КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056.5
DOI https://doi.org/10.32782/2521-6643-2023.1-65.8

Тарасенко Ю. С., кандидат фізико-математичних наук,
доцент, доцент кафедри кібербезпеки
та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-4226-5707

НІВЕЛЮВАННЯ ЕЛЕКТРОМАГНІТНОЇ ВРАЗЛИВОСТІ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У статті представлено огляд досліджень, присвячених ухваленню рішень з позицій ризик-інформаційної безпеки сукупності об'єктів критичної інфраструктури. На даний час, що характеризується неминучістю наступаючих гарячих фаз інформаційних війн, аспекти безпеки проявляються в усіх сферах соціуму: від побутових до науково-виробничих, де домінуючою прийнято вважати безпеку держави, суспільства, людини. У такому контексті значимість оцінювання стану безпеки будь-яких сучасних об'єктів, перш за все критично важливих об'єктів з їх інформаційними інфраструктурами, забезпеченням повноти та достовірності інформації у задіяних комп'ютерних мережах з засобами обчислювальної техніки, завжди актуальна і необхідна, Загрози інформаційним ресурсам необхідно розглядати як потенційно можливі випадки антропогенного, техногенного або природного (стихійного) характеру, що можуть спричинити небажаний вплив на інформаційно-телекомунікаційну систему. Проведено аналіз потенційних джерел електромагнітної вразливості інформації, оброблюваної засобами обчислювальної техніки. Деталізовано потенційні варіанти витоку інформації за рахунок небажаних електромагнітних впливів (випромінювань і наведень) типу паразитних електромагнітних випромінювань та наведень. Розглянуто перспективні захисні заходи щодо нівелювання таких впливів у вигляді створення режиму безеховості та додаткового екранування, які забезпечують мінімізацію негативних наслідків на достовірність, цілісність і конфіденційність інформації, оброблюваної засобами обчислювальної техніки. Запропоновано технологію оцінки паразитних випромінювань за межами контрольованої зони об'єкта засобами обчислювальної техніки як для випадку мобільної (за допомогою дронів) її реалізації, так і для стаціонарних варіантів використання контрольно-вимірювальної апаратури з автоматичною індикацією сигналу тривоги про перевищення допустимого рівня витоку паразитних електромагнітних випромінювань. У частині, що стосується витоку інформації технічними каналами об'єкта інформатизації, можна значно нівелювати електромагнітні вразливості службової інформації, що виникають під час роботи засобів обчислювальної техніки, реалізуючи відповідні заходи протидії щодо недостатнього екранування, побічних електромагнітних випромінювань та наведень, та несанкціонованого використання у засобах обчислювальної техніки високочастотного опромінення.

Ключові слова: *ризик, об'єкт критичної інфраструктури, ризик-інформаційна безпека,дрон, електромагнітна вразливість.*

Tarasenko Yu. S. Mitigating the electromagnetic vulnerability of restricted information

The article presents a review of research on decision-making from the perspective of risk-information security of a set of critical infrastructure facilities. At present, characterized by the inevitability of the coming hot phases of information wars, security aspects manifest themselves in all spheres of society: from domestic to scientific and industrial, where the security of the state, society and the individual is considered dominant. In this context, the importance of assessing the security of any modern facilities, primarily critical facilities with their information infrastructures, ensuring the completeness and reliability of the information in the involved computer networks with computer facilities, is always relevant and necessary, Threats to information resources should be seen as potentially possible cases of man-made, man-made or natural (natural) nature, which may cause undesirable effects on the information and telecommunications industry. The analysis of potential sources of electromagnetic vulnerability of information, processed by computer facilities, is performed. Potential variants of information leakage due to undesirable electromagnetic influence (radiation and pickups) of parasitic electromagnetic emission and pickups type are detailed. Perspective protective actions on leveling such influences in the form of creation of a mode of anechoic stability and additional shielding which provide minimization of negative consequences on reliability, integrity and confidentiality of the information, processed by means of computer techniques are considered. The technology of a parasitic radiation assessment outside the controlled area of the object by computer aids is offered both for mobile (by means of drones) its realization and for stationary variants of control and measuring apparatus usage with automatic indication of alarm signal about exceeding of acceptable level of a parasitic electromagnetic radiation leakage. In the part relating to information leakage through technical

channels of the object of informatization, it is possible to considerably level the electromagnetic vulnerability of service information, occurring during operation of computer facilities, by implementing appropriate countermeasures against insufficient shielding, incidental electromagnetic radiation and induction, and unauthorized use in computer facilities of high-frequency irradiation.

