УДК 355/359.07

Гулак Юрій Степанович *(канд. військ. наук, доцент)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ПРОБЛЕМИ ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ ПО ТЕХНІЧНИМ КАНАЛАХ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Розглядається питання захищеності інформації з обмеженим доступом, яка циркулює в органах державної влади і управління від технічної розвідки, проблеми та шляхи їх вирішення в умовах ведення гібридної війни проти України.

Ключові слова: *органи державної влади, технічна розвідка, захист інформації.*

Вступ

Задовго до початку збройної агресії Російська Федерація (РФ) почала розвивати і посилювати свої розвідувальні служби, удосконалювати технічну розвідку, нарощувати її можливості та значно активізувала її на території України. Зокрема, у другій половині 2013 року було значно активізовано агентурну роботу на території України.

Можливості ведення агентурної розвідки безпосередньо на території України були дуже високі через розвиток співпраці в економічній, науково-технічній, військовій, політичній, соціальній та гуманітарній й інших сферах, створення своїх підприємств та спільних за участю великої частки російського капіталу тощо [1].

Крім цього, відомо, що крім традиційних об'єктів, якими були зацікавлені спецслужби РФ, їх підвищена увага приділялась інформації щодо сучасних технологій, про природні ресурси, стан фінансів, обороноздатності країни, торгівлі, тощо. Доступ до інформації щодо цих питань став спрощений в тому числі і через широке впровадження інформаційних і телекомунікаційних систем.

Російська Федерація приділила великої уваги щодо забезпечення своїх спецслужб та агентуру на території України сучасними системами та засобами ведення технічної розвідки (ТР). В дану сферу вкладаються великі кошти, серійно виробляються и широко розповсюджуються тисячі моделей технічних спеціальних засобів. Вони активно використовуються російськими спецслужбами та агентурою на території України, чому вже маються багаточисельні випадки.

Високі можливості сучасних засобів ТР, висока ймовірність їх застосування російською агентурою або особами, які пов'язані з російськими спецслужбами чи незаконними збройними формуваннями, в сучасних умовах, висуває підвищені вимоги до захищеності інформаційних систем органів державної влади і управління.

Постановка проблеми. З початком опору України воєнній агресії Російської Федерації на території Донецької і Луганської областей, а також окупації і анексії українського Криму, інформаційна політика Російської Федерації трансформувалася у тотальну військову агресію. Україна на собі відчула вагу інформаційного чинника. Причому він в окремих випадках стає самостійним елементом і виявляється не менш важливим, ніж військовий [2].

Східні та південні області України – стали одними із важливих об'єктів, на які була спрямована робота спецслужб РФ, реалізувався дуже потужний та оперативний сценарій [3, 4]. І по сьогоднішній день спецслужби РФ застосовують проти України широкий спектр своїх можливостей, насамперед агентурну розвідку. Арсенал засобів і методів випробуваний у різні часи [5].

Діяльність щодо збору необхідної інформації РФ розпочала ще задовго до анексії Криму. Особливо активними були підлегла головному розвідувальному управлінню РФ (ГРУ) розвідка Чорноморського флоту й розвідувальні центри в прикордонних областях РФ. З 2004 року вони збирали інформацію про дислокацію й склад військових об'єктів ЗС України, наявність засобів зв'язку, озброєння, командний склад тощо. Так, 2009 року на території Одеської області під час успішної контррозвідувальної операції Служба безпеки України затримала на місці злочину групу кадрових розвідників ГРУ, котрі намагалися завербувати офіцера Збройних Сил України й отримати таємні документи [5].

2010 року підривна робота проти України активізувалася, до того ж для агентурного проникнення на об'єкти ЗС України, особливо в Криму, ГРУ вдалося завербувати низку агентів серед українських офіцерів середньої й вищої ланок. Географія цих вербувань охоплювала всю Україну. Агентурна павутина тією чи іншою мірою обплутувала й Службу безпеки України, Міністерство оборони, Генеральний Штаб ЗС України, й певні державні структури, зокрема на рівні областей. І це не враховуючи агентури Федеральної служби безпеки та служби зовнішньої розвідки РФ [5].

Їх дії в середині України були спрямовані на встановлення контролю над окремими територіями та елементами інфраструктури, виведення з ладу (дезорганізація, тощо) об'єктів

критичної інфраструктури, каналів зв'язку або систем управління, які призводять до унеможливлення виконання суб'єктами забезпечення національної безпеки своїх функцій.

