УДК 004.056

А.А. Булаївський
Л.О. Майданевич

ПОРЯДОК СКАНУВАННЯ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ, РОЗМІЩЕНИХ В ІНТЕРНЕТІ: СУТНІСТЬ ТА ОСОБЛИВОСТІ

Вінницький національний технічний університет

Анотація

В доповіді проаналізовано Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет. З'ясовано суть та особливості реалізації вказаного порядку. Встановлено, що цей порядок є спеціалізованою процедурою, яка (в свою чергу) обумовлена Порядком оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Наголошено на превентивному характері сканування державних інформаційних ресурсів та його ролі у підвищенні стійкості вказаних інформаційних ресурсів.

Ключові слова: Інтернет, кібербезпека, інформаційно-комунікаційні системи, державні інформаційні ресурси, сканування вразливостей, оцінка захищеності.

Abstract

The report analyzes the Procedure for scanning for vulnerability of state information resources posted on the Internet. The essence and features of the implementation of the specified procedure are clarified. It is established that this procedure is a specialized procedure, which in turn is determined by the Procedure for assessing the security status of state information resources in information, electronic communication and information and communication systems. The preventive nature of scanning state information resources and its role in increasing the stability of the specified information resources are emphasized.

Keywords: Internet, cybersecurity, information and communication systems, government information resources, vulnerability scanning, security assessment.

Вступ

Захист державних цифрових активів потребує системного виявлення технічних недоліків у сервісах, що мають вихід у мережу Інтернет. Нормативне регулювання цього процесу дозволяє стандартизувати дії відповідальних сторін та забезпечити стійкість державної інфраструктури до актуальних загроз. Це створює умови для своєчасної нейтралізації вразливостей ще до моменту їхнього використання зловмисниками.

Результати дослідження

Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет [1], визначає організаційні та процедурні засади оцінки захищеності в умовах зростання кіберзагроз. Сканування розглядається як форма дистанційної перевірки інформаційно-комунікаційних систем (ІКС). Насамперед, сканування спрямоване: на виявлення вразливостей, що можуть порушити конфіденційність, цілісність, доступність інформації або спостережність функціонування системи. Таким чином, сканування є інструментом превентивного кіберзахсту та складовою національної системи кібербезпеки.

Нормативною основою Порядку є положення законів України у сфері захисту інформації, електронних комунікацій та кібербезпеки. Об'єктами сканування визначено ІКС та їх компоненти (незалежно від наявності комплексної системи захисту інформації чи сертифікованої системи управління інформаційною безпекою), що підкреслює універсальний характер контролю.

Сканування здійснюється Державною службою спеціального зв'язку та захисту інформації України (Держспезв'язок) через Державний центр кіберзахисту. Це відбувається, як за зверненням розпорядників ресурсів, так і в автоматичному режимі (відповідно до планів оцінювання). Водночас, встановлюються суворі вимоги щодо нерозголошення результатів та заборона використання

виявлених вразливостей в деструктивних цілях. У разі виявлення загроз державній таємниці передбачено обов'язкове інформування Службу безпеки України. Такий підхід забезпечує баланс між технічним аудитом, правовими гарантіями та національною безпекою.

Водночас, варто зауважити, що сканування згідно Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет [1] відбувається при умові дотримання Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [2]. Суть їх взаємодії полягає у тому, що обидва Порядки регулюють процеси перевірки та оцінки стану захищеності інформаційних систем, але з різною специфікою та цілями.

Насамперед, Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [2] визначає організаційні засади проведення оцінки безпеки ІКС, зокрема: планування; автоматизоване та письмове проведення оцінки; порядок інформування та реагування на виявленні порушення. Він охоплює широкий спектр систем та об'єктів, незалежно від їх розміщення в мережі Інтернет.

Водночас, Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет [1] зосереджений саме на дистанційній перевірці розміщених у мережі Інтернет державних інформаційних ресурсів на предмет вразливостей, що створюють загрози конфіденційності, цілосності та доступності інформації. Він передбачає конкретні процедури, зокрема: автоматизоване та сканування за письмовим зверненням; складання актів та рекомендацій; а також порядок інформування відповідних органів.

Отже, суть взаємодії між цими Порядками [1], [2] полягає у тому, що перший є більш спеціалізований. Перший деталізує процедури автоматизованого та сканування за письмовим зверненням саме державних інформаційних ресурсів, розміщених у мережі Інтернет. А також, він виконує функцію частини загальної системи оцінки захищеності, яка обумовлена в другому Порядку. Ці порядки доповнюють один одного, забезпечуючи комплексний підхід до забезпечення кібербезпеки державних інформаційних ресурсів.

Висновки

Запровадження цього порядку сприятиме систематичному виявленню та усуненню вразливостей у державних інформаційних ресурсах, підвищенню рівня кібербезпеки та запобіганню можливих кіберзагроз. Це забезпечить більш надійний захист державних інформаційних ресурсів та підвищить довіру до сервісів, а також унормує проведення сканування та обміну його результатами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет. Наказ; Адміністрація Держспецзв'язку від 15.01.2016 року № 20. URL: https://zakon.rada.gov.ua/laws/show/z0196-16#Text
2. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Наказ; Адміністрація Держспецзв'язку від 02.12.2014 року № 2660. URL: https://zakon.rada.gov.ua/laws/show/z0090-15#Text

Булаївський Артем Андрійович – студент групи 2БС-23б, факультет інформаційної технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: artembulaivskiy@gmail.com.

Майданевич Леонід Олександрович – канд. філос. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

Bulaivskyi Artem – student of group 2BS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: artembulaivskiy@gmail.com.

Maidanevych Leonid – PhD in Philosophical Sciences, Associated Professor, 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