ПІДХІД ДО ОЦІНКИ ВРАЗЛИВОСТЕЙ ДО ІНФОРМАЦІЙНИХ АТАК СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ МЕТОДИКИ CVSSv3

канд. техн. наук, доц. А.В. Снігуров, магістр Д.В. Сацюк, Харківський національний університет радіоелектроніки, м. Харків

Методика Common Vulnerability Scoring System версії 3.1 (CVSSv3.1) на даний час популярна для дослідження вразливостей сучасних інформаційних систем до кібератак [1]. В даній методиці для оцінки рівня вразливості використовується три групи метрик: базові (base), тимчасові (temporal) та оточуючої середи (environmental). В кожну групу метрик входить ряд параметрів. Так, наприклад, в групу базових метрик входять такі параметри, як вектор атаки, комплексність атаки, рівень привілеїв зловмисника, рівень взаємодії зловмисника з користувачем, рівень наслідків від атаки. На підставі оцінок формується вектор вразливості, який заноситься в базу вразливостей.

Дана методика на даний час використовується також і для оцінки вразливостей від кібератак систем електронного документообігу (СЕД). Кібератака 24 лютого 2021 року на СЕД ASKOD була реалізована розсилкою документів, які містили шкідливий код для експлуатації відомої вразливості «Microsoft Office» CVE-2017-0199 з вектором CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H і рівнем вразливості по базовій метриці CVSS (за 10 бальною шкалою) [2].

Але сучасні СЕД – це складні організаційно-технічні системи і є необхідність комплексного аналізу вразливостей таких систем, в тому числі для інформаційних атак, які не входять в поняття кібератак, наприклад, атак з використанням побічних електромагнітних випромінювань елементів комп'ютерів та інше. В доповіді наводиться підхід до використання методики CVSSv3 для аналізу вразливостей для подібних атак на СЕД, наводяться приклади оцінки рівня вразливостей.

Список літератури: 1. Common Vulnerability Scoring System [Електронний ресурс]. Режим доступу до ресурсу: https://www.first.org/cvss/. **2.** Поновлення кібератак з використанням ШПЗ Pterodo хакерського угрупування Armageddon/Gamaredon \CERT-UA. [Електронний ресурс]. - 2021. - Режим доступу до ресурсу: https://cert.gov.ua/article/10702.