Нестеренко Олександр Васильович
кандидат технічних наук, доцент, дійсний член Міжнародної академії інформатики, професор ВНЗ «Національна академія управління»
Нетесін Ігор Євгенійович
кандидат фізико-математичних наук, провідний науковий співробітник ДП «УкрНЦРІТ»
Поліщук Валерій Борисович
кандидат технічних наук, директор ДП «УкрНЦРІТ»
Шевченко Віктор Леонідович
доктор технічних наук, професор, Київський національний університет імені Тараса Шевченка
Шевченко Аліна Віталіївна
аспірант, Державний університет телекомунікацій
м. Київ, Україна

ПРОГНОСТИЧНЕ МОДЕЛЮВАННЯ ЗАРАЖЕННЯ КОМП'ЮТЕРНИМИ ВІРУСАМИ ВЕБ-РЕСУРСІВ ОРГАНУ ДЕРЖАВНОГО УПРАВЛІННЯ НА ОСНОВІ ЕПІДЕМІОЛОГІЧНОГО ПІДХОДУ

Сучасний розвиток інформаційно-комунікаційних технологій, їхнє розповсюдження в усьому світі та можливості опрацювання значних об'ємів інформації дозволили створювати в органах державного управління (ОДУ) автоматизовані системи підтримки прийняття рішень з урахуванням парадигми відкритості та оприлюднення інформаційних ресурсів в Інтернеті. Разом із тим на сьогодні вже є очевидною глобальна небезпека, на яку наражаються веб-ресурси ОДУ у зв'язку із екстенсивним зростанням інцидентів інформаційної безпеки (ІБ), що призводить до спотворення ресурсів, перешкоджанню діяльності ОДУ та погіршення їх іміджу, особливо у надзвичайних ситуаціях та в критичних сферах, і, як наслідок, до відповідного зниження рівня безпеки ОДУ та держави в цілому [1, 2].

Однією з найбільш поширених причин виникнення інцидентів у сфері ІБ є зараження комп'ютерними вірусами. Як би добре не зростала кількість та якість технологій захисту від шкідливих програм, але кількість видів атак постійно є більшою (порушник завжди йде на крок попереду). Наприклад, перманентно зростає частка атак «нульового дня» (*Zero-day attack)*, яка потребує застосування заходів, спрямованих на упередження. Водночас необхідно зазначити, що в наші часи відбувається стрімке зростання Інтернету у формі Інтернету речей (*Internet of Things*, *IoT*) і Усеохоплюючого Інтернету (*Internet of Everything*, *IoE*) як агрегації людей, процесів, даних та приладів, що збільшує кількість мережевих підключень до безпрецедентних рівнів. Вочевидь, разом із тим зростає й кількість кібератак. Чим більше

вузлів мережі (кількість з'єднань), тим більше можливостей отримують кіберзлочинці та їх шкідливе програмне забезпечення.

Тому в науково-прикладному плані передусім стоїть проблема прогнозування шляхом математичного моделювання інтенсивності розповсюдження вірусного зараження комп'ютерів, які входять до спільного інформаційного простору ОДУ та установ, підприємств та організацій, що використовують веб-ресурси ОДУ. Іншою проблемою є врахування 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 [3]. Разом із тим необхідно зазначити, що дані щодо здійснення атак надходять у вигляді часових рядів, які, як правило, є нестаціонарними, оскільки їхні основні характеристики змінюються у часі. В цих умовах традиційні регресійні прогноз-моделі лише відбивають статистику того, що вже відбулось і не враховують внутрішню природу джерел даних, особливо що стосуються кібератак. Перспективним підходом є інтелектуальний аналіз даних, який розвивається на базі прикладної статистики та методів штучного інтелекту, що дозволяє здійснити пошук прихованих закономірностей або взаємозв'язків між змінними.

Враховуючи значну динаміку розвитку процесів зараження комп'ютерними вірусами, їх різноманіття і поширення джерел, в рамках нових підходів щодо прогнозування стану зараження об'єктів, що взаємодіють в Інтернеті, доцільним є вивчення прогноз-моделювання для суміжних галузей, а саме медицини [4], адже зі збільшенням кількості ланок в мережі особливий інтерес викликає схожість закономірностей розвитку кібератак та розвитку біологічних епідемій.

