TECHNICAL SCIENCES

ПРОПОЗИЦІЇ ЩОДО ОБҐРУНТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ДЕРЖАВИ

Кучеренко Ю.Ф.
кандидат технічних наук
Александров О.В.
кандидат технічних наук старший науковий співробітник
Власік С.М.
кандидат технічних наук старший науковий співробітник
Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків
Куліш Р.В.
ВАТ «Метінвестхолдінг», Маріуполь
Келлєр І.К.
Льотна академія Національного авіаційного університету, Кропивницький, Україна

PROPOSALS REGARDING THE JUSTIFICATION OF THE INFORMATION PROTECTION SYSTEM OF CRITICALLY IMPORTANT STATE FACILITIES

Kucherenko Yu.
PhD, orcid.org/0000-0001-9937-371X
Aleksandrov O.
PhD, Senior Research, orcid.org/0000-0001-6405-9456
Vlasik S.
PhD, Senior Research, orcid.org/0000-0002-4121-5572
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
Kulish R.
orcid.org/0000-0002-5590-1370
Metinvestholding LTD,Mariupol, Ukraine
Kellier I.
orcid.org/0000-0003-4915-0678
Flight Academy of the National Aviation University, Kropyvnytskyi, Ukraine

Анотація

У роботі запропоновані пропозиції щодо розвитку теоретичних і практичних основ забезпечення циркуляції інформації в інформаційному просторі держави при впливі потенційного противника та при відкритій агресії з метою забезпечення інформаційної безпеки держави. Наведено результати аналізу зовнішніх і внутрішніх факторів впливу на інформацію, яка циркулює при функціонуванні критично важливих об'єктів держави в сучасних умовах протиборства в інформаційній сфері. Визначено основні вимоги до систем захисту інформації критично важливих об'єктів держави, наведено джерела загроз для інформації та визначено основні канали витоку інформації. Результати роботи пропонується використовувати при розробці концепції та програми створення системи захисту інформації критично важливих об'єктів держави.

Abstract

The paper offers proposals for the development of theoretical and practical foundations for ensuring the circulation of information in the information space of the state under the influence of a potential enemy and in the event of open aggression in order to ensure the information security of the state. The results of the analysis of external and internal factors influencing the information that circulates during the functioning of critically important objects of the state in the modern conditions of confrontation in the information sphere are given. The main requirements for the information protection systems of critical state objects are defined, the sources of threats to information are given, and the main channels of information leakage are defined. The results of the work are proposed to be used in the development of the concept and program for the creation of a system of information protection of critical state objects.

Ключові слова: агресія, адаптація, захист, інформація, інформаційна сфера, система захисту, критично важливий об'єкт.

Keywords: aggression, adaptation, protection, information, information sphere, protection system, critical object.

Вступ

Постановка проблеми. В умовах впливу потенційного противника та при відритій агресії з боку противника виникає задача забезпечення захисту інформації, яка циркулює в критично важливих об'єктах держави. До критично важливих об'єктів України відносять об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. До захисту критичної інфраструктури відносять всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення та реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання та нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків уразі їх реалізації

Сьогодні, за досвідом сучасних збройних конфліктів, у тому числі на території України, головними завданнями є не тільки ефективна боротьба з ворогом на полі бою, але й забезпечення інформаційної безпеки держави в умовах ведення противником інтенсивного інформаційного протиборства. Завдання протидії противнику в інформаційній сфері повинні забезпечувати надійне функціонування критично важливих об'єктів держави при виконанні покладених завдань за призначенням в умовах ведення бойових дій.

Таким чином, аналіз і удосконалення системи захисту інформації критично важливих об'єктів держави, як основної складової інформаційної безпеки, особливо під час ведення збройної боротьби, є актуальним завданням.

