано основні канали витоку інформації суб'єктів біологічної безпеки та несанкціонованого доступу до неї. Визначено основні об'єкти захисту інформації суб'єктів біологічної безпеки. Установлено необхідність проведення заходів із виявлення загроз і протидії загрозам біологічній безпеці держави, пов'язаним із використанням кіберпростору, а також посилення контррозвідувального забезпечення суб'єктів біологічної безпеки, інформаційного й науково-технічного потенціалу держави.

Ключові слова: *інформація, суб'єкти біологічної безпеки, захист інформації, об'єкти захисту інформації, канали витоку інформації.*

Постановка проблеми. Відповідно до статті 17 Конституції України, забезпечення інформаційної безпеки зараховано до найважливіших функцій держави. Стратегією кібербезпеки України визначено, що сфера державного управління, інфраструктура електронних комунікацій стають усе більш уразливими до розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі [1]. Стратегією національної безпеки України визначено, що загрозами інформаційній безпеці, кібербезпеці, безпеці інформаційних ресурсів є уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична та моральна застарілість системи охорони державної таємниці й інших видів інформації з обмеженим доступом [2]. Угодою про асоціацію між Україною та Європейським Союзом передбачено співробітництво в боротьбі з кримінальною й незаконною організованою чи іншою діяльністю, а також з метою запобігання їй, включаючи кіберзлочинність [3].

Відкритий і вільний кіберпростір розширює свободу й можливості людей, збагачує суспільство, створює новий глобальний ринок ідей, досліджень та інновацій, стимулює відповідальну й ефективну роботу влади та активне залучення громадян до управління державою [4].

Кіберпростір поєднує всю планету в режимі реального часу, що дає змогу будь-кому в будь-який момент здійснити атаку на будь-яку електронну ціль із будь-якої точки світу, що значно ускладнюється завдання захисту та потребує постійного захисту важливої інфраструктури. Глобалізація мереж і зростаюча інтеграція фізичної інфраструктури у віртуальний світ значно збільшують можливі негативні наслідки протиправного впливу на їх діяльність і призводять до зменшення стійкості.

Водночас на фоні загальносвітової тенденції до ускладнення безпекової ситуації у зв'язку з різким посиленням екстремізму, тероризму, зростанням рівня організованої злочинності існує низка проблемних питань, пов'язаних із віртуальністю кіберпростору. Процеси, що відбуваються в кіберпросторі, впливають на стійкість функціонування критичної інформаційної інфраструктури суб'єктів біологічної безпеки.

Вітчизняні й зарубіжні науковці вважають, що кіберзлочинність набуває вигляду всесвітньої цифрової епідемії, та пов'язують її з такими загрозами національній безпеці, як діяльність іноземних спецслужб і тероризм.

Аналіз останніх досліджень і публікацій. Дослідженню актуальних питань, пов'язаних із різними аспектами захисту інформації з обмеженим доступом, присвячені праці багатьох закордонних і вітчизняних учених. Окремі питання геополітичного суперництва в кіберпросторі, проведення інформаційно-психологічних операцій, протидії інформаційним війнам і забезпечення інформаційної безпеки розглянуто в роботах А. Авраменко, Д. Барлогу, Ю. Вознюк, Я. Волкова, А. Головка, Д. Дубова, І. Діордіца, П. Жантовського, О. Запорожець, В. Кафтан, В. Куткіна, А. Марченко, Н. Марголіної, Т. Матициної, Е. Нестеренко, К. Панцерєва, Л. Піддубної, Ю. Романчик, А. Старунського, С. Соколова, Д.Шибаєва,К.Ширяєва,Ш.Уотермен,Н.Черкасова, С. Хілдрет, Ю. Федоров, О. Яременко та ін.