Не буде перебільшенням зауважити, що уся історія людства пов'язана з великими епідеміями. Досвід вказує, що організувати протидію епідемії набагато легше, якщо спрогнозувати її розвиток, адже таке передбачення дозволяє вчасно вжити адекватних противоепідемічних заходів.

В попередніх дослідженнях виходячи з результатів математичного моделювання встановлені такі умови виникнення епідемій [4]:

1. Поява певної кількості хворих або осіб, які знаходяться в стані інкубаційного періоду.

2. Певне співвідношення частки несприйнятливих осіб та умов передачі інфекції від хворих до сприйнятливих осіб. Математично це визначається певним співвідношенням коефіцієнту сприйнятливості до зараження K_s та коефіцієнту передачі інфекції K_E.

Достатньою умовою виникнення епідемії є одночасне виникнення

першої та другої необхідних умов.

Зазвичай практика висуває до моделей суперечні умови, а саме щодо оперативності, точності, наочності, повноти врахування чинників впливу тощо, що призводить до потреби використання складних моделей. Але чим складніше модель, тим важче забезпечити її вхідними даними, тим вище ступінь невизначеності, в якій вона функціонує. Виходячи з цього моделювання розвитку епідемій варто починати з грубих моделей. Переваги грубих моделей полягають в оперативності підготовки до застосування (оперативність структурного та параметричного синтезу), наочності, простоті вчасного корегування параметрів відповідно до зміни внутрішніх та зовнішніх умов дії об'єкту моделювання.

У якості грубої моделі у [5] визначається більш адекватною S-подібна логістична модель у вигляді звичайного диференціального рівняння

$$\frac{dy}{dt} = m \cdot (y - Y_{min}) \cdot (Y_{max} - y), \quad (1)$$

або у вигляді функції, що є його розв'язком:

$$y(t) = Y_{min} + \frac{Y_{max} - Y_{min}}{1 + e^{-m \cdot (Y_{max} - Y_{min}) \cdot (t - \Delta t)}}, \quad (2)$$

де y – динамічна змінна розвитку (наприклад, кількість інфікованих); t – час; Y_{min}, Y_{max} – нижнє та верхнє обмеження величини y; m – постійний коефіцієнт; Δt – абсциса точки симетрії (зсув кривої вздовж вісі абсцис).

В [6] зазначається, що загалом для моделювання епідемій найбільш підходять інтегрально-диференціальні рівняння. Але для спрощення моделі був виконаний перехід до логістичних звичайних диференціальних рівнянь в кінцевих приростеннях та заміна інтегрування кінцевими сумами.

Реалізація моделі в програмному середовищі MatLab підтвердило її працездатність та адекватність (див. рис.1).

Основна увага приділена багатоетапним або багаторівневим атакам, тому в моделі залишено суто біологічну характеристику – інкубаційний період, який в комп'ютерному світі відповідає латентному періоду, під час якого зловмисний код виконує доналаштування, додаткові проникнення в умовах повної скритності своїх дій.

Головним практичним результатом моделювання є «дзвоноподібна» залежність кількості заражених об'єктів. Амплітуда «дзвоноподібної» залежності визначає рівень епідемічної небезпеки. Передумовою початку епідемії є певна пропорція нестійких щодо зараження об'єктів та наявність умов передачі інфекції від інфікованих до сприйнятливих об'єктів. Це визначається певними співвідношеннями K_s і K_E. Дослідження залежностей епідемічних піків від K_s і K_E є корисним для прийняття рішень. Більш вигідним є визначення залежностей піків епідемій від K_s і K_E одночасно.

