УДК 004:91

Олександр Анатолійович Чорнокнижний *(канд. техн. наук, доцент)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ОСНОВНІ ПІДХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

У процесі проектування і створення географічної інформаційної системи військового призначення необхідно визначити основні напрямки вирішення завдання щодо забезпечення безпеки функціонування такої системи. У статті проаналізовано основні положення щодо забезпечення безпеки функціонування геоінформаційної системи і система показників, що застосовуються для її оцінки.

Розглянуто основні напрями забезпечення захисту інформації, що циркулює в процесі функціонування географічної інформаційної системи і відповідні їм програмно-технічні засоби захисту інформації.

Ключові слова: *геоінформаційна система; безпека функціонування; захист інформації.*

Вступ

Постановка проблеми. Як відомо, якість геоінформаційної системи – це сукупність її властивостей, що обумовлюють можливість використання системи для задоволення певних відповідно до її призначення потреб. Кількісні характеристики цих властивостей визначаються показниками. Основними показниками якості інформаційних систем є надійність, достовірність, безпека [1].

Безпека геоінформаційної системи – властивість, що полягає у здатності системи забезпечити конфіденційність та цілісність інформації, а саме захистити інформацію, яка циркулює в системі, від несанкціонованого доступу, спрямованого на її розкриття, зміну або руйнування.

Аналіз останніх досліджень і публікацій. Проаналізуємо основні теоретичні положення щодо безпеки геоінформаційної системи. Інформаційну безпеку часто вказують серед основних інформаційних проблем XXI століття. Дійсно, розкрадання інформації, її свідоме викривлення і знищення дуже часто призводять до трагічних для постраждалої сторони наслідків, які можуть призвести до руйнування фізичних об’єктів, структур, до людських жертв, нарешті. Як приклад, можна згадати світову трагедію, що призвела до жертв декількох тисяч людей – атаку терористів на Всесвітній торговий центр у Нью-Йорку і Міністерство оборони США у Вашингтоні. Подібний терористичний акт був би неможливий, якби терористи не вивели попередньо з ладу комп'ютерну систему управління безпекою.

За розрахунками міжнародних експертів світовий річний збиток від несанкціонованого доступу до інформації становить зараз приблизно 0,5 млрд. доларів і щорічно збільшується в 1,5 рази, а збиток, нанесений, поширенням по електронній пошті самого “ефективного” комп’ютерного вірусу “I love you” в 1999 році, перевищив 10 млрд. доларів. Перелік тяжких наслідків від порушення безпеки інформації можна було б продовжувати нескінченно (якщо раніше для успішного здійснення революції або державного перевороту важливо було захопити пошту і телеграф, то тепер необхідно паралізувати існуючи системи комп'ютерних телекомунікацій).

Питанням інформаційної безпеки взагалі сьогодні приділяється величезна увага, існують безліч публікацій по даній тематиці, які присвячені різним аспектам і прикладним питанням захисту інформації. На міжнародному і державному рівнях прийнята безліч законів по забезпеченню безпеки інформації.

Метою статті є проаналізувати основні положення щодо безпеки функціонування геоінформаційної системи та на їх основі встановити систему показників для її оцінки та визначити основні напрями забезпечення безпеки функціонування ГІС.

Виклад основного матеріалу дослідження

Світовий досвід використання мереж загального і корпоративного користування показує, що інформаційним ресурсам у цих мережах можуть загрожувати [2,3]:

приведення мережі у непрацездатний стан в результаті зловмисних або необережних дій, наприклад, шляхом перевантаження мережі пошуку інформацією;

несанкціонований доступ до конфіденційних даних як ззовні, так і зсередини мережі, їх використання та розголошення з корисною метою;

цілеспрямоване викривлення, фальсифікація або підміна даних при несанкціонованому доступі;

підміна та викривлення інформації, наданої для вільного доступу (наприклад web-сторінок), що призводить до неможливості використання інформаційних ресурсів у випадку їх зараження вірусами по каналах мережі Інтернет, електронній пошті або за допомогою інфікованих зовнішніх

носіїв (змінних дисків, CD і DVD–дисків) тощо.

