Нестеренко Олександр Васильович
кандидат технічних наук, доцент,
дійсний член Міжнародної академії інформатики,
професор ВНЗ «Національна академія управління»
м. Київ, Україна

МЕТОДОЛОГІЯ ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ ПРОГНОСТИЧНОГО МОДЕЛЮВАННЯ ЗАРАЖЕННЯ КОМП'ЮТЕРНИМИ ВІРУСАМИ ВЕБ-РЕСУРСІВ ОРГАНУ ДЕРЖАВНОГО УПРАВЛІННЯ НА ОСНОВІ ЕПІДЕМІОЛОГІЧНОГО ПІДХОДУ

В наші часи, в умовах стрімкого зростання Інтернету, зокрема у формі Інтернету речей (*Internet of Things, IoT*) і Усеохоплюючого Інтернету (*Internet of Everything, IoE*) як агрегації людей, процесів, даних та пристроїв, кількість мережевих підключень збільшується до безпрецедентних рівнів. Чим більше вузлів мережі (кількість з'єднань), тим більше можливостей отримують кіберзлочинці та їх шкідливе програмне забезпечення, тим прудкіше зростає й кількість кібератак. Як би добре не наростав рівень ефективності технологій захисту від шкідливих програм, але кількість видів атак постійно є більшою, що потребує застосування заходів, спрямованих на упередження.

Однією з найбільш поширених причин виникнення інцидентів у сфері кібербезпеки є зараження комп'ютерними вірусами. Тому в науково-прикладному плані передусім стоїть проблема прогнозування шляхом математичного моделювання інтенсивності розповсюдження вірусного зараження комп'ютерів. Особливо це стосується автоматизованих систем органів державного управління (ОДУ) та установ, підприємств, організацій, які входять до спільного інформаційного простору ОДУ і використовують його відкриті веб-ресурси, адже зниження рівня безпеки ОДУ, особливо у надзвичайних ситуаціях та в критичних сферах, негативно впливає на безпеку держави в цілому [1].

Іншою проблемою є використання результатів цього моделювання при формуванні та розвитку захищеного середовища функціонування інформаційного простору ОДУ, особливо в частині виявлення вразливостей веб-ресурсів та їх захисту для запобігання можливості зараження через них комп'ютерів користувачів.

Прогнозуванню розвитку антибезпекових процесів на основі математичного моделювання присвячено чимало робіт як закордонних, так і вітчизняних учених та фахівців. В рамках нових підходів щодо прогнозування стану зараження комп'ютерними вірусами об'єктів, які взаємодіють в Інтернеті, враховуючи значну динаміку розвитку процесів зараження, їх різноманіття і поширення джерел доцільним є вивчення

прогнозного моделювання у суміжних галузях, а саме в медицині, адже зі збільшенням кількості ланок в Мережі особливий інтерес викликає схожість закономірностей розвитку кібератак та розвитку біологічних епідемій [2].

В попередніх дослідженнях щодо розвитку епідемій запропоновано починати моделювання з грубих моделей, переваги яких полягають в оперативності підготовки до застосування, наочності, простоті вчасного корегування параметрів відповідно до зміни внутрішніх та зовнішніх умов дії об'єкту моделювання. У якості грубої моделі визначається більш адекватною S-подібна логістична модель у вигляді звичайних диференціальних рівнянь в кінцевих приростеннях та інтегрування кінцевими сумами [3].

При реалізації моделі в програмному середовищі MatLab, по-перше, було використано суто біологічну характеристику – інкубаційний період, який в комп'ютерному світі відповідає латентному періоду, під час якого зловмисний код виконує відповідні налаштування, додаткові проникнення в умовах повної скритності своїх дій. Водночас головним практичним результатом моделювання виявилася «дзвоноподібна» залежність кількості заражених об'єктів, амплітуда якої визначає рівень епідемічної небезпеки [4].

