

СКАНУВАННЯ НА ПРЕДМЕТ ВРАЗЛИВОСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ: СУТНІСТЬ ТА ОСОБЛИВОСТІ

Вінницький національний технічний університет

Анотація

В доповіді розглянуто основні аспекти проведення сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті. З'ясовано про сутність та особливості процесу сканування та визначено засадничі компетенції осіб, які в цьому процесі приймають участь. Доведено, що своєчасні організаційно-технічні та правові заходи забезпечення кіберзахисту державних інформаційних ресурсів, розміщених в Інтернеті, обумовлюють ефективність їх захищеності.

Ключові слова: Інтернет, сканування на предмет вразливості державних інформаційних ресурсів, Державний центр кіберзахисту.

Abstract

The report examines the main aspects of scanning for vulnerability of state information resources located on the Internet. The essence and features of the scanning process are clarified and the main competencies of the persons participating in this process are defined. It is proven that timely organizational, technical and legal measures to ensure cyber protection of state information resources located on the Internet determine the effectiveness of their security.

Keywords: Internet, scanning for vulnerability of state information resources, State Cyber Defense Center.

Вступ

В 1998 році в Україні була схвалена Концепція Національної програми інформатизації. В цій Концепції передбачалося, що «інформатизація – це сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб, реалізації прав громадян і суспільства на основі створення, розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, створених на основі застосування сучасної обчислювальної та комунікаційної техніки» [1].

В 2003 році відбулося схвалення Концепції формування системи національних електронних інформаційних ресурсів. Зокрема, в цій Концепції було визначено, що «національні ресурси є важливою складовою стратегічних ресурсів держави, значення якої зростає із розвитком інформаційних технологій та їх використанням в усіх сферах суспільного життя» [2]. Надалі в Україні було прийнято ряд нормативно-правових актів та проведено організаційно-технічні заходи, які були спрямовані на розвиток та захист системи державних інформаційних ресурсів.

Результати дослідження

Згідно наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2016 № 20: «сканування є однією з форм проведення оцінки стану захищеності інформації в інформаційно-комунікаційних системах і полягає у дистанційній перевірці ІКС, яка забезпечує розміщення державних інформаційних ресурсів у мережі Інтернет, на предмет виявлення в ній вразливостей, які створюють передумови до порушення конфіденційності, цілісності та доступності інформації та державних інформаційних ресурсів, що обробляються ІКС, або спостережності самої ІКС» [3]. Отже, об'єктами сканування є:

- інформаційно-комунікаційна система, в якій обробляються розміщені в Інтернеті державні інформаційні ресурси (її окремі елементи);
- програмні і програмно-апаратні засоби, що застосовуються в інформаційно-комунікаційній системі.

Сканування проводиться Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України згідно наказу Адміністрації Держспецзв'язку від 02 грудня

2014 року № 660 [4], в якому обумовлено порядок оцінки стану захищеності ДІР, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Таблиця 1 – Основні аспекти сканування ДІР [4]

Етапи сканування	Зміст заходів	Примітки
Оцінка (оцінювання) стану захищеності ДІР в ІКС (оцінка стану захищеності)	- це «сукупність заходів, спрямованих на виявлення загроз ДІР та запобігання несанкціонованим діям щодо інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»; - «оцінка стану захищеності є складовою частиною заходів із захисту інформації»	- «в ІКС де створено КСЗІ з підтвердженою відповідністю, оцінка стану захищеності здійснюється з метою виявлення нових загроз ДІР, які виникли у процесі експлуатації КСЗІ та які не враховані у КСЗІ»
Оцінка (оцінювання) захищеності інформації (оцінка захищеності)	- це «заходи щодо виявлення в ІКС технічних рішень, що створюють передумови для порушення конфіденційності, цілісності та доступності інформації, яка в них обробляється»	

Розпорядниками розміщених в Інтернеті ДІР є: органи влади та органи місцевого самоврядування, установи, організації, підприємства та інші формування згідно закону. Відповідальним за оцінку стану захищеності ДІР у розпорядників розміщених в Інтернеті ДІР є: Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (який для реалізації своїх повноважень створює відповідну комісію з оцінки стану захищеності).

Також, ДЦКЗ Держспецзв'язку розробляє загальну програму та методiku оцінки стану захищеності на вказаних об'єктах та визначає інші вимоги для належного функціонування ІКС. Сканування проводиться:

- за письмовим зверненням розпорядника розміщених в Інтернеті ДІР;
- в автоматичному режимі відповідно до сформованого переліку об'єктів сканування.

За результатами сканування (ініційованого за письмовим зверненням) посадові особи ДЦКЗ Держспецзв'язку складають акт сканування на предмет вразливості. Акт складається за визначеною формою: результати сканування; висновки; рекомендації.

