КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

КІБЕРНЕТИЧНА БЕЗПЕКА ДЕРЖАВИ: ХАРАКТЕРНІ ОЗНАКИ ТА ПРОБЛЕМНІ АСПЕКТИ

Олександр Корченко[1], Володимир Бурячок[2], Сергій Гнатюк[1]

[1]Національний авіаційний університет, Україна
[2]Військова частина А1906, Україна

КОРЧЕНКО Олександр Григорович, д.т.н., професор

Рік та місце народження: 1961 рік, м. Київ, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1983 рік.
Посада: завідувач кафедри безпеки інформаційних технологій з 2004 року.
Наукові інтереси: інформаційна та авіаційна безпека.
Публікації: більше 240 наукових публікацій, серед яких монографії, словники, підручники, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: icaocentre@nau.edu.ua

БУРЯЧОК Володимир Леонідович, д.т.н., с.н.с

Рік та місце народження: 1963 рік, м. Лутугіне, Луганська область, Україна.
Освіта: Київське вище інженерне радіотехнічне училище Протиповітряної оборони імені Маршала авіації О.І. Покришкіна, 1985 рік.
Посада: начальник науково-дослідного управління з 2007 року.
Наукові інтереси: системний аналіз, прийняття рішень та науково-технічне прогнозування, інформаційна і кібербезпека
Публікації: більше 120 наукових публікацій, серед яких монографії, навчальні посібники, бюлетені, наукові статті та тези доповідей.
E-mail: BVL-home@ua.fm

ГНАТЮК Сергій Олександрович, к.т.н.

Рік та місце народження: 1985 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, реагування на інциденти інформаційної безпеки, квантова криптографія, кібербезпека цивільної авіації.
Публікації: більше 100 наукових публікацій, серед яких монографії, лабораторний практикум, наукові статті, тези доповідей та патенти на винаходи.
E-mail: s.gnatyuk@nau.edu.ua

Анотація. *Останнім часом досить гостро постає проблема захисту кібернетичного простору держави. Особливої важливості ця проблема набуває у галузях, де циркулює велика кількість критичної інформації (наприклад, галузь цивільної авіації). У зв'язку з цим, у цій роботі визначено характерні ознаки кібербезпеки держави, а також проведено аналіз проблем кібернетичної безпеки України. Крім того, наведено актуальні проблеми кібербезпеки у галузі цивільної авіації і можливі шляхи їх вирішення. Також сформульовано практичні рекомендації щодо забезпечення кібернетичної безпеки як цивільної авіації, так і всього кібернетичного простору України.*

Ключові слова: *кібернетичний простір, кібербезпека, кіберінфраструктура, кібернетичний вплив, цивільна авіація, критична авіаційна інформаційна система, контрзаходи.*

Вступ

Неконтрольоване поширення та необмежене застосування інформаційного і кіберпросторів [1, 2] протягом останніх десятиріч: 1) призвело до *уразливості інформаційної сфери* більшості країн світу *від стороннього кібернетичного впливу;* 2) визначило політичну необхідність *контролю і подальшого регулювання взаємовідносин* у цій царині; 3) дало підстави стверджувати про *особливу актуальність:* процесів *пошуку, збору і добування інформації* у відкритих, відносно відкритих і закритих електронних джерелах; заходів із *забезпечення конфіденційності, цілісності та доступності* власного ІР, а також *протидії цілеспрямованому впливу з боку потенційно можливих кібернетичних втручань і загроз.*