Актуальні питання, пов'язані із забезпеченням кібербезпеки, виявленням кібератак і захистом об'єктів критичної інформаційної інфраструктури, висвітлено в роботах Б. Ахметова, С. Андреєва, А. Бабенко, В. Бурячок, Г. Бекетова, Є. Бабич, О. Баранова, І. Валюшко, О. Волох, А. Грабарєва, С. Гнатюк, Ю. Грицюк, В. Грохольського, А. Демцова, Д. Дубова, О. Доброжанської, О. Доколяса, А. Давидюк, О. Йона, О. Зерницької, К. Ісмайлова, Є. Кільчицького, О. Корченко, Л. Красненкова, Н. Казакова, Ю. Ковальова, М. Кондратюк, Т. Ключник, В. Лахно, Д. Мініна, С. Мельник, І. Нечипоренко, М. Ожеван, О. Орлова, Ю. Оніщенко, А. Письменницького, В. Сидоренко, Г. Ситника, Н. Сейлова, Р. Сачук, І. Терейковського, Н. Ткачук, Л. Щербак, В. Фурашева, М. Ярової та ін.

Однак до цього часу залишається недостатньо дослідженим питання захисту інформації суб'єктів забезпечення біологічної безпеки, що стало підставою для проведення дослідження.

Постановка завдання. Метою статті є дослідження забезпечення захисту інформації суб'єктів біологічної безпеки

Виклад основного матеріалу дослідження. Процеси глобалізації сприяють розвитку інтернет-ресурсів, стрімкому розвитку геноміки, біоінформатики, синтетичної біології, нанотехнологій, систем цілеспрямованої доставки небезпечних агентів, розширенню спектру загроз для національної безпеки. Темпи розвитку нових технологій значно випереджають темпи вдосконалення державних регуляторних механізмів, що призводить до збільшення кількості протиправних дій, пов'язаних із використанням кіберпростору.

Аналіз сучасної наукової літератури свідчить, що низка специфічних ознак кіберпростору перетворює його на поле воєнного протистояння. Кіберпростір має фізичний рівень інфраструктури, підпорядкований економічним законам суперництва за ресурси й політичним законам суверенної юрисдикції та контролю. Атаки з інформаційної реальності мають низьку вартість, однак можуть бути спрямовані проти фізичного домену, що має обмежені та дороговартісні ресурси. Водночас наслідки впливу кіберсили можуть відчуватися як у кіберпросторі, так і за його межами [5].

Законодавство України визначає інформацію як відомості в будь-якій формі й вигляді, збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації, пояснення осіб і будь-які інші публічно оголошені чи документовані відомості) [6]. Технічний захист інформації здійснюється за допомогою інженерно-технічних заходів і/або програмних і технічних засобів з метою унеможливлення витоку, знищення та блокування інформації, порушення цілісності й режиму доступу до неї [7].

Вітчизняні та зарубіжні науковці поділяють інформацію, що підлягає захисту технічними засобами, на семантичну й ознакову. До семантичної інформації зараховують алфавіт, цифри, символи, професійні визначення тощо. До ознакової інформації – матеріальні об'єкти, властивості яких підлягають технічному захисту, зокрема інформацію щодо їх виду та властивостей [8]. Суб'єкти біологічної безпеки володіють як семантичною, так й ознаковою інформацією, що підлягає технічному захисту.

Основними об'єктами захисту інформації суб'єктів біологічної безпеки, які підлягають технічному захисту, є інформація з обмеженим доступом; будівлі, споруди, приміщення, в яких зберігається інформація, що підлягає охороні; приміщення для ведення перемовин та обробки важливих документів; сейфи й матеріальні носії інформації, які містять інформацію з обмеженим доступом; чернетки та засоби обробки інформації, а також технічні засоби приймання, обробки, зберігання й передавання інформації, зокрема системи та засоби інформатизації, програмні засоби, автоматизовані системи управління та зв'язку, їх інформативні фізичні поля; допоміжні технічні засоби й системи, що не належать до технічних засобів передачі інформації з обмеженим доступом, однак розміщуються в приміщеннях, де обробляється така інформація, а також самі приміщення, в яких циркулює інформація з обмеженим доступом [8; 9].