Key words: *risk, critical infrastructure facility, risk and information security, drone, electromagnetic vulnerability.*

Вступ і постановка проблеми. На даний час, що характеризується неминучістю наступаючих гарячих фаз інформаційних війн, аспекти безпеки проявляються в усіх сферах соціуму: від побутових до науково-виробничих, де домінуючою прийнято вважати безпеку держави, суспільства, людини. У такому контексті значимість оцінювання стану безпеки будь-яких сучасних об'єктів, перш за все критично важливих (КВО) з їх інформаційними інфраструктурами (ІІ), забезпеченням повноти та достовірності інформації у задіяних комп'ютерних мережах з засобами обчислювальної техніки (ЗОТ), завжди актуальна і необхідна, що вагомо підтверджується прийняттям Закону України [1]. Причому «віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму» [1, ст. 8, п. 2]. Тому, загрози інформаційним ресурсам необхідно розглядати як потенційно можливі випадки антропогенного, техногенного або природного (стихійного) характеру, що можуть спричинити небажаний вплив на інформаційно-телекомунікаційну систему (ІТС), а також на інформацію, яка зберігається в ній [2]. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози, характеризується таким елементом, як вразливість. Вразливість зазвичай розуміється як слабкий момент інформаційной системи (ІС), на основі якої можлива успішна реалізація загрози. Зі свого боку, загроза – це потенційно можлива подія, дія, явище чи процес які можуть завдати шкоди системному ресурсу [3]. Саме за наявносності вразливості, як певної характеристики системи, відбувається активізація базових (найбільш поширених) загроз безпеці інформації: доступності (розкриття інформаційних ресурсів та несанкціонованого доступу до них); цілісності (умисний антропогенний вплив); конфіденційності (викрадення, утрата інформації та засобів її обробки).

Загрози доступності і цілісності інформації пов'язані з неправомірним впливом на неї у вигляді факторів (явищ, дій або процесу), результатом яких можуть бути несанкціоноване знищення, модифікація (спотворення або підміна) або блокування доступу до інформації. Загрози конфіденційності інформації реалізуються за допомогою витоку інформації у вигляді неконтрольованого поширення підзахисної інформації, у результаті чого можливим є несанкціонований до неї доступ і її розголошення зацікавленим суб'єктам, у тому числі державам, іноземним розвідкам, юридичним і фізичним особам. Реалізація таких загроз забезпечується технічними (апаратними) засобами виявлення, прийому (перехвату), регістрації та обробки інформативних сигналів і є найбільш відмінною рисою будь-якої технічної розвідки (ТР) об'єктів інформатизації (ОІ). Під ОІ прийнято розуміти сукупність інформаційних ресурсів, засобів і систем обробки інформації у відповідності до заданої інформаційної технології, включаючи будівлі, споруди, приміщення і технічні засоби, у яких ці засоби та системи встановлені. При цьому об'єкти інформатизації, на яких обробка інформації здійснюється з використанням засобів обчислювальної техніки (ЗОТ), називають об'єктами ЗОТ.

Аналіз останніх досліджень і публікацій. В 2003 року було озвучено «Архітектуру безпеки для систем, що забезпечують зв'язок між кінцевими пристроями», фактично вперше було визначено методологію організації інформаційної безпеки телекомунікаційних систем [4]. Зі створення цифрових мереж інтегрального обслуговування і технології асинхронного методу передачі (ATM – Asynchronous Transfer Mode) почалася реалізація транспортного механізму для передачі усіх видів інформації з QoS (Quality of Service). Їх представлення у єдиному цифровому форматі з виділенням потрібних ресурсів мережі, які гарантують QoS перед початком передачі інформації користувача, є обов'язковими компонентами технологій IP/MPLS (Internet Protokol / Multiprotocol Label Switching – мультипротокольна комутація за мітками) і ATM. Дана архітектура безпеки з гарантованою якістю обслуговування QoS передбачувала розподілення усіх ресурсів телекомунікаційних систем (канали зв'язку, програмно-апаратні комплекси, додатки і т.д.) на незалежні модулі захисту інформації. При цьому кожен модуль повинен задовольняти задекларованим параметрам інформаційної безпеки.

