АНОТАЦІЯ

Киричок Р.В. Метод автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека». – Державний університет телекомунікацій, МОН України, Київ, 2021.

Дисертаційна робота присвячена вирішенню актуального наукового завдання, сутність якого полягає в розвитку методу автоматичного активного аналізу захищеності корпоративних мереж на основі оцінювання якості механізму валідації вразливостей функціонуючих інформаційних систем.

Безперечно, сьогодні, одним із провідних напрямів забезпечення кібербезпеки корпоративних мереж є впровадження не лише детектуючих механізмів кіберзахисту, які несуть завідомо запізнілий характер реагування, але й превентивних механізмів, серед яких, найперспективнішими залишаються методи активного аналізу захищеності. Дані методи дозволяють окрім своєчасного виявлення вразливостей цільової системи (системи над якою здійснюється аналіз) ще й валідувати їх, тобто підтверджувати можливість реалізації конкретних вразливостей завдяки моделюванню дій потенційного зловмисника шляхом проведення повноцінного тестування на проникнення. При цьому, валідація виявлених вразливостей є ключовим та досить вагомим елементом активного аналізу захищеності, оскільки деякі з вразливостей є лише теоретичними, інші ж можуть бути реалізовані за допомогою відомих експлойтів.

Однак, вирішення питання автоматизації процесу активного аналізу захищеності корпоративних мереж, яке дозволяє мінімізувати основні недоліки такого аналізу, зокрема, обробка великого об’єму інформації, якість активного аналізу захищеності, яка залежить від кваліфікації оператора та ризик виведення з

ладу цільової системи в процесі валідації її вразливостей, залишається нерезультативним. Тобто, існує протиріччя між необхідністю оперативного (в режимі реального часу), якісного виявлення та підтвердження вразливостей корпоративних мереж і можливостями існуючих методів автоматизації процесу активного аналізу їх захищеності.

Для досягнення мети підвищення результативності автоматичного активного аналізу захищеності корпоративних мереж завдяки інтелектуалізації процесу валідації вразливостей програмних та апаратних платформ на основі фаззі-технології було вирішено наступні задачі:

1. Вперше запропоновано математичну модель аналізу кількісних характеристик процесу валідації вразливостей, що ґрунтується на поліномах Бернштейна, які дозволяють описати динаміку даного процесу. Використання даної моделі дозволяє отримувати аналітичні залежності для кількості успішно валідованих та невалідованих вразливостей, а також для кількості випадків валідації вразливостей, що призвели до критичних помилок за час раціонального циклу валідації виявлених вразливостей під час активного аналізу захищеності корпоративної мережі.

2. Вперше розроблено методику аналізу якості роботи механізму валідації виявлених вразливостей корпоративної мережі, яка базується на інтегральних рівняннях, що враховують кількісні характеристики досліджуваного механізму валідації вразливостей в певний момент часу. Дана методика дозволяє будувати закони розподілу показників якості процесу валідації вразливостей та кількісно оцінювати якість роботи механізму валідації виявлених вразливостей, що в свою чергу дозволяє в режимі реального часу відслідковувати та контролювати хід валідації виявлених вразливостей під час активного аналізу захищеності.

3. Вперше розроблено метод побудови нечіткої бази знань для прийняття рішень при валідації вразливостей програмних та апаратних платформ під час активного аналізу захищеності цільової корпоративної мережі, що базується на використанні нечіткої логіки, яка дає можливість забезпечити отримання достовірної інформації про якість механізму валідації вразливостей непрямим

шляхом. Побудована база знань дозволяє формувати вирішальні правила прийняття рішень щодо реалізації тієї чи іншої атакуючої дії, що в свою чергу дозволяє розробляти експертні системи для автоматизації процесу прийняття рішень при валідації виявлених вразливостей цільових інформаційних систем та мереж.

4. Отримав подальший розвиток метод автоматичного активного аналізу захищеності корпоративних мереж, який на основі синтезу запропонованих моделі, методики та методу дозволяє, на відміну від існуючих, абстрагуватися від умов динамічної зміни середовища, тобто постійного розвитку інформаційних технологій, що призводить до зростання кількості вразливостей та відповідних векторів атак, а також зростання готових до використання експлойтів вразливостей та їх доступності, і враховувати лише параметри якості самого процесу валідації вразливостей.