Автоматичне дистанційне сканування проводиться ДЦКЗ Держспецзв'язку з урахуванням даних, що містяться в Реєстрі інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління [5]. Про результатами проведення автоматизованого дистанційного сканування ДЦКЗ Держспецзв'язку інформує:

- розпорядників відповідних інформаційних ресурсів (якщо виявлено вразливості тощо);
- Національний координаційний центр кібербезпеки Ради національної безпеки і оборони України (щотижня – про встановленні вразливості та недоліки функціонування ІКС);
- Службу безпеки України (по факту затвердження щорічного переліку об'єктів сканування; у разі виявлення інших обставин, оцінка яких виходить за межі компетенцій).

Водночас, посадові особи ДЦКЗ Держспецзв'язку при скануванні ДІР мають враховувати обставини, які надалі можуть формувати типові слідчі версії. Наприклад, пов'язані із виявленням шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ІКС.

Таблиця 2 – Типові слідчі версії у разі виявлення порушення стану захищеності ДІР пов'язаних із ШПЗ [6]

Слідча версія	Особливі примітки
виявлено факт ШПЗ	відомі дані про: несанкціоноване втручання комп'ютерних програм в функціонування операційної системи комп'ютера/комп'ютерів або окремих програм; докази такого втручання; підозрюваних, які надають правдиві свідчення
	відомі дані про: несанкціоноване втручання комп'ютерних програм у функціонування операційної системи комп'ютера/комп'ютерів або окремих програм; докази такого втручання; підозрюваних, які заперечують свою вину, і можливість доведення їх провини ускладнена через неможливість перевірити їхні свідчення
	встановлено факт шкідливого впливу програмного забезпечення на операційні системи комп'ютера/комп'ютерів або окремі програми; є докази вчинення злочину; визначені особи, які можуть мати інтерес у здійсненні шкідливого комп'ютерного впливу та відповідальні за забезпечення

	комп'ютерної безпеки, однак обставини злочину не з'ясовані
	встановлено факт шкідливого програмного впливу на операційні системи комп'ютера/комп'ютерів або окремі комп'ютерні програми; сліди відсутні; особи, підозрювані у вчиненні злочину, не встановлені

Висновки

Сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті є важливим етапом у забезпеченні кібербезпеки України. Дана процедура включає використання спеціальних програмних, програмно-апаратних засобів на предмет виявлення вразливостей, які створюють передумови до порушення конфіденційності, цілісності та доступності інформації та державних інформаційних ресурсів, що обробляються ІКС. Особливістю такого сканування є: нормативно-правове обумовлення цієї процедури; високі стандарти до захисту даних; специфіка функціонування державних органів в цій процедурі. Ефективне виявлення та усунення вразливостей сприяє зниженню ризику кібератак та забезпеченню стійкості державних інформаційних ресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Концепція Національної програми інформатизації : Закон України «Про Концепцію Національної програми інформатизації» від 04.02.1998 № 75/98-ВР. URL : <https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text> (дата звернення: 22.03.2025)
2. Концепція формування системи національних електронних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 05.05.2003 № 259. URL : <https://zakon.rada.gov.ua/laws/show/259-2003-%D1%80#Text> (дата звернення: 22.03.2025)
3. Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2016 № 20. URL : <https://zakon.rada.gov.ua/laws/show/z0196-16#Text> (дата звернення: 22.03.2025)
4. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02.12.2014 № 660. URL : <https://zakon.rada.gov.ua/laws/show/z0090-15#n14> (дата звернення: 22.03.2025)
5. Положення про Реєстр інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління : постанова Кабінету Міністрів України від 03.08.2005 № 688. URL : <https://zakon.rada.gov.ua/laws/show/688-2005-%D0%BF#Text> (дата звернення: 22.03.2025)
6. Техніко-криміналістичне забезпечення розслідування кіберзлочинів : навчальний посібник / Л.О. Майданевич, О.П.Войтович, Г.В.Шелепало. Вінниця : ВНТУ, 2025. 117с.

Майданевич Леонід Олександрович – канд. філос. наук, старший викладач кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

Діденко Дмитро Андрійович – студент групи ІБКС-21Б кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, м. Вінниця, e-mail didenkdmytr@gmail.com

Усатюк Віталій Ярославович – студент групи ІБКС-22Б кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, м. Вінниця, e-mail vitalijusatuk582@gmail.com

Maidanevych Leonid – Candidate of Philosophical Sciences, Senior Lecturer, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com

Didenko Dmytro – Student, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, email: didenkdmytr@gmail.com

Usatyuk Vitaly – Student, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, email: vitalijusatuk582@gmail.com