Нажаль, будь-яка, навіть гіпотетично наднадійна, система захисту інформації від навмисних або випадкових впливів природного або штучного походження не здатна повністю забезпечити режим безпечного функціонування як суб'єктів генерування інформації, так і її підтримуючої інфраструктури. Очевидно, що доцільно попереджувати, ніж отримувати наслідки інформаційного протиборства в сфері досягнення односторонніх переваг зловмисником при отриманні, зборі, обробці та використанні інформації обмеженого доступу. Тому, серед більшого різноманіття демаскуючих ознак вразливості інформації, насамперед

доцільно розглядати можливості нівелювання різноманітних електричних і електромагнітних витоків, які можна вважати особливо шкідливими. Їх реалізація можлива на будь-якому підприємстві, що використовує комп'ютери, сервісні стійки, мережі. При цьому основними причинами виникнення електричних каналів витоку інформації є наведення інформативних сигналів, під якими розуміють струми і напруги в струмопровідних елементах, що викликають інформативні та не інформативні побічні (паразитні) електромагнітні випромінювання (ПЕМІ), що призводять до додаткових ємнісних і індукцій. паразитних електромагнітних випромінювань та наведень (ПЕМІН).

Результати дослідження. Як правило, базовим джерелом інформаційного сигналу є засоби обчислювальної техніки, яким властива побічна генерація паразитних електричних і електромагнітних випромінювань і наведень у вигляді ПЕМІ та ПЕМІН. Використовуючи ці супутні фізичні явища, можна засобами ТР вилучати будь-яку інформацію обмеженого доступу, яка оброблюється ЗОТ. Даний процес прийнято називати витоком інформації. Для такої інформації найбільш значимими (актуальними) є наступні форми витоків: 1) розголошення інформації, тобто передача носія інформації сторонній особі (навмисне) або обробка інформації на ЗОТ у присутності сторонньої особи (ненавмисне); 2) несанкціонований доступ (НСД) до інформації, наприклад шляхом: розкриття системного блоку ЗОТ і вилучення HDD диску для копіювання (фізичний); скиду встановлених параметрів BIOS та зміною пріоритету послідовності завантаження носія з наступним завантаженням альтернативної операційної системи і копіюванням цікавої інформації на flash-накопичувач (програмно-апаратний); впровадження в ЗОТ шкідливих програм для здійснення НСД до інформації або її копіювання (програмний); 3) викрадення носіїв інформації; 4) розповсюдження (витік) інформації по технічним каналам приміщень або об'єктів (будівель, споруд, технічних засобів), в яких ці засоби і системи обчислювальної техніки встановлені. При цьому під технічним каналом витоку інформації (ТКВІ) розуміють сукупність об'єкту розвідки, технічного засобу розвідки (ТЗР), за допомогою якого добувається інформація про цей об'єкт, і фізичного середовища, у якій розповсюджується інформаційний сигнал. По суті, під ТКВІ розуміють спосіб отримання з допомогою ТЗР розвідувальної інформації про об'єкт. Причому під розвідувальною інформацією зазвичай розуміють дані чи сукупність даних про об'єкти розвідки незалежно від форму їх представлення.

У залежності від природи виникнення інформативного сигналу технічні канали витоку інформації можна розділити на натуральні та спеціально створювані.