Постановка завдання дослідження

Зважаючи на зазначене та враховуючи постійно зростаючий потенціал використання мережі Internet у військових цілях, провідні країни світу такі, як США, Японія, Франція, Великобританія, Росія, Китай та багато інших протягом останніх років активно модернізують власні сектори безпеки [1] й, передусім, безпеки кібернетичної, віддаючи при цьому головну роль проблемі завоювання інформаційної переваги в управлінні військами (силами) і зброєю, а також удосконаленню нормативно-правової бази. У практику збройної боротьби вони активно впроваджують концепцію інформаційного протиборства, що передбачає ведення активних розвідувальних дій щодо об'єкта нападу або потенційного порушника та дій, спрямованих на захист національних інтересів від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз. Наслідком таких дій невдовзі можуть стати так звані кібернетичні війни [3], основними методами ведення яких на тактичному рівні вже нині визнані кібератаки, а на стратегічному та спеціальному рівнях – кібероперації. Практично усі вони в умовах сьогодення досягають очікуваного від них результату. Підтвердженням цьому є атаки, спричинені вірусами Stuxnet і Hydraq – двома найпомітнішими кіберподіями 2010 року, троянськими вірусними програмами Duqu та Flame (2011 рік), Mahdi та Gauss (2012 рік), а також події навколо сайту Wikileaks, які кардинально змінили межі загроз та показали усьому світу, що можливості кіберзброї можуть бути досить вражаючими, а протидія її негативному впливу може виявитися вкрай складним завданням для сторін, що захищаються. З огляду на це, **метою** цієї статті є визначення характерних ознак кібербезпеки держави, а також аналіз проблем кібернетичної безпеки України (зокрема у галузі цивільної авіації). Досягнення мети дослідження дозволить формалізувати необхідні контрзаходи, яких необхідно вжити для підвищення загального рівня кібербезпеки держави.

Характерні ознаки кібернетичної безпеки держави

Такий стан справ дає підстави стверджувати, що відсутність надійної системи кібернетичної безпеки (*стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури та засобів їх взаємодії від ризику стороннього кібернетичного впливу*) може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам іншої (протиборчої) сторони (рис. 1) [1, 2].

Рис. 1. Складові кібернетичної безпеки

Характерними ознаками, які нині уособлюють поняття кібербезпеки є *сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційного ресурсу (ІР), інформаційно-комунікаційних технологій (ІКТ) та інформаційно-телекомунікаційних систем (ІТС)* [4], та які спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої інформаційної і кіберінфраструктури. Останнім часом такі дії займають чільне місце у геополітичній конкуренції переважної більшості країн світу, що, в свою чергу, обумовлює нові завдання їх збройних сил й виводить на перший план проблеми так званого інформаційного протиборства. Серед причин такої ситуації можна назвати:

– *відсутність або недосконалість нормативно-правової бази,* яка б забороняла застосування інформаційної і кіберзброї, та проведення інформаційних і кібероперацій, а також встановлювала б відповідальність протиборчих сторін за здійснення злочинів у ІТ сфері;

– *формування* окремими державами власних

доктрин і стратегій *наступальних та підривних дій в інформаційному і кіберпросторах;*

– *створення та застосування* спеціальних сил і засобів *негативного впливу на критично важливу інформаційну і кіберінфраструктуру;*

– *проникнення ІТ в усі сфери державного й громадського життя,* побудова на їх основі систем державного і військового управління;

– *розвиток державних проектів і програм у сфері інформатизації* (електронний документообіг, міжвідомча електронна взаємодія, універсальні електронні карти, надання державних послуг в електронній формі), спрямованих на формування інформаційного суспільства тощо.

Проблеми кібербезпеки України

Наша держава, як самодостатня і суверена держава, з моменту здобуття незалежності, шляхом налагодження співробітництва з міжнародними інституціями, прагне створити комплексну систему протидії внутрішнім і зовнішнім загрозам власному кібернетичному простору. Тим не менш, як відмічають вітчизняні і західні фахівці, нині існує ціла низка проблем, що заважають нашій державі, яка прагне до ЄС, це зробити. До *найбільш значущих,* серед них, слід віднести [1]:

– деградацію науково-технічного потенціалу України, нерозвиненість національної інноваційної системи в інфосфері та низький рівень конкурентоспроможності в ній;

– значну уразливість інфосфери України через надмірно широке впровадження у ній західних програмних продуктів (зокрема фірми Microsoft) та використання матеріально-технічних засобів іноземного виробництва;

– непрозорість розподілу обов'язків між певними відомствами, правоохоронними органами і силовими структурами України, що спеціалізуються на проблемах кіберзахисту та їх незадовільне кадрове забезпечення каліфікованими фахівцями з цих питань;

– відсутність загальнонаціонального координаційного центру, який був би спроможним узгоджувати і координувати діяльність зазначених вище правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному і кіберпросторам України, та керувати проведенням комплексних навчань з проблеми забезпечення кібернетичної безпеки держави в інфосфері на кшталт навчань «Cyber Storm», які проводяться в США та/або «Cyber Europe», що проводяться у ЄС;

– відсутність єдиного понятійно-термінологічного поля кібербезпеки України, як головної складової інформаційної безпеки, а також системних нормативно-правових документів, які б регламентували діяльність зазначених відомств, правоохоронних і силових структур у сфері кіберзахисту тощо.