Аналіз літератури. В наведеній літературі [1-36] розглядаються питання щодо особливостей сучасних війн [1-15], в тому числі ведення гібридних та інформаційних війн [1, 3-5], інформаційної безпеки держави [6-9], військового управління [2, 10, 11], функціонування та розвитку критично важливих об'єктів держави, вирішення питань захисту інформації в них, розробки комплексної системи захисту інформації в інформаційних системах та таке інше [12-16]. У відомих роботах не достатньо уваги приділялося розробці адаптованої системи захисту інформації критично важливих об'єктів держави в умовах збройної боротьби.

Метою статті є розробка пропозицій щодо удосконалення системи захисту інформації критично важливих об'єктів держави в умовах інформаційного та збройного протиборства.

Основна частина

При протиборстві з потенційним противником до початку агресії у інформаційній сфері здійснюється інформаційне протистояння, яке має не менше значення за протистояння військ на полі бою. Складовими такого протиборства є висвітлення питань непорозуміння між державами для зосередження уваги мирової спільноти на своїх ключових позиціях. На прикладі збройної агресії проти України, причинами непорозуміння виступали територіальні та політичні мотиви, але у інформаційному просторі це представлено захистом «дружнього народу». З початком збройної агресії протиборство здійснюється не тільки на полі бою із застосуванням різноманітних зразків озброєння, але й у інформаційному просторі. Тому основними цілями при агресії є критично важливі об'єкти держави, які знищуються як фізично (із застосуванням зразків озброєння), так і у інформаційній сфері (засобами інформаційної боротьби).

Застосування сучасних засобів озброєння, які побудовані на основі інформаційно-телекумікаційних систем, забезпечить завоювання інформаційної переваги над противником. Збройні сили, які управляються за допомогою таких систем будуть мати більшу бойову міць за рахунок синхронізації своїх дій та максимальної адаптації їх під зміну обстановки в ході ведення бойових дій ніж ті, які не мають інформаційної складової, хоча мають навіть і більший бойовий потенціал. Це свідчить про те, що настала епоха ведення мережецентричних війн, однією з головних ознак яких є жорстке протиборство різних зразків озброєння та засобів (вогневих, інформаційних, нелетальної дії, психологічного впливу) між собою в єдиному командно-інформаційному просторі в зоні ведення бойових дій. Таким чином, можна констатувати, що в сучасних війнах ефективність застосування військ та озброєння буде визначатись мірою отримання відповідної інформаційної переваги над противником. Це дозволить здійснювати управління своїми військами та бойовими засобами за менші часові показники (терміни циклів управління) порівняно з противником і мати повну усвідомленість о власних діях. Отже, сучасні війни стали не тільки високотехнологічними, але й набули інформаційного характеру (в них відбувається жорстке протиборство у інформаційному просторі), бо вирішальним значенням при досягненні мети в них є не перевага у чисельності військ чи озброєнні, а вміння командирів (командування) синхронізовано застосовувати усі наявні сили та бойові засоби різних компонентів міжвидових угруповань у реальному масштабі часу за єдиним задумом командування. За таких умов надійне функціонування критично важливих об'єктів держави, особливо при веденні бойових дій, має одне з головних факторів щодо отримання перемоги над ворогом на полі бою.

Функціонування сучасних критично важливих об'єктів держави направлено на створення глобальної ситуаційної оцінки обстановки і знання про противника на відповідних рівнях управління для кожного елементу військ (сил), що територіально розподілені у зоні ведення бойових дій. Головною особливістю їх функціонування, як взаємопов'язаної сукупності програмно-технічних комплексів, засобів зв'язку, обміну даними і автоматизації, а також різних джерел інформації є формування єдиного командно-інформаційного простору, використання можливостей якого керівним складом дає

можливість використовувати у реальному масштабі часу три основні компоненти інформаційної сфери:

інформаційно-розвідувального (розвідувально-інформаційний компонент) характеру;

інформаційно-управлінського (компонент збору, обробки, оцінювання, зберігання та розподілу інформації між користувачами) характеру;

виконавчого (компонент військових підрозділів (формувань), їх особового складу, бойової техніки, систем летальної та не летальної зброї) характеру.