Усі загрози геоінформаційним системам можна об'єднати в три узагальнюючі групи [2]:

Погроза розкриття – можливість того, що інформація стане відомою тому, кому не варто було б її знати.

Погроза цілісності – навмисна несанкціонована зміна (модифікація або видалення) даних, що зберігаються в обчислювальній системі або переданих з однієї системи в іншу.

Погроза відмови в обслуговуванні – небезпека появи блокування доступу до деякого ресурсу обчислювальної системи.

Засоби забезпечення інформаційної безпеки залежно від способу її реалізації можна розділити на наступні класи методів [2,3]: організаційні, технологічні, апаратні та програмні методи.

Організаційні методи реалізуються шляхом раціонального конфігурування, організації та адміністрування системи. У першу чергу це стосується мережних інформаційних систем, операційних систем, повноважень мережевого адміністратора, набору обов'язкових інструкцій, що визначають порядок доступу та роботи в мережі.

Технологічні методи включають у себе наступні технології: виконання мережевого адміністрування; моніторингу та аналізу безпеки інформаційних ресурсів; ведення електронних журналів реєстрації користувачів; фільтрації і антивірусної обробки вихідної інформації.

Апаратні методи, у свою чергу, реалізують фізичний захист системи від несанкціонованого доступу, апаратні функції ідентифікації периферійних терміналів системи та користувачів, режими підключення мережних компонентів тощо.

Що стосується програмних методів, то сьогодні це найпоширеніші методи захисту інформації (наприклад, програми ідентифікації користувачів, парольного захисту, перевірки повноважень, криптопротоколи тощо). Без використання програмної складової практично нездійсненні ніякі, у тому числі і розглянуті перші три групи методів. В той же час необхідно враховувати, що сьогодні самостійно організаційні, технологічні та апаратні методи захисту, як правило, реалізовані бути не можуть – усі вони містять програмний компонент.

Аналізуючи існуючий сьогодні досвід забезпечення інформаційної безпеки можна зробити висновок, що найбільшу увагу з боку розробників та користувачів геоінформаційних систем викликають наступні три напрямки реалізації захисту інформації та відповідні їм програмно–технічні засоби захисту [4].

Перший напрямок передбачає захист від несанкціонованого доступу інформаційних ресурсів автономно працюючих і мережевих комп'ютерів. Найбільш гострою ця проблема є для серверів і користувачів мережі Інтернет та Інтранет–мереж. Така функція реалізується багаточисельними програмними, програмно–апаратними та апаратними засобами.

Другий напрямок реалізується шляхом захисту секретної, конфіденційної та особистої інформації від несанкціонованого перегляду сторонніми особами та цілеспрямованого її викривлення. Дана функція забезпечується як засобами захисту від несанкціонованого доступу, так і за допомогою криптографічних засобів, які традиційно становлять окремий клас засобів захисту інформації.

Третій напрямок полягає у захисті геоінформаційних систем від численних комп'ютерних вірусів, здатних не тільки зруйнувати інформацію, але іноді і вивести з ладу окремі технічні компоненти системи, наприклад такі, як BIOS.

Активно розвиваються також засоби захисту від витоку інформації по мережах живлення, каналам електромагнітного випромінювання комп'ютера або монітора. Для цього реалізуються наступні варіанти захисту: екранування приміщень; використання генераторів шумових випромінювань; спеціальний відбір моніторів і комплектуючих комп'ютера, які володіють найменшим випромінюванням; використання засобів захисту від електронних "жучків", що встановлюються безпосередньо в комплектуючі комп'ютера тощо.

Захист від несанкціонованого доступу до ресурсів комп'ютера – це комплексна проблема, що передбачає вирішення комплексу наступних питань:

присвоєння користувачу, а рівно і терміналам, програмам, файлам та каналам зв'язку унікальних імен і кодів (ідентифікаторів);

виконання процедур ідентифікації користувачів в процесі доступу до інформаційної системи або обміну інформацією за запитом. Для цього повинна автоматично здійснюватися перевірка того, що особа або пристрій, який повідомив свій ідентифікатор, у дійсності йому відповідає. Сьогодні на практиці ідентифікація програм, терміналів і користувачів в процесі доступу до системи найчастіше виконується шляхом перевірки паролів, рідше – зверненням до спеціальної служби, яка здійснює та контролює сертифікацію користувачів.