Східні та південні області України, поміж тим, що деякі з них межують з РФ, являються розвиненими промислово-аграрними територіальними утворенням, які мають великий вплив на економічний, науково-технічний і оборонний потенціал України. На багатьох підприємствах областей ведуться новітні розробки державного значення в галузі створення і виробництва ракетно-космічної і авіаційної техніки, засобів управління і зв'язку для військ, танкобудування тощо. На їх території розташовані велика кількість військових формувань, арсеналів, баз та складів боєприпасів, штаби Оперативних командувань, тощо. Природно, що велика кількість інформації (конфіденційної, службової і таємної) щодо цих об'єктів, як прямої так і непрямої, концентрується в органах державної влади і управління.

Високий економічний, військово-науковий та військово-політичний потенціал регіонів і по цей день утримує його в сфері інтересів спецслужб РФ. За останні роки виявлено декілька десятків громадян РФ, які відвідували дані області та підозрювались в належності до агентури або кадровому складу спецслужб РФ. В результаті оперативно-розшукової діяльності неодноразово виявлялись засоби технічної розвідки в державних установах. Це вказує на необхідність приділяти значно більше уваги захисту інформації, яка циркулює в органах державної влади і управління від технічної розвідки.

Аналіз остатніх досліджень і публікацій. Аналіз останніх досліджень і публікацій з даній тематиці показує, що сучасним дослідженням, присвяченим проблематиці інформаційної безпеки, у тому числі у сфері організації захисту інформації в органах державної влади (І.Арістова, І.Бачило, В.Брижко, В.Гавловський, Р.Калюжний, В.Копилов, В.Ліпкан, А.Марущак, В.Цимбалюк, М.Швець, Ю.Шемшученко, та інші), притаманна відсутність широкої різноманітності поглядів на вищезазначену проблему. Праці названих науковців створили методологічне підґрунтя для системного розгляду переважної більшості проблем у сфері державного управління забезпеченням інформаційної безпеки. Аналіз історіографії цього питання дає підстави констатувати, що у вітчизняній і зарубіжній літературі недостатньо досліджені формування та реалізації державної політики щодо реагування на сучасні виклики і загрози інформаційній безпеці, потребує обґрунтування процес розробки та вдосконалення організаційно правових механізмів забезпечення інформаційної безпеки в сучасних умовах інформаційного протистоянні гібридної війни Росії проти України.

Захист інформаційних і телекомунікаційних систем – виклик сучасності. Реформи в Україні проходять під знаком стійкого й зростаючого попиту із сторони органів державної влади і управління, державних установ на послуги сучасних інформаційних систем (ІС). Ця тенденція, добре помітна як на національному, так і на регіональних рівнях, об'єктивно відображає потребу суспільства в своєчасному отриманні об'єктивної і усесторонньої інформації, яка необхідна, зокрема, для аналізу ситуації, яка склалася, управління соціальними процесами тощо, скорочення матеріальних, фінансових та інших витрат щодо її отримання, що фактично є відображенням ринкових процесів, що стрімко розвиваються в Україні [6].

В той же час ІС, особливо ті, що інтегровані в глобальні мережі, достатньо уразливі для ТР. При зростанні економічних можливостей України, буде підвищуватись об'єм і цінність інформації, яка буде в них циркулювати, і, відповідно, зростати збиток від її витоку.

Тенденція використання засобів ТР для добування різного роду інформації росте у всьому світі. Сьогодні інформація становиться таким же стратегічним ресурсом, як, наприклад, корисні копалини. Тому у всьому світі значна увага приділяється посиленню контролю за зберіганням і використанням інформації з обмеженим доступом, створенню необхідної правової бази, яка б регламентувала підвищену відповідальність за її витік.

Метою статті є висвітлення стану захищеності інформації з обмеженим доступом, яка циркулює в органах державної влади і управління від технічної розвідки, проблем та можливості подальшого його підвищення в умовах ведення РФ гібридної війни проти України.

Виклад основного матеріалу дослідження.

В ході зростання процесу інформатизації державних і управлінських структур держави важливо знайти "золоту середину" між доступністю інформаційних систем для конкретних легальних користувачів і обмеженими заходами з метою попередження випадкової або навмисно організованого витоку із них інформації з обмеженим доступом, яка може призвести до збитків для регіону і Україні в цілому. З цією метою необхідно розробити чітку концепцію системи захисту і розмежування доступу до інформації з обмеженим доступом, особливо її елементів, що мають стратегічне значення, а потім послідовно реалізувати її при створенні конкретних інформаційних систем.

Природно, що широке впровадження в практику діяльності органів державної влади, органів військового управління тощо, сучасних телекомунікаційних систем, засобів електронно-обчислювальної техніки, спеціальних та інших технічних засобів, як правило іноземного виробництва, об'єктивно призводить до збільшення ймовірності витоку інформації з обмеженим доступом. Тому намічене інтегрування України в європейські та міжнародні системи телекомунікацій і інформаційного обміну неможливе без комплексного рішення проблем інформаційної безпеки.