Натуральні канали витоку інформації створюються: 1) за рахунок побічних електромагнітних випромінювань, що виникають при обробці інформації ЗОТ (що і прийнято називати електромагнітними каналами витоку інформації – ЕМКВІ). Основними причинами їх виникнення є: – побічні електромагнітні випромінювання, що виникають внаслідок протікання інформативних сигналів по елементам технічних засобів і систем, які безпосередньо оброблюють інформацію обмеженого доступу (ТСОІ); – модуляція інформативним сигналом побічних електромагнітних випромінювань високочастотних генераторів ТСОІ; – модуляція інформативним сигналом паразитного електромагнітного випромінення ТСОІ (наприклад, яке виникає внаслідок самозбудження підсилювачів низької частоти); 2) внаслідок наведень інформативних сигналів у лініях електроживлення і заземлення ЗОТ, з'єднувальних лініях допоміжних технічних засобів і систем (ДТСС) і сторонніх провідниках у вигляді металічних труб систем опалення, водопостачання, будь-яких металоконструкцій і т.д., що і прийнято називати електричними каналами витоку інформації (ЕКВІ).

До спеціально створюваним каналам витоку інформації відносять канали, реалізовані шляхом впровадження в ЗОТ електронних закладних пристроїв перехоплення інформації або шляхом високочастотного опромінення засобів обчислювальної техніки.

З позицій кібербезпеки ІТ-інфраструктури прийнято аналізувати інформаційну безпеку з використанням двох способів: аудиту системи або проведення тестів на проникнення (penetration test, pentest) [5,6]. Ці тести на проникнення або пентести реалізують метод оцінки безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника. З позицій кібербезпеки об'єктів критичної інфраструктури (ОКІ) нівелювання таких загроз за своєю сутністю мають багатогранну сферу діяльності, включаючи и багатоликий арсенал технічних засобів розвідок. Основна їх відмінність від легальної розвідки, яка добуває інформацію при різноманітних офіційних зв'язках і контактах із засобів масової інформації, пов'язана з використовуваною спецапаратурою і способами ведення розвідки. Зазвичай к ТСР відносять такі види розвідок: радіоелектронні, гідроакустичні, акустичні, оптико-електронні, візуально-оптичні, хімічні, радіаційні, сейсмічні, магнітометричні, комп'ютерні, фотографічні та їх різновиди. Зокрема, радіоелектронна розвідка (РЕР) дозволяє отримувати інформацію шляхом прийому та аналізу електромагнітного випромінення (ЕМВ) радіодіапазону, створюваного різноманітними радіоелектронними засобами.

Безперечно всі ці ТСР направлені також и на об'єкти інформаційної безпеки, що об'єднують інформаційні ресурси, канали інформаційного обміну та телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури [7].

Для протидії загрозам інформаційній безпеці (ІБ), зниження ризиків ІБ, результативної обробки інцидентів ІБ і ефективної боротьби з методами будь-яких розвідок необхідно забезпечувати, і протягом

тривалого часу, зберігати штатний рівень ІБ у вигляді стабільного стану захищеності інформації у відповідності з позиціями законодавчої реалізації сукупності її властивостей: доступності, цілісності, достовірності, конфіденційності, автентичності і т.д.

Інформативні ПЕМІ, як небажані електромагнітні випромінювання, призводять до витоку інформації, що обробляється. Неінформативні ПЕМІ дозволяють одержати лише уявлення про режим роботи ЗОТ, але не розкривають характер інформації, оброблюваної на ціх ЗОТ. Тому з погляду захисту інформації небезпеку створюють лише інформативні ПЕМІ, що представляє є високочастотну несучу, модульовану інформацією оброблюваної засобами обчислювальної техніки. Вони виникають за різних режимах обробки інформації засобами обчислювальної техніки. Зокрема, при: виведенні інформації на монітор; введення даних із клавіатури; запису/читанні інформації на/з накопичувачів; передачі даних в канали зв'язку та на друковані пристрої тощо. Залежно від режиму роботи і типу ЗОТ виникають свої ознаки, що демаскують, включаючи і характерні амплітудно-частотні особливості ПЕМІ, частотний діапазон яких може становити від сотень Гц до десятків ГГц. При цьому навколишній простір, в межах якого можливий перехоплення побічних електромагнітних випромінювань і подальше відновлення інформації, що міститься в них, залежить від інтенсивності ПЕМІ і чутливості приймальної апаратури ТСР.

