АНАЛІЗ МЕТОДІВ РЕАЛІЗАЦІЇ ЦІЛЬОВИХ АТАК НА ІНФОРМАЦІЙНІ СИСТЕМИ

Євгеньєв А. М., Дорофєєва К. І.
Харківський національний університет радіоелектроніки, Харків, Україна

Захист даних в інформаційних системах під час їх функціонування потребує не тільки дотримання політики безпеки, здійснення організаційних заходів чи технічного обслуговування засобів захисту, але й ефективного менеджменту, моніторингу, контролю та оцінки ризиків інформаційної безпеки. Однією із складових ефективного менеджменту інформаційної безпеки в інформаційних системах є правильне реагування на вразливості.

Цільові атаки, на відмінну від масових атак, характеризуються зломом і обходом захисту ІС з більш глибоким проникненням в систему [1,2].

Атака такого типу проводиться у декілька етапів: аналіз «поверхні» проникнення в інформаційну систему; експлуатація вразливості з установкою на пристрої жертви дистанційно керованого програмного забезпечення; закріплення в системі з придушенням засобів захисту, блокуванням контрольних систем і знищенням слідів проникнення; установка цільового ПО і його експлуатація.

Метою доповіді є обґрунтування підходів до розробки ефективної системи керування вразливостями для захисту інформаційних систем від цільових атак. В доповіді наводяться методи забезпечення захисту інформаційної системи, а також аналіз сучасних системи оцінювання ризиків та обґрунтовуються вимоги до наступних функцій самої системи [3]: відслідковування впливу вразливості на компоненти системи; забезпечення відтворюваності дії атак; Захист від цільових атак – це комплексна задача, яку не можна вирішити використовуючи один рівень захисту [4,5]. Для досягнення мети, потрібно застосовувати весь спектр засобів забезпечення інформаційної безпеки; тільки в цьому випадку можна підвищити можливість успішного виявлення і нейтралізації атак.

Список літератури

1. Cyber Risk Remediation Analysis // Systems Engineering Guide : [англ.]. — MITREruen, 2014. — P. 184—191. — ISBN 978-0-615-97442-2.

2. О.В. Сєвєрінов, А.Г. Хрєнов, А.О. Поляков. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. Системи обробки інформації, 9 (2015): 101-104.

3. Левцов, В. Анатомия таргетированной атаки, часть 1 : [рус.] / Левцов, В., Демидов, Н. // Information Security. — 2016. — № 2. — P. 36—39.

4. Jeun, I. A practical study on advanced persistent threats // Computer Applications for Security, Control and System Engineering : [англ.] / Jeun, I., Lee, Y., Won, D.. — Springer Berlin Heidelberg, 2012. — P. 144—152. — doi:10.1007/978-3-642-35264-5_21.

5. Поддубний В.О., Сєвєрінов О.В., Пустомельник О.С. Менеджмент вразливостей як складова частина політики безпеки ІТС. Системи управління, навігації та зв'язку. Збірник наукових праць, 4.62 (2020): 55-58.