перевірку повноважень, тобто перевірку права користувача на доступ до системи або запиту даних (на виконання над даними певних операцій – читання, оновлення), з метою розмежування прав доступу до мережних і комп'ютерних ресурсів;

автоматичну реєстрацію в спеціальному журналі всіх як виконаних, так і відмовлених запитів до інформаційних ресурсів із вказівкою ідентифікатора користувача, термінала, часу та сутності запиту, тобто ведення журналів контролю, які дозволяють визначити, через який хост–комп'ютер діяв несанкціонований користувач (хакер), а іноді і визначити його IP–адрес та точне місце розташування.

Сьогодні у випадку реалізації найвищого ступеня захисту вже використовуються і екзотичні апаратно–програмні системи біометричної ідентифікації користувачів (миші та клавіатури з функцією дактилоскопічної ідентифікації, системи розпізнавання користувача по голосу, по відеозображенню, у тому числі по сітківці та райдужній оболонці ока тощо.

Для кількісної оцінки параметрів існуючих систем захисту інформації розроблені певні рекомендації. Так, у керівних документах Держтехкомісії Росії "Автоматизовані системи. Захист від несанкціонованого доступу до інформації. Класифікація автоматизованих систем і вимоги до захисту інформації" та "Засоби обчислювальної техніки. Захист від несанкціонованого доступу до інформації. Показники захищеності від несанкціонованого доступу до інформації" рекомендовано для оцінки захисту інформації від несанкціонованого доступу використовувати наступні показники:

P_a – імовірність вручення інформації абоненту, якому вона не призначена;

P_c – імовірність не проходження сигналу тривоги.

При оптимізації систем захисту інформації використовуються замість ймовірностей P_a та P_c коефіцієнти K_a – умовна імовірність вручення інформації абоненту, якому вона не призначена за умови виникнення несанкціонованого доступу та K_c – умовна імовірність не проходження сигналу тривоги за умови виникнення несанкціонованого доступу до інформації:

$$K_a = P_a / P_{нд} \quad \text{та} \quad K_c = P_c / P_{нд},$$

де $P_{нд}$ – імовірність появи несанкціонованого доступу.

У цих же керівних документах пропонується визначити п'ять класів конфіденційності інформації. Для кожного класу рекомендовані відповідні значення показників конфіденційності інформації, які наведені у табл. 1.

Таблиця 1

Характеристика класів конфіденційності інформації

Клас конфіденційності інформації	**1**	**2**	**3**	**4**	**5**
Ра	10^{-5}	10^{-4}	10^{-3}	10^{-2}	-
Рс	10^{-5}	10^{-4}	10^{-3}	10^{-2}	-

Висновки й перспективи подальших досліджень

На підставі вище розглянутих положень можна зробити наступні висновки.

Безпека та захист інформації в геоінформаційній системі військового призначення має будуватися з урахуванням комплексного підходу до побудови системи захисту, який передбачає об'єднання в єдиний комплекс розглянутих заходів та засобів захисту інформації на всіх рівнях системи.

Система інформаційної безпеки в ГІС повинна базуватися на положеннях Закону України "Про захист інформації в автоматизованих системах", "Положенні про технічний захист інформації в Україні" (постанова КМ України №632 від 09.09.94) та вимогах ДСТУ 3396.0-96.

Система захисту інформації має бути спрямована на запобігання втрати інформації, її спотворення, несанкціонованого доступу та незаконного використання на етапах проектування, впровадження та експлуатації геоінформаційної системи [4].

Безпека інформації забезпечується на технологічних етапах створення, оновлення, накопичення, зберігання, обробки та передачі інформації. Відповідальність за безпеку інформації на відповідних технологічних етапах функціонування ГІС несуть підрозділи, які їх здійснюють.

З метою виконання функцій щодо захисту інформації, яка циркулює в геоінформаційній системі військового призначення, на всіх її рівнях створюються відповідні підрозділи або призначаються відповідальні посадові особи, що у своїй діяльності керуються відповідними наказами та інструкціями.

Нормативними документами при створенні ГІС, її підсистем та окремих елементів повинен бути передбачений перелік заходів захисту інформації.