Відносно ПЕМІН необхідно акцентувати увагу на тому, що вони проявляються як результат електромагнітного наведення інформативних сигналів від ЗОТ, що викликані побічними електромагнітними випромінюваннями у вигляді індукованих струмів і напруг в струмопровідних елементах з ємкісними та індуктивними зв'язками. Такі електромагнітні наведення можуть призводити до витоку інформації по струмопровідним комунікаціям, що мають вихід за межі безпечної (контрольованої) зони. При цьому виявлення інформативних сигналів з інженерних комунікацій ТСР ПЕМІН залежить від відстані між джерелом випромінювання, типу електроживлення, якості заземлення ЗОТ, характеристик антени, що приймає (зондує), рівня супутніх пасивних шумів і активних перешкод, а також і інших факторів.

Залежно від фізичних причин виникнення ПЕМІ та ПЕМІН за рахунок ЗОТ використовують різні методи (принципи) їх реалізації або нівелювання. До активних способів такого впливу (наприклад, перехоплення) інформації, що обробляється ЗОТ, відносять технічні канали витоку інформації (ТКВІ) з високочастотним опроміненням ЗОТ та встановленням у ЗОТ спеціальних закладних пристроїв.

У першому випадку, наприклад, для їх нівелювання, на ЗОТ впливають потужним високочастотним сигналом, бажано реалізованому в режимі свіпування, завдяки чому перекривається (активно зашумлюється) вторинне випромінювання у вигляді ПЕМІ та ПЕМІН, апріорі промодульовані інформативним сигналом. Таким чином, порушується можливий несанкціонований відбір інформації.

У другому випадку для перехоплення інформації, що обробляється ЗОТ, встановлюють у них спеціальні заставні пристрої, що забезпечують або витік інформації, або блокування, або порушення цілісності інформації. Класифікацію таких закладних пристроїв можна проводити за багатьма ознаками, у тому числі: – за способом передачі інформації (по радіо або оптичному каналу, по мережі електроживлення, використання цифрових накопичувачів типу flash-пам'яті і т.д.); – за засобом передачі інформації (типу ІЧ-порту або пристроїв типу Wi-Fi, Bluetooth, WiMAX і т.д.); – за місцем установки (у корпусі системного блоку, або монітора, або клавіатури, або принтера тощо); – за видом перехоплюваної інформації (з клавіатури, з принтера, з відеозображення монітора, використовуючи апаратні кейлоггери – keylogger hardware, каналами зв'язку при запису на жорсткий диск комп'ютера (HDD) або зовнішні накопичувачі типу flash-пам'яті, CD, DVD, USB, апаратні кейлогери з передачею інформації з радіоканалу); – за типом джерела живлення, способами накопичення та кодування, за видом виконання та способом управління передавачем.

Закладні пристрої складаються з електроних блоків перехоплення/передачі інформації (або модуля запису інформації), радиотехничного блоку дистанційного управління і електричного блоку живлення. Очевидно, що виявлення таких блоків та захист від їх шкідливих впливів потребують серйозних, і не лише технічних засобів інформаційної безпеки. До найперспективніших захисних заходів щодо нівелювання таких впливів слід вважати методи з використанням безеховості, екранування та технологію нелінійної радіолокації, в основі якої використовують нелінійні властивості напівпровідників, наявні у складі будь-яких радіоелектронних закладок [8].

У першому випадку режим безеховості реалізують, наприклад, за допомогою безехових камер (БЕК), які, крім того, здатні конструктивно забезпечувати будь-який заданий рівень екранування [8; 9]. В основі створення режиму безеховості лежить принцип поглинання електромагнітного сигналу від будь-якої перешкоди на шляху розповсюдження акустичної або електромагнітної хвилі. Під перешкодою прийнято розуміти будь-яку неоднорідність параметрів середовища, в якій поширюється хвиля. Для електромагнітних хвиль – це будь-яка зміна діелектричної та/або магнітної комплексних проникностей середовища, яка оцінюється як неоднорідність. Основними факторами, що визначають якість БЕК, є їх розміри й форма, а також якість застосованого радіопоглинаючого матеріалу. Очевидно, що чим менше значення паразитних розсіяних полів, тем менший коефіцієнт безеховості (КБЕ) й тим краща якість БЕК. При цьому робочий об'єм БЕК, як область простору БЕК з апріорі заданим КБЕ, (який прийнято також називати безеховою зоною), варто використовувати для ЗОТ. В такому випадку забезпечується додаткова екранування джерел паразитних

електромагнітних випромінень и наведень від ЗОТ у вигляді потенційно можливих ПЕМІ та ПЕМІН, що не виходять за кордони контрольованої зони об'єкту інформатизації. Крім того реалізується можливість оцінки рівня достовірності контрольних (експертних) вимірювань через апостеріорне їх підтвердження або оптротестування, так необхідних при аналізі штатної працездатності ЗОТ. Хоча залишковий вибір рішення по використанню задіяної контрольно-вимірювальної апаратури може бути оцінений тільки після її експериментальної апробації.