Основними загрозами безпеці інформації з обмеженим доступом, розпорядниками якої є суб'єкти біологічної безпеки, можуть бути візуальний аналіз об'єкта охорони, підслуховування з використанням технічних засобів, перехват радіосигналів із наступним проведенням семантичного аналізу отриманої інформації тощо. Водночас на підставі аналізу сучасної наукової літератури до основних каналів витоку інформації суб'єктів біологічної безпеки та несанкціонованого доступу до неї можна зарахувати системи вентиляції, лінії зв'язку, наведення на лінії комунікації і сторонні провідники, електроживлення, заземлення, опалення, водопостачання й газопостачання, охоронно-пожежну сигналізацію, трансляційні мережі й гучномовний зв'язок, програмно-апаратні закладки в ПЕОМ, комп'ютерні віруси, радіо закладки в стінах і меблях, виробничі й

технологічні відходи, розкрадання носіїв інформації, витік за рахунок структурного звуку в стінах і перекриттях, а також знімання інформації з дисплею електромагнітним каналом, акустичним каналом з клавіатури і принтера, зі стрічки принтера, погано стертих дискет, за допомогою відеозакладок, лазерного знімання акустичної інформації з вікон, знімання інформації за рахунок наведень і «нав'язування», дистанційне знімання відеоінформації, знімання акустичної інформації з використанням диктофонів, спрямованих мікрофонів або з використанням «телефонного вуха», візуальне знімання з дисплею і принтера, розкрадання носіїв інформації, високочастотні канали витоку в побутовій техніці, витік за рахунок побічного випромінювання термінала, несанкціоноване копіювання, внутрішні канали витоку інформації тощо [8; 9].

Важливу роль у забезпеченні стійкості функціонування інформаційних систем відіграє людський фактор. Так, за даними вітчизняних і зарубіжних науковців, найбільш поширеною та небезпечною загрозою для інформаційних систем є активний вплив людини на керовану систему, понад 61,8% випадків витоку інформації припадає на користувачів, які мають доступ до комп'ютерних інформаційних систем і системи управління обробкою інформації. У цьому випадку технічні засоби захисту виявляються неефективними. Тому сьогодні рівень професіоналізму користувачів, які мають доступ до інформаційних ресурсів, є важливим фактором, що визначає рівень стійкості функціонування комп'ютерних інформаційних систем [10].

Так, за даними щорічного звіту про глобальне дослідження витоків конфіденційної інформації аналітичного центру компанії InfoWatch, найбільше випадків навмисних витоків даних від загальної їх кількості за галузями у 2017 році зареєстровано в США (1089), Російській Федерації (254), Сполученому Королівстві Великої Британії та Північної Ірландії (104), Канаді (69), Австралії (65), Республіці Індія (46), Україні (34), Китайській Народній Республіці (29), Ірландії (15), Південній Кореї (14), Федеративній Республіці Німеччині (11). Також зареєстровано 802 випадки витоку інформації, пов'язані із зовнішніми причинами, і 1228 випадків витоку інформації, пов'язаних з внутрішніми порушеннями. Причинами витоку в 50,3% були співробітники, 41,7% – зовнішні зловмисники, 2,4% – колишні співробітники, у 2,2% – керівники, 2,2% – підрядники та в 1,1% випадків – системні адміністратори. Основними каналами витоку інформації були такі: комп'ютерна мережа (69,8%), електронна пошта (13,3%), паперові носії інформації (8,2%), крадіжки й утрата обладнання (3,3%), знімні носії інформації (2,2%), текстові, голосові, відео- (2,4%) та мобільні пристрої (0,7%) [6].

Витоки інформації внаслідок низької кваліфікації персоналу становили близько 82,9%, шахрайства з використанням даних 11,2% та несанкціонованого доступу 5,9%. За результатами проведеного дослідження компанії InfoWatch установлено, що найбільший відсоток витоку конфіденційної інформації від загальної кількості витоків зареєстровано в медицині (17,4%), у сфері високих технологій (16,7%), у державних органах і силових структурах (16,5%). При цьому найбільший відсоток від загальної кількості навмисних витоків конфіденційної інформації зареєстровано у сфері високих технологій (64,3%), банківській і фінансовій сфері (55,6%), медицині (44,5%), торгівлі (45,1%), освіті (40,5%), державних органах і силових структурах (37,8%) [6].