Захист інформації у геоінформаційній системі, у тому числі від несанкціонованого доступу, здійснюється комплексним використанням заходів організаційного, методичного, правового, кадрового, технічного, програмного та математичного характеру відповідно до діючих нормативних документів. Вибір конкретного комплексу методів здійснюється, виходячи з установленого порядку функціонування, потрібного рівня та терміну захисту інформації та наявних можливостей щодо реалізації різних заходів захисту інформації в процесі функціонування геоінформаційної системи.

Контроль стану підсистем та окремих елементів ГІС, комплексів захисту інформації забезпечується використанням комплексів діагностичних програмних засобів, які здійснюють автоматизовану перевірку їх технічного стану (як в цілому, так і окремих елементів) під час контролю функціонування як до початку, так і в ході роботи системи.

Література

1. Тарасов В. М., Чорнокнижний О. А. Система показників ефективності побудови геоінформаційної системи Збройних Сил України // Сучасні інформаційні технології у сфері безпеки та оборони. – 2012. – №1(13). – С. 94 – 96. **2. Афоничкин А. И.,** Панфилов С. И. Качество информационного обеспечения в процессах управления / под. ред. А.А. Денисова. – Саранск: Изд-во Саранского университета, 1988. 176 с. **3. Теоретичні основи** автоматизації процесів вироблення рішень в системах управління Повітряних Сил / О. В. Александров, Д. Е. Двухглавов, М. А Павленко та ін. – Х. : ХУПС. 2010. – 172 с. **4. Географічні інформаційні** системи / Мосов С. П., Тарасов В. М., Чорнокнижний О.А. та інш. – Київ: НАО України, 2006. – 237 с.

ОСНОВНЫЕ ПОДХОДЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО ПРЕДНАЗНАЧЕНИЯ

***Александр Анатольевич Чернокнижный** (канд. техн. наук, доцент)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В процессе проектирования и создания географической информационной системы военного назначения необходимо определить основные направления решения задачи по обеспечению безопасности функционирования такой системы. В статье проанализированы основные положения по обеспечению безопасности функционирования геоинформационной системы и система показателей, применяемых для ее оценки.

Рассмотрены основные направления обеспечения защиты информации, циркулирующей в процессе функционирования географической информационной системы и соответствующие им программно-технические средства защиты информации.

***Ключевые слова:** геоинформационная система; безопасность функционирования; защита информации.*

GENERAL APPROACHES TO THE SAFETY OF MILITARY GEOGRAPHIC INFORMATION SYSTEMS

***Oleksandr A. Chornoknyzhnyi** (Candidate of Technical Sciences, Associate Professor)*

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

In the course of design and creation of military geographical information system it is necessary to define the main directions of the task solution of safety approaches of such system functioning. In the article the main safety approaches of geographic information system functioning and the indicators system are applied for its assessment were analyzed.

The main directions of ensuring information security, circulating in the course of functioning geographical information system and information security program technical means related to directions are considered.

***Keywords:** geographic information system; safety of functioning; information security.*

References

1. Tarasov V. M., Chornoknyzhnyi O. A. (2012), The system performance of construction geographic information system of the Armed Forces Ukraine. [*Systema pokaznykiv efektyvnosti pobudovy heoinformatsiinoi systemy Zbroinykh Syl Ukrainy*], Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, vol. 1(13), pp. 94–96. **2. Afonychkyn A. Y.,** Panfylov S. Y. (1988), The quality of information support in the management processes, [*The quality of information support in the management processes*], under. Ed. A. A. Denisova, Saransk, Izd-vo Saranskoho unyversyteta,. 176 p. **3. Aleksandrov O. V.,** Dvukhhlavov D. E., Pavlenko M. A. Theoretical Foundations of automated the decision making process in the systems of Air Force (2010), [*Teoretychni osnovy avtomatyzatsii protsesiv vyroblennia rishen v systemakh upravlinnia Povitrianykh Syl*], Kharkiv, KhUPS, 172 p. **4. Mosov S. P.**, Tarasov V. M., Chornoknyzhnyi O. A. (2006), Geographic Information Systems [*Heohrafichni informatsiini systemy*], Kyiv, NAO Ukrainy, 237 p.

Отримано: 05.03.2015 року