З появою ближньої, а в подальшому й нелінійної радіолокації з'явилася можливість вирішувати, крім радіолокаційних, цілий ряд інших прикладних задач, наприклад, задач діагностичного й дефектоскопічного характеру, криміналістики та боротьби з тероризмом [10-12, с.16]. З огляду на це виявлення прихованих закладних пристроїв в ЗОТ, як об'єктів штучного походження, які перебувають в умовах взаємодії з контрольна–вимірювальною радіоапаратурою які використовують ефекти нелінійного розсіювання електромагнітних хвиль (ЕМХ), випромінюваних радіолокаційної станцією ближній взаємодії, також не є проблематичним. При цьому у якості мобільного технічного засобу, що реалізує вивчення за витоком ПЕМІН в ІТС за межі кордону контрольованої зони об'єкта дослідження, доцільно використовувати дрони з відповідною контрольно-вимірювальною апаратурою (КВА), що забезпечує режими виявлення, вимірювання, розпізнавання і дозволу ТКВІ.

Як правило, у прихованні роботи безпілотних літальних апаратів (БЛА, дронів або безпілотних авіаційних систем – БПЛС) зацікавлені усі сторони, особливо в період їхньої конфронтації. Тому дрони, залежно від позицій конфліктуючих сторін, прийнято ділити на ворожі та свої. Причому за відсутності конкретної нормативно-правової основи на рівні ISO, незважаючи на серію стандартів на кшталт ISO 21384 та ISO 23629 щодо БЛА, не існує чіткої класифікації дронів. Проте очевидно, що дуже ефективним, під час виконання завдань забезпечення безпеки підвідомчих об'єктів (і не тільки від ворожого моніторингу), є використання дронів, здатних реалізовувати як відеоспостереження з урахуванням комп'ютерного зору [13], так й виявлення ПЕМІН від ЗОТ. В обох випадках використання радіодіапазону, як і раніше, є актуальне. Таким чином, фактично методи радіолокації виявлення, дозволу, вимірювання та розпізнавання стають основними при створенні систем контролю та управління доступу, перш за все, до об'єктів критичної інфраструктури [14], до яких слід відносити і ЗОТ.

Зазвичай у дронах використовують різні рівні автономності: від керованих дистанційно до автоматичного рівня. У випадку дистанційно пілотованого дрона успішність виконання польотного завдання багато в чому визначатиметься властивостями інформаційно-вимірювальної системи дронів, яка має володіти як елементами інтелекту, так і відповідною системою захисту від несанкціонованих до неї вторгнень з метою порушення штатної працездатності дрону. Такі дрони вертолітного типу у найнижчіх ешелонах (тобто притискаючись до землі) могут входить у зони дії ближньої, а також і нелінійної радіолокації. У таких реальних умовах відповідна КВА з визначенням паразитних випромінювань за межами контрольованої зони об'єкта ЗОТ реализує вимірювання у зовнішньому ефірі витоків ПЕМІН с високою достовірністю і надійністю.