Оскільки функціонування критично важливих об'єктів держави пов'язано із перетворенням різних видів інформації (збором, обробкою, зберіганням, відображенням, передачею тощо), то можливо констатувати, що в основі їх функціонування та виконання завдань за призначенням знаходиться інформація. Це підтверджує той факт, що надійний захист інформації, яка циркулює в критично важливих об'єктах держави, є базою їх надійного функціонування.

Із аналізу можливих шляхів впливу на інформацію, що циркулює в критично важливих об'єктах держави, можливо виділити наступні її порушення, які можуть привести до збоїв у їх функціонуванні:

фізичної цілісності (знищення інформації в елементах системи);

логічної цілісності (порушення логічних зв'язків);

змісту (зміни інформаційних блоків, зовнішнє нав'язування хибної інформації);

конфіденційності (зміна ступеню захисту інформації);

прав власності на інформацію (несанкціоноване копіювання чи використання без дозволу) і таке інше.

На сучасному етапі розвитку критично важливих об'єктів держави, враховуючи умови в яких вони функціонують, для забезпечення адаптації системи захисту інформації в них необхідно приділити увагу вдосконаленню та впровадженню перспективних методів, механізмів та засобів забезпечення інформаційно-технічної безпеки функціонування даних систем, а саме:

вдосконаленню методів аналізу комп'ютерних програм на наявність вразливості та не декларованих можливостей;

вдосконаленню антивірусних технологій;

впровадженню перспективних методів та механізмів ідентифікації та аутентифікації користувачів із застосуванням електронних ключів і інших засобів їх розпізнавання;

забезпеченню екранування та фільтрації інформації (позбавлення від непотрібної та надлишкової інформації);

вдосконаленню методів логічного розмежування доступу користувачів до певної інформації;

вдосконаленню засобів моніторингу стану функціонування елементів інформаційної сфери з метою вияву аномальних ситуацій при їх функціонуванні;

впровадженню нових методів шифрування та дешифрування інформації;

впровадженню перспективних засобів перевірки цілісності інформації на носіях і таке інше.

Інтегроване застосування перспективних методів, механізмів та засобів забезпечення інформаційно-технічної безпеки функціонування даних систем повинні формуватися у адаптовану систему захисту інформації певного критично важливого об'єкту держави у відповідності до конкретних загроз, що впливають на їх функціонування, у зв'язку із порушенням циркуляції інформації в даних системах або порушенням самої інформації.

Із системних позицій під джерелом загроз, стосовно їх впливу на інформацію в критично важливих об'єктах держави пропонується виділити наступні групи: люди; технічні засоби; моделі, алгоритми, програми; зовнішнє довкілля (атмосферні умови, вплив вогневих та інформаційних засобів противника та таке інше).

Тому, при розробці або обґрунтуванні системи захисту інформації критично важливих об'єктів держави необхідно визначити та сформувати повний перелік загроз інформації в даній системі. Крім того, обов'язково необхідно врахувати можливість адаптації системи захисту інформації критично важливих об'єктів держави до виникнення нових загроз, які не були враховані раніше. Це пов'язано з тим, що існування неврахованої загрози може в значній мірі знизити ефективність захисту інформації в системі, тобто знизити її надійність функціонування.

Система захисту інформації критично важливих об'єктів держави повинна розв'язувати наступні функціональні завдання щодо забезпечення інформаційної безпеки:

забезпечення захисту критично важливих об'єктів держави від виявлення її функціонування (особливо систем управління, командних пунктів тощо);

забезпечення захисту інформації, що циркулює в критично важливих об'єктах держави;

забезпечення захисту критично важливих об'єктів держави від інформаційного впливу.

Оскільки система захисту інформації представляє взаємопов'язану сукупність засобів, методів і заходів, які направлені на запобігання знищення, зміну змісту, несанкціонованого отримання та використання інформації, що циркулює в критично важливих об'єктів держави, то функціонально її можливо представити наступними підсистемами: організаційною; технічною (інженерно-технічною); програмно-апаратною.