Для практичного застосування результатів моделюванні необхідно враховувати такі показники:

P – загальна кількість можливих об'єктів зараження (кількість комп'ютерів в інфраструктурі, що досліджується);

S, N – кількість об'єктів, сприйнятливих та несприйнятливих до зараження (відповідно, наявність незахищених або недостатньо захищених комп'ютерів і комп'ютерів, обладнаних надійними засобами захисту);

E – кількість об'єктів в інкубації (заражені комп'ютери, які поки що не заражають інших і не ідентифікуються);

I – заражені об'єкти, які активно заражають інших;

R – об'єкти, які вилікувані та отримали імунітет (комп'ютери, в яких зловмисний код знищено антивірусними засобами);

F – об'єкти, які довелося повністю вилучити з роботи після зараження (тобто частка комп'ютерів, які виявилися неспроможними до функціонування внаслідок зараження);

T_E – інкубаційний період, тобто тривалість часу від умовного нуля до того, поки поширення вірусу в інфраструктурі не розпочалося;

T_I – період стану зараження, тобто тривалість часу від умовного нуля до того, коли зараження почало наростати.

Передумовою початку епідемії є певна пропорція нестійких щодо зараження об'єктів S та наявність умов передачі інфекції від інфікованих до сприйнятливих об'єктів. Це визначається певними співвідношеннями: K_S, K_E, K_F – відповідно коефіцієнти сприйнятливості до зараження, передачі зараження, вилучення з роботи. Для прийняття рішень корисним є

дослідження залежностей епідемічних піків від K_S і K_E, а також визначення залежностей піків епідемій від K_S і K_E одночасно, що є більш вигідним.

Якщо небезпечний рівень епідемічного піку є відомим (наприклад, 700 об'єктів з 1000), то необхідно намагатися утримувати в певних межах величини K_S і K_E, тому що їх певні значення будуть вести до небезпечного рівня епідемічного піку у випадку виникнення інцидентів (у даному прикладі K_S має бути меншим 0.7, а $K_E < 0.00674$ (e^{-5}). У цьому сенсі K_S і K_E є головними чинниками для керування епідемічним процесом інциденту.

Якщо проаналізувати основні параметри епідемічного процесу з точки зору мережевого середовища, тоді частка вузлів мережі, які мають абсолютний захист від атак буде оцінюватися як $1 - K_S$. Збільшення цього показника досягається застосуванням широковідомих засобів і заходів антивірусного захисту (від антивірусних програм до потужних IDS – систем запобігання вторгнень).

Ці системи також дозволяють суттєво понизити значення показника ефективності розповсюдження зловмисного коду по всій інфраструктурі K_E. Вони спроможні виявляти сам факт атаки за ознаками нетипової поведінки комп'ютера, навіть, якщо атака такого виду відбулась уперше. Далі виконується миттєве блокування можливих шляхів розповсюдження зараження, а заражена частина системи переводиться у режим карантину, де вивчається, аналізується, лікується.

Також досить ефективними можуть виявитись дії організаційного характеру, наприклад, щодо мінімально можливого рівня включення деякого комп'ютера в обмін даними з іншими комп'ютерами, ретельно проаналізувавши функціональність кожного з комп'ютерів та визначившись стосовно задовільності виконання ними їх функцій.

Список використаних джерел

1. Нестеренко О.В. Безпека інформаційного простору державної влади. Технологічні основи / О.В. Нестеренко. – К.: Наук. думка, 2009. – 352с.

2. Шевченко А.В. Математична модель прогнозування динамики епідемій / А.В. Шевченко, А.Л. Гепко // Профілактична медицина. - 2011. - №3(15). - С. 3-6.

3. Шевченко В.Л. Оптимізаційне моделювання в стратегічному плануванні / В.Л. Шевченко. – К.: ЦВСД НУОУ, 2011. – 283 с.

4. Нестеренко О.В. Прогностичне моделювання зараження комп'ютерними вірусами веб-ресурсів органу державного управління на основі епідеміологічного підходу / О.В. Нестеренко, І.Є. Нетесін, В.Б. Поліщук, В.Л. Шевченко, А.В. Шевченко // Національна безпека у фокусі викликів глобалізаційних процесів в економіці: матеріали ІІІ-ої Міжнародної наукової Інтернет-конференції (Київ – Баку, 15-17 лютого 2019 року) / ВНЗ «Національна академія управління». – Київ: НАУ. – 2019. – С. 78-82.