Такий стан справ фактично є каталізатором для реалізації втручань і загроз в інфосферу України, результатом чого може стати порушення управління державою, її інституціями та окремими об'єктами критично важливої інформаційної і кіберінфраструктури, виникнення техногенних катастроф тощо. Це, у свою чергу, вимагає від керівництва нашої держави як розроблення національної стратегії кібернетичної безпеки, яка має чітко визначити мету, завдання та пріоритети такої діяльності, а також структури, відповідальні за реалізацію заходів щодо протидії сторонньому кібервпливу, так і формування в межах окремої цільової програми державної системи кібербезпеки, варіант структурно-функціональної моделі формування якої поданий на рис. 2:

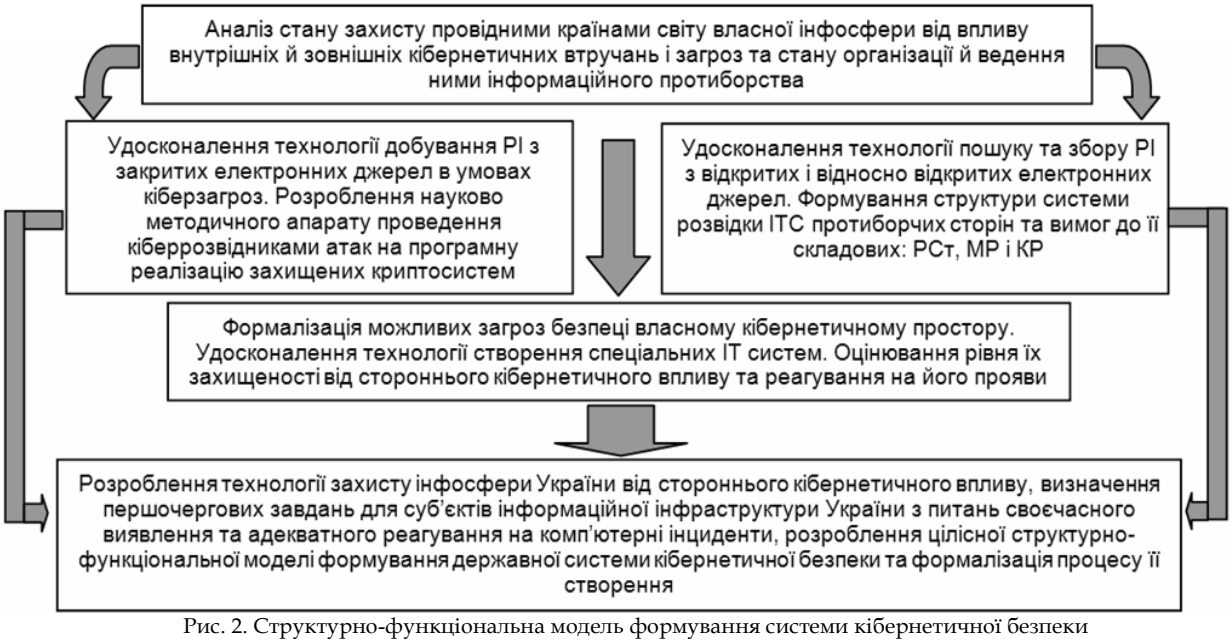

Рис. 2. Структурно-функціональна модель формування системи кібернетичної безпеки

Враховуючи досвід іноземних країн та особливості українських реалій, розв'язання основних завдань кібербезпеки неможливе без створення [1, 2]:

1. Міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки;

2. Центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення та оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розробки концептуальних засад та надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін та впливу на їх ІТС;

3. Органів власної інформаційної і кібербезпеки державних установ (відомств) та комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів.