Розроблений та доведений до практичної реалізації метод автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей, завдяки оперативному контролю та корегуванню ходу валідації виявлених вразливостей дозволяє підвищити, згідно з єдиним інтегральним показником, якість валідації вразливостей до 20 разів, що в свою чергу свідчить про підвищення загальної результативності автоматичного активного аналізу захищеності корпоративних мереж.

У вступі обґрунтовується важливість й актуальність теми дисертаційного дослідження, сформульовано мету та задачі роботи, визначено основні положення, наукову та практичну цінність отриманих результатів роботи та наведено особистий внесок автора.

У першому розділі здійснено аналіз поточного стану та перспектив застосування активного аналізу захищеності корпоративних мереж, зокрема проблеми його автоматизації.

У другому розділі проведено експериментальне дослідження функціонування сучасних засобів експлуатації вразливостей, зокрема досліджено сам процес перевірки та підтвердження можливості реалізації вразливостей. Виділено

узагальнюючі характеристики процесу валідації вразливостей, які враховують складну та мінливу природу середовища, а також ризик появи критичної помилки в функціонуванні цільової системи під час експлуатації вразливостей. Здійснено регресійний аналіз отриманих результатів експериментальних досліджень та запропоновано математичну модель аналізу кількісних характеристик процесу валідації вразливостей на основі поліномів Бернштейна. Окрім цього, було вперше отримано аналітичні залежності для кількості успішно валідованих та невалідованих вразливостей, а також для кількості випадків валідації вразливостей, що призвели до критичних помилок за час раціонального циклу валідації виявлених вразливостей під час активного аналізу захищеності корпоративної мережі.

У третьому розділі, на основі проведеного практичного аналізу процесу валідації вразливостей та отриманих, за допомогою поліномів Бернштейна, аналітичних залежностей базових характеристик процесу валідації вразливостей, було виділено додаткові ключові показники якості механізму валідації вразливостей: акуратність, похибка та критична помилка, які дозволяють з великою достовірністю стверджувати про позитивний хід або наслідки валідації вразливостей цільової корпоративної мережі. Окрім цього, для оцінки якості механізму валідації виявлених вразливостей з врахуванням всіх зазначених показників якості, було виведено єдиний інтегральний показник. В результаті, запропоновано методику аналізу якості роботи механізму валідації виявлених вразливостей корпоративної мережі.

На основі аналізу отриманих залежностей показників якості механізму валідації вразливостей корпоративної мережі було виявлено можливість будувати функції належностей для нечітких множин, елементами яких є безпосередньо акуратність, похибка та критична помилка. Виходячи з цього, було прийнято рішення інтелектуалізації процесу валідації вразливостей програмних та апаратних платформ на основі фаззі-технології, шляхом створення бази знань для автоматичного прийняття рішень при валідації вразливостей під час проведення активного аналізу захищеності корпоративних мереж.

В результаті, запропоновано метод побудови нечіткої бази знань та сформовано вирішальні правила прийняття рішень щодо реалізації тієї чи іншої атакуючої дії з врахуванням рангу якості експлойта вразливості під час активного аналізу захищеності цільової корпоративної мережі, а також, на основі синтезу запропонованих наукових результатів, удосконалено метод автоматичного активного аналізу захищеності корпоративних мереж.

У четвертому розділі запропоновано архітектуру програмного прототипу автоматизованої системи активного аналізу захищеності корпоративних мереж, проведено математичне моделювання для підтвердження достовірності отриманих наукових результатів, а також, експериментальне дослідження результативності запропонованого методу автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей.

Узагальнюючим результатом проведених досліджень є метод автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей. Даний метод включає 4 основних етапи. Кожен з яких містить конкретну частину комплексного дослідження, що проведено в рамках цієї роботи.

Дисертація виконувалась в Державному університеті телекомунікацій.

Результати наукових досліджень були використані на кафедрі інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації під час виконання науково-дослідної роботи на тему «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах кібернетичних атак» (№ 0114V00391, ДУТ, м. Київ).

Також результати наукових досліджень прийняті до впровадження в діяльність НДУ «ІНСТИТУТ КІБЕРБЕЗПЕКИ» (акт від 18.02.20); в ТОВ «ЄВРОТЕЛЕКОМ» (акт від 02.03.20).