Організаційна підсистема є сукупністю взаємопов'язаних заходів і вимог, які направлені на організацію роботи з користувачами відповідних критично важливих об'єктів держави (організацію систем фізичного захисту, визначення відповідальності персоналу за виконання заходів захисту, організації контролю виконання політики безпеки при функціонуванні системи, встановлення переліку та змісту заходів захисту і таке інше) з дотримання

ними вимог щодо захисту інформації в даній системі [10, 12, 35].

Технічна підсистема (інженерно-технічна) – це сукупність певних заходів, що направлені на зниження загроз, які обумовлені зовнішніми факторами впливу на функціонування критично важливих об'єктів держави (стихійні лиха, техногенні явища, засоби вогневого ураження, інформаційні засоби та інші). Вона забезпечує необхідний рівень живучості системи захисту інформації критично важливих об'єктів держави в частині впливу інформаційних та інших засобів на її функціонування та забезпечує усунення дії певних загроз щодо безпеки інформації, що циркулює в системі, за рахунок застосування різних інженерно-технічних засобів (рішень) захисту інформації та контролю безпекової обстановки (навколишньої безпекової зони тощо).

Програмно-апаратна підсистема як сукупність функціонуючих програмних і апаратних засобів та методів (алгоритмів, програм) забезпечує захист від загроз, що пов'язані з процесом збору, обробки, зберіганням, пошуком, відображенням, передачею інформації в системі між її користувачами [11, 19].

Необхідно зазначити, що рівень безпеки та надійності системи захисту інформації критично важливих об'єктів держави буде не тільки залежати від засобів і заходів, що обрані для захисту інформації та загальної політики безпеки в системі але, на наш погляд, і від якості інтегрованого застосування цих заходів, засобів і методів для реалізації цільового ефекту у системі відповідного об'єкту.

Отже, вибір стратегії захисту інформації критично важливих об'єктів держави в загальному вигляді є пошуком компромісу між необхідним ступенем захисту інформації у відповідному об'єкті та потрібним для реалізації цих цілей ресурсами. Необхідність захисту інформації в критично важливих об'єктів держави визначається важливістю об'єкта, об'ємами інформації, а також умовами її зберігання, обробки та використання. Об'єм ресурсів для захисту такої інформації визначається умовою обов'язкового досягнення потрібного рівня безпеки циркуляції інформації.

Таким чином, система захисту інформації певного критично важливого об'єкта держави повинна представляти собою сукупність всіх засобів, методів і заходів, необхідних для реалізації визначених задач щодо захисту інформації в об'єкті, відповідати основним принципам їх створення та бути адаптованою до зміни відповідних внутрішніх та зовнішніх загроз, які впливають на інформацію, що циркулює під час функціонування об'єкта.

Висновки

Сучасна система захисту інформації критично важливих об'єктів держави повинна представляти собою сукупність всіх засобів, методів та заходів, необхідних для реалізації визначених завдань щодо захисту інформації в системі, відповідати основним принципам їх створення, включати в себе організаційну, технічну (інженерно-технічну) і програмно-апаратну функціональні підсистеми та буди адаптованою до зміни відповідних внутрішніх та зовнішніх загроз, які впливають на інформацію, що циркулює під час функціонування об'єкта.

Розроблені пропозиції щодо створення системи захисту інформації критично важливих об'єктів держави пропонується використовувати при розробці вимог до перспективних засобів (заходів) та методів адаптивної системи захисту інформації критично важливих об'єктів держави з врахуванням їх функціонування в умовах ведення інформаційного протиборства в інформаційній сфері та збройної боротьби.

Список літератури

1. Владимиров А.И., Основы общей теории войны: монографія, Москва: Московский финансово-промышленный университет «Синергия», 2013, Книга 1, 832 с.

2. Сидорин А.Н., Прищепов В.М., Акуленко В.П., Вооруженные силы США в XXI веке: Военно-теоретический труд, Москва: Кучково поле, Военная книга, 2013, 800 с.

3. Кушнір О.І., Давикоза О.П., Кучеренко Ю.Ф. Аналіз впливу «гібридної» війни на розвиток автоматизованої системи управління авіацією та ППО Збройних Сил України, Наука і техніка Повітряних Сил Збройних Сил України, 2017, № 2 (27), с. 116-120, https://doi.org/10.30748/nitps.2017.27.22.