Кібербезпека критичних авіаційних інформаційних систем

Не є виключенням і галузь цивільної авіації, на суб'єктах якої (повітряні судна, авіакомпанії, аеропорти тощо) циркулює значна кількість *державних інформаційних ресурсів* [5, 6]. Умови функціонування цивільної авіації швидко і суттєво змінюються із впровадженням сучасних технологій обробки, передачі та збереження інформації, що забезпечують підвищення рівня захисту і спрощення формальностей. Найбільшого захисту потребують ресурси *критичних авіаційних інформаційних систем (КАІС),* до яких, серед іншого, відносять [7]: системи контролю доступу та охоронної сигналізації; системи контролю вильоту; системи організації повітряного руху; системи дистанційного технічного обслуговування; системи бронювання та реєстрації пасажирів; диспетчерські системи тощо. Основними нормативними документами, що регламентують процеси захисту цивільної авіації від кіберзагроз є [**7-9**], проте у жодному з них *не визначено вичерпний перелік КАІС,* що значно ускладнює аналіз їх уразливостей і унеможливлює організацію ефективної комплексної системи інформаційної безпеки.

Під типовою *авіаційною інформаційною системою* необхідно розуміти сукупність взаємопов'язаних компонентів, що являють собою інформаційні, кадрові та матеріальні ресурси, процеси і технології, які забезпечують ефективне збирання, обробку, перетворення, збереження та передавання інформації в галузі авіації. Згідно ж [9] *КАІС* – це набір інформаційних ресурсів, організованих з метою збирання, обробки, використання, передачі та поширення доступної інформації, яка має відношення до усіх важливих аспектів безпеки авіаційної діяльності. Варто зауважити, що визначення КАІС міститься лише в одному нормативному документі (як уже зазначалось – це документ регіонального рівня [9]), а чіткі критерії віднесення тих чи інших авіаційних інформаційних систем до КАІС не визначені.

Іншою серйозною проблемою у цій галузі є *відсутність чітко визначеного понятійного апарату,* що ґрунтується, для прикладу, на загальноприйнятих міжнародних [10], регіональних чи галузевих стандартах (наприклад, поняття «кіберзагроза» зустрічається у кожному із зазначених документів [7-9], але його визначення чи посилання на інші нормативні документи є відсутніми).

Контрзаходи

Серед *реалізованих контрзаходів* світової спільноти для протидії кіберзагрозам та кібертероризму варто виділити такі:

– 2009 рік – введення в США посади Національного радника щодо кібербезпеки;

– 2011 рік – заснування у Великобританії Міжнародного альянсу забезпечення кібербезпеки;

– 2009-2013 роки – створення загонів кібервійськ у КНР, США, Росії (початок створення аналогічних загонів в Україні), організація агентств кібероборони у Австрії (APCIP), Великобританії (CPNI), Німеччині (NCAZ), Швейцарії (MELANI) та Нідерландах (NICC), а також включення вимог щодо забезпечення кібербезпеки у ключові нормативні документи критично важливих галузей народного господарства (до яких безсумнівно відноситься галузь цивільної авіації).

Згідно з європейською політикою [9] заходи щодо забезпечення кібербезпеки мають бути включеними в Національні програми безпеки цивільної авіації, контролю якості, навчання й підготовки з питань безпеки цивільної авіації, а перелік необхідних заходів обмежується оцінкою загроз, розділенням мереж, підготовкою персоналу та управлінням інцидентами. Варто відзначити, що найповніший перелік заходів, яких необхідно вжити для мінімізації впливу кіберзагроз на ресурси КАІС. міститься у 8-й редакції керівництва [7]. Серед таких заходів найбільш вагомими є:

– *адміністративні* (стандарти, процедури та політики безпеки, аналіз загроз та оцінка ризиків, відбір та підготовка персоналу та ін.);

– *віртуальні (логічні) засоби контролю* (IDS-системи, антивірусний захист, шифрування та захист мережевих сервісів);

– *фізичні засоби контролю* (аутентифікація, контроль та управління доступом, резервне копіювання тощо).