Також у 2018 р. в усьому світі зареєстровано 429 витоків інформації з медичних закладів (лікарень, поліклінік, військових госпіталів, лабораторій, аптек тощо), що перевищило аналогічний показник 2017 р. на 16%, а кількість скомпрометованих персональних даних збільшилась майже вдвічі і становила 27 млн. Кожен третій виток інформації стався внаслідок хакерської атаки, на частку працівників медичної сфери припадає 53,7% зареєстрованих інцидентів. Співвідношення навмисних і випадкових витоків у медицині становило 47,5% та 52,5%. При цьому серед витоків, що сталися з вини співробітників, відсоток навмисних інцидентів становив приблизно 20%. В основному витоки інформації з обмеженим доступом траплялися внаслідок помилок і недбалості співробітників. Витоки інформації через мережеві канали становили більше ніж 45% від загальної кількості витоків, через електронну пошту сталося 21,1% витоків від загальної кількості, а через паперові носії – 20,2% витоків інформації від загальної кількості витоків. У США з вини компанії, що поставляла програмне забезпечення для медичних закладів, інформація близько 200 000 пацієнтів залишена на незахищеному сервері [11]. За даними порталу TechGoondu в Сінгапурі, з вини підрядної компанії, яка займалась адмініструванням сервера, база даних Сінгапурського управління охорони здоров'я зберігалась на незахищеному паролем сервері, скомпрометовано захищені медичні дані 808,2 тис. донорів крові [12].

Також до основних кіберзлочинів зараховують хакерство, шахрайства й фальсифікації, несанкціоновані проникнення в національні бази даних, учинені за допомогою комп'ютерної техніки, правопорушення у сфері контенту тощо [1].

Розвиток сучасних інформаційних технологій призводить до збільшення кількості можливих каналів витоку інформації, розпорядниками якої є суб'єкти біологічної безпеки. Тому під час удосконалення систем технічного захисту інформації необхідно враховувати особливості реальних каналів витоку інформації. Збільшення рівня інформатизації суб'єктів забезпечення біологічної безпеки, формування великих сховищ даних структурованої інформації, зростання вартості різних типів інформації у сфері біологічної безпеки збільшують ризики витоків інформації з обмеженим доступом.

За прогнозами вітчизняних і зарубіжних учених, найближчим часом зберігатиметься тенденція до збільшення кількості витоків інформації з обмеженим доступом, спричинених діями внутрішніх порушників, і ймовірність виведення з ладу кіберзлочинцями великих об'єктів критичної інфраструктури. Водночас прогнозується збільшення кількості хакерських атак, спрямованих на великі бази даних, що зберігаються з використанням хмарних технологій, і зростання ризику шпіонажу через «розумні пристрої».

Проведений аналіз сучасної наукової літератури свідчить, що натепер реальними є загрози настання негативних наслідків, спричинених уведенням до національних інформаційних баз з питань забезпечення біологічної безпеки недостовірної, руйнівної для них інформації. Водночас глобальна інформатизація збільшує доступність знань із питань синтетичної біології, зокрема, внаслідок розміщення в усесвітній мережі Інтернет наукових статей. Крім того, незважаючи на труднощі у визначенні мети придбання компонентів, що використовуються в синтетичній біології, такі компоненти, зокрема стандартизовані послідовності ДНК, можна замовити та придбати на окремих веб-сайтах.

Наявні системи спостереження за спробами незаконного проникнення до комп'ютерних мереж, наявні бази даних комп'ютерних вірусів та антивірусні програми не забезпечують необхідного рівня кіберзахисту і швидко застарівають [1]. Доступність через кіберпростір автоматизованих систем управління, що забезпечують взаємодію інформаційно-телекомунікаційних мереж, призначених для вирішення завдань державного управління забезпеченням біологічної безпеки, припинення функціонування яких може призвести до тяжких наслідків, ставить забезпечення національної безпеки в залежність від рівня їх захищеності.

Національним законодавством України до критично важливих об'єктів інфраструктури зараховано підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами й/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства й безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей. Комунікаційні або технологічні системи об'єктів критичної інфраструктури, кібератаки на які безпосередньо вплинуть на стале функціонування такого об'єкта критичної інфраструктури, зараховують до об'єктів критичної інформаційної інфраструктури [13].