4. Савин Л.В. Сетецентрическая и сетевая война. Введение в концепцію, Москва: Евразийское движение, 2011, 130 с.

5. Кучеренко Ю.Ф., Носик А.М., Погляди щодо напрямів розвитку тактики дій формувань тактичного рівня при їх застосуванні в сучасних операціях (війнах), Наука і техніка Повітряних Сил Збройних Сил України, 2015, № 2 (19), с. 24-26.

6. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А., Кибервойны – реальная угроза национальной безопасности? Москва: КРАСАНД, 2011, 96 с.

7. Сидорин А.Н., Рябченко И.А., Герасимов В.П., Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств: Информационно-аналитический сборник, Москва: Воениздат, 2011. 344 с.

8. Основы теории применения управления в системах специального назначения, за ред. Ю.В. Бородакия, В.В. Масановца, Москва: Управление делами президента РФ, 2008, 400 с.

9. Демідов Б.О., Величко О.Ф., Кучеренко Ю.Ф., Концептуальні положення щодо створення автоматизованої системи управління протиповітряною обороною держави, Наука і оборона, 2014, №3, с. 51-56.

10. Макаров И.М., Лохин В.М., Манько С.В., Романов М.П., Искусственный интеллект и ителектуальные системы управления, Москва: Наука, 2006, 333 с.

11. Московитов Н., Рыбаков Г., Перспективы создания глобальной информационной сети МО США, Зарубежное военное обозрение, 2013, №7, с. 8-19.

12. Войтенко С.С., Герасимов С.В. Нормативні

та організаційні основи метрологічного забезпечення військ (сил), Харків: ХУПС, 2012, 292 с.

13. Демідов Б.О., Величко О.Ф., Кучеренко Ю.Ф., Куцак М.В., Управління проектами зі створення зразків озброєння та військової техніки в умовах прояву факторів невизначеності та ризику, Озброєння та військова техніка, Київ: ЦНДІ ОВТ ЗС України, 2016, №2 (10), с. 15-19.

14. Кучеренко Ю.Ф., Гордієнко В.М., Литвинов Ю.С., Метод оцінювання ефективності автоматизованої системи військового призначення за станом її складових основ, Системи управління, навігації та зв'язку, 2012, № 2 (22), с. 141-143.

15. Кучеренко Ю.Ф. Методика оцінки загального стану автоматизованої системи військового призначення на основі визначення технічного стану комплексів засобів автоматизації, що її складають, Системи обробки інформації, 2017, №3 (149), с. 118-120, https://doi.org/10.30748/soi.2017.149.23.

16. Герасимов С.В., Модель оцінки похибки обробки інформації у навігаційних системах крилатих ракет в умовах невизначеності, Наука і техніка Повітряних Сил Збройних Сил України, 2019, № 2 (35), с. 151-157, https://doi.org/10.30748/nitps.2019.35.19.

17. Чинков В.Н, Герасимов С.В., Комплексная методика оптимизации контролируемых параметров сложных технических объектов, Украинский метрологический журнал, 2003, № 1, с. 11-15.

18. Кучеренко Ю.Ф., Методологічні аспекти проектування матеріально-технічної основи автоматизованої системи військового призначення, Системи озброєння і військова техніка, 2018, № 2 (54), с. 94-98, https//doi.org/10.30748/soivt.2018.54.13.

19. Herasimov S., Tymochko O., Kolomiitsev O., Formation Analysis Of Multi-Frequency Signals Of Laser Information Measuring System, EUREKA: Physics and Engineering, 2019, Number 5, p.p. 19-28, https//doi.org/10.21303/2461-4262.2019.00984.

20. Васильев В.И., Ильясов Б.Г., Интеллектуальные системы управления, Теория и практика, Москва: Радиоэлектроника, 2009, 392 с.