Висновки

Для вирішення зазначених проблем необхідно, перш за все, на базі відповідних наукових досліджень розробити *єдиний понятійний апарат,* створити *вичерпний перелік КАІС* і сформулювати *практичні рекомендації щодо впровадження кожного із вказаних заходів.* Що ж стосується більш глобального (державного) рівня, то необхідно на суб'єктах цивільної авіації створити ефективні *спеціалізовані підрозділи кібербезпеки* і приділити увагу *багаторівневій системі підготовки*

фахівців у галузі забезпечення захисту цивільної авіації від кіберзагроз.

Література

[1] Бурячок В.Л. Кібернетична безпека — головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спеціальна техніка. — 2011. — № 3 (26). — С. 104-114.

[2] Бурячок В.Л., Бурячок Л.В., Угрімов В.В. Кібернетична безпека: характерні ознаки, існуючі поняття і визначення. стан питання в ГУР МО України, на державному рівні та у світі // Вісник воєнної розвідки. — 2013. (подано до друку).

[3] Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі // Наука і оборона. — 2011. — № 3. — С. 35-42.

[4] Бурячок В.Л., Корченко О.Г., Хорошко В.О., Кудінов В.А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу // Захист інформації. — 2013. — Том 15, № 1. — С. 5-12.

[5] Марущак А.І. Щодо поняття «інформаційні ресурси держави» / А.І. Марущак // Інформаційна безпека людини, суспільства, держави. — 2009. — №1 (1). — С. 11-15.

[6] Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. — К. : ВБ «Аванпост-Прим». — 2012. — С. 31.

[7] Doc 8973 ICAO «Керівництво з авіаційної безпеки» (Restricted). — Вид. 8. – 2011. – 748 с.

[8] Додаток 17 до Конвенції про міжнародну цивільну авіацію «Безпека. Захист міжнародної цивільної авіації від актів незаконного втручання». — Вид. 9. — 2011. — 60 с.

[9] Doc 30 «Політика ЄКЦА у сфері авіаційної безпеки» (Restricted). — Вид. 13. — 2010. — 138 с.

[10] ISO/IEC 27032, Information technology — Security techniques — Guidelines for cybersecuritv. — 2012. — 50 с.

УДК 004.056.5:343.326 (045)

Корченко А.Г., Бурячок В.Л., Гнатюк С.А. Кибернетическая безопасность государства: характерные признаки и проблемные аспекты

Аннотация. *В последнее время довольно остро стоит проблема защиты кибернетического пространства государства. Особую важность эта проблема приобретает в отраслях, где циркулирует большое количество критической информации (например, отрасль гражданской авиации). В связи с этим, в этой работе определены характерные признаки кибербезопасности государства, а также проведен анализ проблем кибернетической безопасности Украины. Кроме того, приведены актуальные проблемы кибербезопасности в области гражданской авиации и возможные пути их решения . Также сформулированы практические рекомендации по обеспечению кибернетической безопасности как гражданской авиации, так и всего кибернетического пространства Украины.*

Ключевые слова: *кибернетическое пространство, кибербезопасность, киберинфраструктура, кибернетический влияние, гражданская авиация, критическая авиационная информационная система, контрмеры.*

Korchenko O.G., Buryachok V.L., Gnatyuk S.O. Cybernetic security of the state: characteristic features & problem aspects

Abstract. *Recently the problem of cybernetic space of the state security arises sufficiently acute. This problem is particularly important in areas where a large quantity of critical information is circulating (e.g. in civil aviation). In this context in the paper the characteristic features of the state cybersecurity were defined and the problems of cybernetic security of Ukraine were analyzed. In addition, the actual problems of civil aviation cybersecurity and their possible solutions were given. The practical recommendation to provide cybernetic security of civil aviation and whole cyberspace of Ukraine were also formulated.*

Key words: *cybernetic space, cybersecurity, cyberinfrastructure, cybernetic influence, civil aviation, critical aviation information system, countermeasures.*

Отримано *24 січня 2013 року*, затверджено редколегією *4 березня 2013 року*