Застосування кібератак з метою ведення гібридної війни може спричинити порушення функціонування об'єктів інформаційної інфраструктури суб'єктів забезпечення біологічної безпеки, призвести до втрати управління або їх фізичного знищення. У разі використання кібернетичної зброї інформаційні системи й автоматизовані системи управління об'єктів атаки переводяться в кризовий режим функціонування. Ця проблема набуває актуальності під час вирішення завдань забезпечення безпеки об'єктів інформаційної інфраструктури, що мають важливе значення, руйнування яких призведе до негативних наслідків для прилеглих об'єктів, територій, обслуговуючого персоналу та населення [14].

Разом із тим в умовах глобалізації в структурі інформаційних ресурсів вагоме значення мають національні інформаційні ресурси, основані на національній традиції, що використовуються для інформаційного виробництва, інформаційних обмінів в інформаційних комунікаціях всередині країни та за її межами [15].

У розпорядженні суб'єктів забезпечення біологічної безпеки перебувають різноманітні компоненти інформаційної інфраструктури, комп'ютеризовані й пов'язані комп'ютерними мережами з багатьма життєво важливими центрами суспільного життя й галузями господарської діяльності, що займаються виробництвом суспільно зна-

чущої інформації, включаючи управлінську інформацію з питань забезпечення біологічної безпеки. Крім того, Розпорядженням Кабінету Міністрів України передбачено впровадження електронної системи управління інформацією в лабораторній мережі системи громадського здоров'я й електронної інформаційної системи спостереження за інфекційними захворюваннями [16]. Системи, які призначені для посилення епідеміологічного нагляду, збирання, передачі та аналізу даних щодо інфекційних захворювань, поєднують клінічні, епідеміологічні, лабораторні дані, сприяють проведенню детального аналізу зібраних даних, допомагають підвищувати якість прийнятих рішень за рахунок зменшення втрати часу й ресурсів.

Недостатнє усвідомлення суб'єктами забезпечення біологічної безпеки наявних небезпек під час використання кіберпростору може призвести до настання негативних наслідків, про що свідчить недостатнє нормативно-правове регулювання питань використання суб'єктами забезпечення біологічної безпеки незахищених імпортних технічних засобів для зберігання, оброблення й передачі інформації, а також зростання обсягів інформації, що передається відкритими каналами.

Глобальна інформаційна експансія помітно впливає на національні інформаційні ресурси, відбувається їх уніфікація в інтересах держав, що займають провідні позиції у сфері розвитку інформаційних технологій. Недостатня організація захисту національних інформаційних ресурсів за умов активізації інформаційних впливів іноземних держав призводить до введення в обіг несанкціонованої інформації та можливості введення до інформаційних ресурсів суб'єктів забезпечення біологічної безпеки чужорідної, шкідливої інформації.

Висновки. Ужиття заходів, спрямованих на нейтралізацію кіберзагроз суб'єктам біологічної безпеки, потребує відповідного нормативно-правового регулювання, включаючи процеси виробництва, обігу, зберігання та використання національних інформаційних ресурсів у сфері біологічної безпеки, і має базуватись на національній науково-технічній базі.

Існування об'єктів критичної інфраструктури суб'єктів біологічної безпеки в кібернетичному просторі створює нові загрози та потребує розроблення нових інструментів забезпечення безпеки критичної інформаційної інфраструктури, які б гарантували стабільну працездатність в умовах комп'ютерних атак будь-якої інтенсивності.

Забезпечення належного рівня захисту інформації, розпорядниками якої є суб'єкти біологічної безпеки, обов'язково вимагає проведення розвідувальних заходів із виявлення та протидії загрозам біологічній безпеці держави, пов'язаним із використанням кіберпростору, а також посилення контррозвідувального забезпечення інформаційного, науково-технічного потенціалу держави, суб'єктів біологічної безпеки для своєчасного усунення умов виникнення, виявлення і протидії загрозам національній безпеці, пов'язаних із використанням сучасних інформаційних технологій, і забезпечення захисту суб'єктів біологічної безпеки від розвідувально-підривної діяльності, актів зовнішньої інформаційної агресії іноземних спецслужб або інших агентів впливу.

Список літератури:

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016 / Верховна Рада України. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 20.03.2019).

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2015 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 20.03.2019).

3. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16 вересня 2014 р. № 1678-VII / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/1678-18 (дата звернення: 20.03.2019).