21. Борисенко М.В., Герасимов С.В., Костенко О.І., Макарчук Д.В., Development of optimum navigation information processing algorithm, Наука і техніка Повітряних Сил Збройних Сил України, 2018, № 3(32), с. 38-44, https//doi.org/10.30748/nitps.2018.32.06.

22. Войтенко С.С., Герасимов С.В., Особливості метрологічного забезпечення озброєння і військової техніки у локальних війнах останніх десятиріч, Системи озброєння та військової техніки, № 1 (13), с. 42-46.

23. Фадеев А.С. & Ничипор В.И., Военные конфликты современности, перспективы развития способов их ведения, Прямые и непрямые действия в вооруженных конфликтах XXI века, Военная мысль, 2019, адрес доступа: https://vm.ric.mil.ru/Stati/item/222832.

24. Herasimov S., Pavlenko M. Roshchupkin E., Aircraft flight route search method with the use of cellular automata. International Journal of Advanced Trends in Computer Science and Engineering, 2020, 9 (4), p. 5077-5082, https://doi.org/10.30534/ijatcse/2020/129942020.

25. Худов Г.В., Таран І.А., Методика синтезу раціональної структури підсистеми розвідки системи протиповітряної оборони з використанням генетичного алгоритму, Наука і техніка Повітряних Сил Збройних Сил України, 2016, № 2 (23), с. 25-31.

26. Zhuravlev O., Kolomiytsev O., Herasimov S., Method for determining coefficient power error of front resistance missile by means station outwardly trajectory measurements, Зб. наук. пр. Харківського національного університету Повітряних Сил, 2017, вип. 3 (52), с. 72-76.

27. Войтенко С.С., Герасимов С.В., Куценко В.В., Напрями удосконалення системи контролю технічного стану зразків озброєння та військової техніки, Наука і техніка Повітряних Сил Збройних Сил України, 2016, № 3 (24), с. 127-131.

28. Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В.А. Кротюка, Харків: ФОП Федорко М.Ю., 2021, 558 с.

29. Асавалюк А.В., Герасимов С.В. & Рощупкін Є.С., Похибки визначення повного вектора швидкості в єдиній прямокутній системі координат системою оглядових станцій радіолокації з різною точністю, Системи озброєння і військова техніка, 2017, вип. 2 (50), с. 53-56.

30. Войтенко С.С., Волобуєв А.П., Герасимов С.В., Методика визначення складу та виробничих можливостей виїзної метрологічної групи, Наука і техніка Повітряних Сил Збройних Сил України, 2011, вип. 2 (6), с. 136-139.

31. Чинков В.М., Герасимов С.В., Варіаційний метод і методики синтезу оптимального вимірювального сигналу для контролю технічного стану системи автоматичного управління, Український метрологічний журнал, 2014, № 1, с. 59-64.

32. Герасимов С.В., Макарчук Д.В., Костенко О.І., Метод адаптивної обробки навігаційної інформації в умовах невизначеності, Системи обробки інформації, 2018, вип. 3 (154), с. 19-25, https://doi.org/10.30748/soi.2018.154.03.

33. Герасимов С.В., Рощупкін Є.С., Теоретические основы оценки ошибок значений сигналов с гармонически меняющимися параметрами, Озброєння та військова техніка, 2018, вип. 2 (18), с. 43-49.

34. Чинков В.М., Герасимов С.В., Дослідження та обґрунтування критеріїв оптимізації вимірювальних сигналів для контролю технічного стану систем автоматичного управління, Український метрологічний журнал, 2013, № 4, с. 43-47.

35. Kriukov O., Melnikov R., Bilenko O., Modeling of the process of the shot based on the numerical solution of the equations of internal ballistics, Applied physics. Eastern-European Journal of Enterprise Technologies, 2019, 1/5 (97), p.p. 40-46, https://doi.org/10.15587/1729-4061.2019.155357.

36. Herasimov S., Gridina V. Method justification nomenclature control parameters of radio systems and purpose of their permissible deviations, Information processing systems, 2018, № 2 (153), p.p. 159-164, https://doi.org/10.30748/soi.2018.153.20.