Впровадження сучасних інформаційних технологій по своїй суті являється створенням

нової культури, перш за все культури роботи з інформацією, навиків безпечного поводження з нею. Це, як правило, достатньо довгий процес. В різних регіонах він буде протікати поступово і потребує для реального освоєння можливостей нових технічних засобів декілька років. З метою прискорення даного процесу доцільно організувати різнорівневу систему навчання перспективним технологіям обробки інформації в тому числі і регіональну.

Щодо проблем комп'ютерної безпеки, то на сьогоднішній день дуже широке розповсюдження, в тому числі і державних установах, отримали персональні комп'ютери, які стали в силу своїх зручностей одним із основних засобів обробки інформації. Особливості їх захисту обумовлюється специфікою їх використання: автономно або в складі локальної мережі. Оскільки комп'ютером, як правило, користується група осіб, то постає проблема обмеження доступу до інформації різних користувачів [7].

В той же час має місце компроміс (який важко вирішується) між ефективністю і зручністю комп'ютерної системи в роботі і ступенем забезпечення вимог щодо її безпеки. Чим більш високі вимоги висуваються до безпеки системи, тим більша кількість ресурсів системи витрачається на забезпечення цих вимог, тим сильніше понижується продуктивність системи і збільшуються терміни вирішення задач, і тим самим незручність працювати в даній системі користувачам. Тобто, чим складніше для рядового користувача здійснити доступ до інформації, тим більше допускається порушень встановленого режиму безпеки.

При проектуванні систем, в яких повинна циркулювати інформація з обмеженим доступом, не завжди враховується можливість "злому" системи шляхом аналізу електромагнітних наведень і випромінювань по радіоканалу. Причому величина зони випромінювання, на якій можливе перехоплення радіосигналів, які містять інформацію, може досягати декілька десятків метрів. У зв'язку з цим у вказаних системах доцільно використовувати лише обладнання, яке має відповідний сертифікат.

Звідси очевидна і важливість проведення регулярних інструментальних перевірок захищеності приміщень органів державної влади і технічних засобів, які в них використовуються, фізичного пошуку можливо закладених в приміщення малогабаритних закладних пристроїв ТР, захисту обчислювальної техніки від несанкціонованого доступу.

На жаль, українська промисловість сьогодні по відомим причинам не може задовольнити попит на сучасне комп'ютерне і комунікаційне обладнання. Тому при створенні вітчизняних інформаційно-телекомунікаційних систем приходиться використовувати імпортні апаратні і програмно-апаратні комплекси. Дана обставина суттєво збільшує можливості спецслужб країни агресора отримувати інформацію з обмеженим доступом із наших телекомунікаційних систем.

Активізувались також спроби просування на український ринок засобів захисту інформації, які розроблені в РФ. Можна констатувати, що вони розроблені з урахуванням потреб спецслужб РФ.

Мусимо визнати, що війна триває не лише на полі бою. Атаки ворога у кіберпросторі – це цілком військова загроза, на яку необхідно відповідно реагувати. Методи цивільного регулювання і контролю тут не діють. У невеличкій Естонії це давно усвідомили. Розуміючи свою фізичну слабкість перед російською армією, там створили надпотужне кібервійсько [8].

В Україні, на жаль, за кіберпостір кожен орган відповідає сам. Це колективна безвідповідальність, а отже, програш у війні. Кібератаки нині – не точкові дії, а спланові акції, протистояти яким може лише якісний захист. Нема жодного сумніву в тому, що для створених у лютому 2017 року військ інформаційних операцій у складі Міноборони РФ, найвразливішою мішенню є Україна, що продемонстровано 27.06.2017 року [9], на якій відпрацьовуються нові методи ведення гібридної війни.

Україна п'ятий рік захищається у цій виснажливій гібридній війні, маючи слабке законодавство, яке регулює сферу кібербезпеки.

У цій ситуації в України як суб'єкта гібридної війни нема іншого вибору, як у стислі строки створити реальний інформаційний захист та кіберзахист, що в даний час робиться за допомогою західних партнерів. Врегулювати законодавство і врешті зрозуміти, що інформаційна загроза у гібридній війні – це не пусті слова, а реальна військова загроза, що має таку ж убивчу силу [8].

Висновки й перспективи подальших досліджень

Таким чином, тенденція до значного збільшення складності і об'єму вирішуємих задач щодо забезпечення інформаційної безпеки органів державної влади, державних установ країни ставить на порядок денний питання про вдосконалення координації діяльності в сфері захисту інформації, зокрема, і від витоку по технічним каналах. Необхідно створити науково обґрунтовану систему взаємодії, обміну інформацією, нормативно-технічною документацією по даній проблемі.