4. Цивільний кодекс України від 16 січня 2003 р. № 435-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/435-15/print (дата звернення: 20.03.2019).

5. Дубов Д.В. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України: дис. ... докт. політ. наук: спец. 21.01.01. Київ, 2016. 431 с.

6. InfoWatch. Глобальное исследование утечек конфиденциальной информации в 2017 году. URL: https://www.infowatch. ru/analytics/repor2017 (дата звернення: 20.03.2019).

7. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/print (дата звернення: 20.03.2019).

8. Черкасова Н.В., Нестеренко Е.І., Соколов С.С. Виды информации, защищаемой техническими средствами и демаскирующие признаки объектов защиты. *Новая наука: от идеи к результату:* Международное научное периодическое издание по итогам Международной научно-практической конференции (29 января 2016 г., г. Сургут): в 3 ч. Стерлитамак: РИЦ АМИ, 2016. Ч. 2. 213 с.

9. Василюк В. Об'єкти захисту інформації. Методи та засоби захисту інформації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2006. Вип. 2 (13). 102 с.

10. Ченцов С.В., Краснов И.З., Сидарас А.А. Обеспечение устойчивости информационных систем с учетом человеческого фактора. *Фундаментальные исследования.* 2017. № 11-1. С. 140–144.

11. InfoWatch. Число утечек из медицинских учреждений выросло на 16%. URL: https://www.infowatch.ru/ analytics/digest/15414 (дата звернення: 20.03.2019).

12. More than 800,000 blood donors had personal data exposed, in latest leak in Singapore. March 19th, 2019 by Alfred Siew. URL: https://www.techgoondu.com/ (дата звернення: 20.03.2019).

13. Про телекомунікації: Закон України від 18 листопада 2003 р. № 1280-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show /1280-15 (дата звернення: 20.03.2019).

14. Grechishnikov E., Lybimov V., Komolov D. Influence of the stages of operation of communication facilities on the model of variation of reliability. Telecommunications and Radio Engineering. vol.69, 2010. iss.3, p. 247-256 URL: http://ire.kharkov.ua/tcre/69/69_03.htm (дата звернення: 20.03.2019).

15. Інтернет-комунікація в діяльності інститутів сектору безпеки: теоретико-прикладний аспект: монографія. Луганськ: Янтар, 2013. 664 с.

16. Про затвердження плану заходів щодо реалізації Концепції розвитку системи громадського здоров'я: Розпорядження Кабінету Міністрів України від 18 серпня 2017 р. № 560-р / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/560-2017-%D1% (дата звернення: 20.03.2019).

ЗАЩИТА ИНФОРМАЦИИ СУБЪЕКТОВ ОБЕСПЕЧЕНИЯ БИОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ: ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ

В статье проведен анализ теоретических аспектов защиты информации субъектов обеспечения биологической безопасности. Рассмотрены основные угрозы безопасности информации с ограниченным доступом, распорядителями которой являются субъекты биологической безопасности. Проанализированы основные каналы утечки и несанкционированного доступа к информации субъектов биологической безопасности. Определены основные объекты защиты информации субъектов биологической безопасности. Установлена необходимость проведения мероприятий по выявлению угроз и противодействию угрозам биологической безопасности государства, связанным с использованием киберпространства, а также усилению контрразведывательного обеспечения субъектов биологической безопасности, информационного и научно-технического потенциала государства.

Ключевые слова: *информация, субъекты биологической безопасности, защита информации, объекты защиты информации, каналы утечки информации.*

PROTECTION OF INFORMATION OF SUBJECTS OF ENSURING BIOLOGICAL SECURITY: THEORETICAL ASPECTS

The article analyzes the theoretical aspects of information protection of subjects of providing biological security. The main threats to the security of sensitive information, the managers of which are the subjects of biological security, have been considered. The analysis of the main channels of leak of information the subjects of biological security and unauthorized access to it has been carried out. The main objects of information protection of the subjects of biological security have been identified. Measures to identify and counter the threats to the biological security of the state stemmed from the use of cyberspace, as well as to strengthen the counter-intelligence support for the subjects of biological security, the information and scientific and technical potential of the state have been found necessary.

Key words: *information, subjects of biological security, information protection, objects of information protection, channels of information leakage.*