Ключові слова: корпоративна мережа, активний аналіз захищеності, цільова система, валідація вразливостей, експлойт, якість механізму.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Kyrychok R. The method of building a knowledge base for dicision-making when validating corporate networks vulnerabilities. / R. Kyrychok, G. Shuklin // Scientific Discussion. – 2020. – Vol. 1, №47. – p. 7-11. (Praha, Czech Republic).

Автором було виділено вхідні та вихідні параметри, що описують хід та наслідки валідації вразливостей, введено лінгвістичні змінні, а також сформовано відповідні їм нечіткі множини, які характеризують якість механізму валідації вразливостей.

2. Киричок Р.В. Метод контролю послідовності реалізації атакуючих дій під час активного аналізу захищеності корпоративних мереж. / Р.В. Киричок, Г.В. Шуклін, З.М. Бржевська // Сучасний захист інформації. – 2020. - №2(42). с. 52-58.

Автором запропоновано перспективний підхід щодо підвищення ефективності валідації вразливостей під час автоматичного активного аналізу захищеності корпоративних мереж на основі контролю послідовності реалізації атакуючих дій (експлойтів) згідно зі стратегією вибору дій softmax з використанням ймовірнісного розподілу Гіббса.

3. Киричок Р.В. Методика аналізу якості роботи механізму валідації вразливостей корпоративних мереж. / Р.В. Киричок, Г.В. Шуклін // Телекомунікаційні та інформаційні технології. – 2020. - №2(67). с. 29-40.

Автором розроблено методику аналізу якості роботи механізму валідації виявлених вразливостей корпоративних мереж, яка дозволяє отримувати точну картину якості процесу валідації виявлених вразливостей під час проведення активного аналізу захищеності

4. Киричок Р.В. Моделювання механізму валідації вразливостей при активному аналізі захищеності корпоративних мереж за допомогою поліномів

Бернштейна. // Р.В. Киричок, Г.В. Шуклін, О.В. Барабаш, Г.І. Гайдур / Сучасні інформаційні системи. – 2020. – Том 4, №3. с. 118-123.

Автором визначено та сформовано базові кількісні характеристики процесу валідації вразливостей, а також розроблено математичну модель їх аналізу на основі поліномів Бернштейна, що враховують динаміку процесу валідації.

5. Киричок Р.В. Тест на проникнення як імітаційний підхід до аналізу захищеності корпоративних інформаційних систем. / Р.В. Киричок // Сучасний захист інформації. - 2018. - №2(34). с. 53-58.

6. Киричок Р.В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення / Р.В. Киричок, П.М. Складанний, В.Л. Бурячок, Г.М. Гулак, В.А. Козачок // Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. - № 3. - с. 48-61.

Автором проведено аналіз технології реалізації тестування на проникнення, як одного з ключових елементів активного аналізу захищеності корпоративних мереж.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Киричок Р.В. Алгоритм побудови аналітичних залежностей показників якості валідації вразливостей при активному аналізі захищеності корпоративних мереж. / Р.В. Киричок, Г.В. Шуклін // IX Міжнародна науково-практична конференція «SCIENCE, SOCIETY, EDUCATION: TOPICAL ISSUES AND DEVELOPMENT PROSPECTS»: 2-4 серпня 2020 р. -Харків. с. 113-115.

Автором запропоновано алгоритм побудови початкових аналітичних залежностей кількісних характеристик процесу валідації виявлених при автоматизованому активному аналізі захищеності корпоративної мережі.

8. R. Kyrychok. Intellectualization of information and communication systems vulnerabilities validation process. / R. Kyrychok // Fourth International Scientific and Technical Conference «COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES»: April 22-23, 2020. – Kharkiv: National university of radio electronics, - 2020. – p. 22-23.

9. Киричок Р.В. Використання технологій штучного інтелекту для підвищення якості аналізу захищеності інформаційної системи. / Р.В. Киричок // Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської наукової конференції: 24 жовтня 2019 р. – Київ: Державний університет телекомунікацій, - 2019. – с. 108-111.

10. Киричок Р.В. Гостра необхідність в навчальних кібератаках на критично важливі об’єкти країни / Р.В. Киричок // X Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави»: 4 квітня 2019 року. – Київ: Національна академія Служби безпеки України, - 2019. – с. 312-314.