При цьому використовуючи оптимальну фільтрацію, наприклад, кореляційним приймачем, граничний пристрій якого налаштований відповідно до критерію Неймана-Пірсона або за критерієм ідеального спостерігача, можна навіть забезпечити автоматичну індикацію (в аналоговій, в цифровий, в звуковий або у візуальній формі) сигналу тривоги про перевищення допустимого рівня витоку. Очевидно, що рівень достовірності тривоги доцільно виставляти (вибирати) за апріорі заданою величиною ймовірності правильного виявлення або ймовірності хибної тривоги. Вибір останніх регламентують не тільки в процесі метрологічного калібрування чутливості КВА, а й її потенційної роздільної здатності за вторинним електромагнітним перевипромінюванням у вигляді каліброваних цілей на кшталт сфери, кутових відбивачів, металевих поверхонь різної геометрії і т.д. Отже, підключаючи методи радіолокаційної роздільної здатності, з'являється можливість розпізнавання джерела паразитного витоку, використовуючи арсенал апріорних значень ефективних поверхонь розсіювання об'єкта інформатизації. Якщо контрольовані зони об'єктів ІБ мають вигляд закритих приміщень, то бажано всі виявлені під час пуско-налагоджувальних робіт так звані «блискучі точки» нівелювати шляхом використання радіопоглинаючих матеріалів [8; 9].

Висновки. Проведено аналіз потенційних джерел електромагнітної вразливості інформації, оброблюваної засобами обчислювальної техніки. Деталізовано потенційні варіанти витоку інформації за рахунок небажаних електромагнітних впливів (випромінювань і наведень) типу паразитних електромагнітних випромінювань та наведень.

Розглянуто перспективні захисні заходи щодо нівелювання таких впливів у вигляді створення режиму безеховості та додаткового екранування, які забезпечують мінімізацію негативних наслідків на достовірність, цілісність і конфіденційність інформації, оброблюваної засобами обчислювальної техніки.

Запропоновано технологію оцінки паразитних випромінювань за межами контрольованої зони об'єкта засобами обчислювальної техніки як для випадку мобільної (за допомогою дронів) її реалізації, так і для стаціонарних контрольно-вимірювальної апаратури з автоматичною індикацією сигналу тривоги про перевищення допустимого рівня витоку паразитних електромагнітних випромінювань.

Таким чином, у частині, що стосується витоку інформації по технічних каналах об'єкта інформатизації, можна значно нівелювати електромагнітні вразливості службової інформації, що виникають при роботі засобів обчислювальної техніки, реалізуючи відповідні (наведені вище) заходи протидії щодо недостатнього екранування, побічних електромагнітних випромінювань, ворожого впливу потужним високочастотним сигналом та електромагнітних наведень.

Список використаних джерел:

1. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. *Голос України*. 2021. 14 груд. (№ 236).
2. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. *Методологія побудови класифікатора загроз* : монографія. Київ : НАУ, 2015. 214 с.
3. Kurt Jensen. Coloured Petri Nets: Basic Concepts (Volume 1). Monographs in Theoretical Computer Science. Springer Verlag, Heidelberg, Germany, 1997.
4. UTI-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications, 2003.
5. Frank Swiderski and Window Snyder. Threat Modeling. Microsoft Press, 2004. 288 pages.
6. Стеценко І. В., Савчук В. В. Метод автоматизації тестування на проникнення вебатак. *Технічні науки та технології.* 2021. № 1 (19). С. 98–103. DOI: https://doi.org/10.25140/2411-5363-2020-1(19)-98-103
7. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. Київ : КНТ, 2006. 280 с. (Серія: Національна і міжнародна безпека)
8. Тарасенко Ю.С. Фізичні основи радіолокації. Дніпро : Пороги, 2011. 487 с.
9. Тарасенко Ю.С., Смірнов В.В., Стелюк Б.Б., Прокопович-Ткаченко Д.І. Режим безеховості в інформаційно-вимірювальної системі митного контролю. *Системи та технології*. 2019. № 2 (58) С. 170–182.
10. Тарасенко Ю.С., Смірнов В.В., Прокопович-Ткаченко Д.І. Особливості виявлення прихованих об'єктів штучного походження в умовах митного контролю. *Системи та технології*. 2019. № 2 (58) С. 161–169.
11. Заїчко К.В. Аспекти безпечної роботи при користуванні нелінійним локатором. *Науково-практичний журнал Сучасна спеціальна техніка*. 2015. № 3 (42). С. 16–23.
12. Юсупов В. В., Приходько Ю. П., Фурман Я. В. та ін. Пошук та знешкодження саморобних вибухових пристроїв : метод. рек. Київ : Нац. акад. внутр. справ, 2017. 31 с.
13. Вовк С.М., Гнатушенко В.В., Бондаренко М.В. Методи обробки зображень та компютерний зір : навчальний посібник. Д. : ЛІРА, 2016. 148 с.
14. Tarasenko Yu.S., Klym V.Yu. Safety of critical infrastructure objects from the positions of risk effectiveness reduction. *System technologies.* 2022. Vol. 4. No. 141. Pp. 158–168. DOI: https://doi.org/10.34185/1562-9945-4-141-2022-13