Становиться все більш ясним, що надійний захист інформації, яка циркулює в органах державної влади і державних установах, неможлива без створення чіткої системи, яка б включала в себе структури, що займаються інформаційно-аналітичним забезпеченням (аналізом, оцінкою і прогнозуванням) щодо можливих загроз в даній сфері, виявлення слабких місць, розробкою рекомендацій, методик безпечної роботи з інформацією з обмеженим доступом, навчання ними персоналу, а також впровадження режимних, технічних та інших заходів захисту.

Разом з цим у реформуванні потребує і система технічного захисту інформації, особливо стосовно державних ресурсів. Комплексна система

захисту інформації як механізм більш десятиліття доводив свою ефективність, проте в нинішніх реаліях також вимагає перегляду і доопрацювання. На окрему увагу заслуговує і організація реагування на комп'ютерні інциденти, підкріплена актуальною правовою базою. Безумовно, на першому етапі буде потрібно і якісно інше фінансування цієї діяльності, і тісний контакт між регулятором, правоохоронними органами, державними та громадськими організаціями, проте до кожного з нас має прийти розуміння необхідності формування нової оборонної інформаційної стратегії як в розрізі загальної, так і кібербезпеки.

Література

1. Війна Росії проти України і світу. [Електронний ресурс]. – Режим доступу: http:// www.pravda.com.ua/articles/2014/08/6/7034046/. **2. Шевчук В. П.** Сепаратизм, як інструмент гібридної війни Росії проти України / В. П. Шевчук // Труди університету. – 2017. – № 5 (138). – С. 176 – 179. **3.** Сценарії війни з Росією: бойовики спробують захопити увесь схід України. [Електронний ресурс]. – Режим доступу: http://ipress.ua/news/114337.html. **4.** Східний ексцес. За якими сценаріями може розвиватися ситуація на сході України і хто за цим стоїть [Електронний ресурс]. – Режим доступу: http://ua.korrespondent.net/ukraine/politics/3347801. **5.** "Акваріум" проти України. або таємна війна російського ГРУ. [Електронний ресурс]. – Режим доступу: http://www.viche.info/journal/4793/. **6.** Захист інформації в органах державної влади: виклики сучасності. [Електронний ресурс]. – Режим доступу: http://infosafe.ua/article-3. **7. Мельников В.** Защита информации в компьютерных системах. "Финансы и статистика", М., 1997. **8.** Кіберзахист, що рятує: як нам посилити опір агресії Росії. [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua /columns. **9.** "Промацати слабкі місця цифрової інфраструктури". [Електронний ресурс]. – Режим доступу: http://nv.ua/ukr/ukraine/events/1418907. html.

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Гулак Юрий Степанович (канд. воен. наук, доцент)
Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Рассматриваются вопросы защищенности информации с ограниченным доступом, которая циркулирует в органах государственной власти и управления от технической разведки, проблемы и пути их решения в условиях ведения гибридной войны против Украины.

Ключевые слова: *органы государственной власти, техническая разведка, защита информации.*

THE COUNTERACTION PROBLEMS OF INFORMATION LEAKAGE VIA TECHNICAL CHANNELS IN THE PUBLIC AUTHORITIES UNDER CURRENT CONDITIONS

Yurii S. Hulak (candidate of military sciences, associate professor)

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The article uncovers the issues of the protection of classified information, which circulates in governmental bodies from tactical technical reconnaissance. The problems it faces and the ways of their solution in the context of a hybrid war against Ukraine.

Keywords: *state authorities, technical intelligence, information security*

References

1. The war of Russia against Ukraine and world. [Electronic resource]. it is access Mode: http://www.pravda.com.ua/articles/2014/08/6/7034046/. **2. Shevchuk V.P.** Separatism, as an instrument of hybrid war of Russia against Ukraine / of B. Shevchuk V.P // Labours of university. - 2017. - № 5 (138). - C. 176 - 179. **3.** Scenarios of the war with Russia: the fighters are trying to seize the whole east of Ukraine. [Electronic resource]. - Mode of access: http://ipress.ua/news/114337.html. **4.** Eastern Excess According to what scenarios the situation in the east of Ukraine can develop and who is behind it [Electronic resource]. - Access mode: http://ua.korrespondent.net/ukraine/politics/3347801. **5.** Aquarium "against Ukraine. or the secret war of the Russian GRU. [Electronic resource]. - Access mode: http://www.viche.info/journal/4793/. **6.** Protection of information in state authorities: the challenges of our time. [Electronic resource]. - Mode of access: http://infosafe.ua/article-3. **7. Melnikov V.** Protection of information in computer systems. "Finance and Statistics", Moscow, 1997. **8.** Cybersecurity, which saves: how to strengthen the resistance to Russia's aggression. [Electronic resource]. - Access mode: https://www.epravda.com.ua/columns. 9. "To feel of the weaknesses of digital infrastructure" [Electronic resource]. - Access mode: http://nv.ua/ukr/ukraine/events/1418907.html.