References:

1. Pro krytychnu infrastrukturu [On critical infrastructure]: Zakon Ukrayiny vid 16.11.2021r. № 1882-IX. Holos Ukrayiny. 2021. 14 hrud. (№ 236).
2. Yudin O.K., Buchyk S.S. Derzhavni informatsiyni resursy. Metodolohiya pobudovy klasyfikatora zahroz [State information resources. Methodology for building a threat classifier]: monohrafiya – K.: NAU, 2015. -214s.
3. Kurt Jensen. Coloured Petri Nets: Basic Concepts (Volume 1). Monographs in Theoretical Computer Science. Springer Verlag, Heidelberg, Germany, 1997.
4. UTI-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications, 2003.
5. Frank Swiderski and Window Snyder. Threat Modeling. Microsoft Press, 2004. 288 pages.
6. Stetsenko, I. V., Savchuk, V. V. Metod avtomatyzatsiyi testuvannya na pronyknennya vebatak [Method of automating web attack penetration testing]. Tekhnichni nauky ta tekhnolohiyi, (1(19), 2021. C. 98–103. https://doi.org/10.25140/2411-5363-2020-1(19)-98-103
7. Lipkan V. A., Maksymenko Yu. Ye., Zhelikhovskyy V. M. Informatsiyna bezpeka Ukrayiny v umovakh yevrointehratsiyi [Information security of Ukraine in the conditions of European integration]: Navchalnyy posibnyk. K.: KNT, 2006. 280 s. (Seriya: Natsionalna i mizhnarodna bezpeka)
8. Tarasenko Yu.S. Fizychni osnovy radiolokatsiyi [Physical foundations of radar]. Dnipro: Porohy, 2011. 487 s.
9. Tarasenko Yu.S., Smirnov V.V., Stelyuk B.B., Prokopovych-Tkachenko D.I. Rezhym bezekhovosti v informatsiyno-vymiryuvalnoyi systemi mytnoho kontrolyu [Anechoic mode in the information and measurement system of customs control]. *Systemy ta tekhnolohiyi*. Dnipro: UMSF. 2019. № 2(58). S. 170-182.
10. Tarasenko Yu.S., Smirnov V.V., Prokopovych-Tkachenko D.I. Osoblyvosti vyyavlennya prykhovanykh obyektiv shtuchnoho pokhodzhennya v umovakh mytnoho kontrolyu [Peculiarities of detection of hidden objects of artificial origin in the conditions of customs control]. *Systemy ta tekhnolohiyi*. Dnipro : UMSF. 2019. № 2(58). S. 161–169.

11. Zayichko K.V. Aspekty bezpechnoyi roboty pry korystuvanni neliniynym lokatorom [Aspects of safe work when using a non-linear locator]. Naukovo-praktychnyy zhurnal Suchasna spetsialna tekhnika. 2015. № 3(42). S. 16–23.

12. Yusupov V.V., Prykhod'ko Yu.P., Furman Ya.V. ta in. Poshuk ta zneshkodzhennya samorobnykh vybukhovykh prystroyiv [Search and disposal of improvised explosive devices]: metod. rek. K.: Nats. akad. vnutr. sprav, 2017. 31 s.

13. Vovk S.M., Hnatushenko V.V., Bondarenko M.V. Metody obrobky zobrazhen ta kompyuternyy zir [Image processing methods and computer vision]: Navchalnyy posibnyk. D.: LIRA, 2016. 148 s.

14. Tarasenko Yu.S., Klym V.Yu. Safety of critical infrastructure objects from the positions of risk effectiveness reduction. Vol. 4 No. 141 (2022): System technologies. Pp. 158–168. DOI: https://doi.org/10.34185/1562-9945-4-141-2022-13