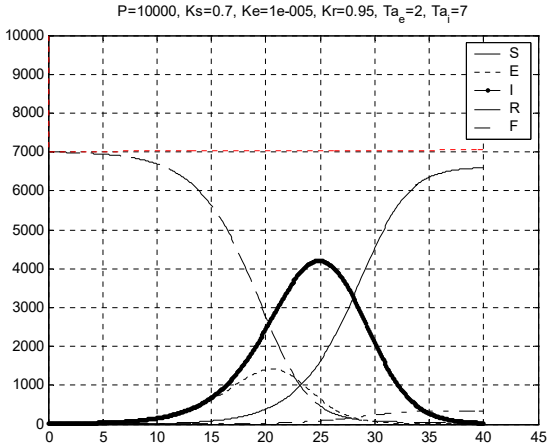

Рис.1. Результати чисельного моделювання кібератак

(P – загальна кількість об'єктів зараження, S, N – сприйнятливі та несприйнятливі до зараження, E – в інкубації (заражені самі, але поки що не заражають інших і не ідентифікуються), I – заражені об'єкти, які активно заражають інших, R – об'єкти, які вилікувані та отримали імунітет (антивірус), F – об'єкти, які довелося повністю вилучити з роботи після зараження; K_S, K_E, K_F – відповідно коефіцієнти сприйнятливості до зараження, передачі зараження, вилучення з роботи (повна втрата працездатності); T_E – інкубаційний період; T_I – період стану зараження)

Якщо ми знаємо небезпечний рівень епідемічного піку, то ми можемо намагатися утримати в певних межах величини K_s і K_E, тому що певні значення K_s і K_E будуть вести до небезпечного рівня епідемічного піку у випадку виникнення інцидентів. У цьому сенсі K_s і K_E є керуючими факторами для епідемічного процесу кібер-інцидентів.

Якщо проаналізувати основні параметри епідемічного процесу з точки зору мережевого середовища, тоді:

$1 - K_s$ – це частка вузлів мережі, які мають абсолютний захист від атак. Це досягається такими шляхами як повне відключення від мережі та заборона використання зовнішніх носіїв інформації, які потенційно можуть бути підключені до інших комп'ютерів (100%-ий захист), а також встановлення антивірусних програм, захисних приладів (*firewall*), або більш складних застосувань, таких, наприклад, як систем запобігання вторгнень (*IPS – Intrusion protection system*) тощо (захист наближений до 100%);

K_E – показник ефективності розповсюдження зловмисного коду по всій інфраструктурі у випадку, якщо десь у ній відбулось зараження.

Список використаних джерел

1. Горбулін В.П. Системно-концептуальні засади стратегії національної безпеки України / В.П. Горбулін, А.Б. Качинський. – К.: ДП «НВЦ «Євро-атлантикінформ», 2007. – 592 с.

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

3. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б. Качинський; Інститут проблем національної безпеки; Національна академія Служби безпеки України. – К., 2004. – 472 с.

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

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

6. Shevchenko A. The Epidemiological Approach to Information Security Incidents Forecasting for Decision Making Systems / A. Shevchenko, V. Shevchenko // 13-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. – Polyana, April 20-23, 2017. – P. 174-177.

Шпак Олександр Іванович
викладач кафедри програмного забезпечення систем
факультету інформаційних технологій
ДВНЗ «Ужгородський національний університет»
Струков Богдан Миколайович
студент 4-го курсу факультету інформаційних технологій
ДВНЗ «Ужгородський національний університет»
м. Ужгород, Закарпатська область, Україна

МЕТОДИ ЕФЕКТИВНОСТІ АГРЕГАЦІЇ КАДРІВ В БЕЗПРОВІДНИХ МЕРЕЖАХ

За останні два десятиліття безпровідний зв'язок в Україні набув стрімкого розвитку. Швидкість передачі даних за цей час зросла в сотні разів. Тим не менше, реальна пропускна здатність безпровідних мереж, вимірювана на канальному рівні, стала значно нижчою [1].

Часові витрати, викликані необхідністю прослуховування каналу, передачею службових кадрів і використанням для цього спеціальних міжкадрових проміжків, а також очікуванням станціями випадкового часу при вирішенні конфліктів, призводять до того, що навіть «ідеальний» безшумний канал зазвичай використовується неефективно. Більше того, при подальшому збільшенні швидкості передачі протокол управління доступом до середовища стає вузьким місцем всієї системи, не дозволяючи отримати суттєвий приріст пропускної здатності каналу навіть при використанні найефективніших технологій фізичного рівня.

Стандартом IEEE 802.11n передбачено три типи агрегації кадрів:

– AMSDU (Aggregated Mac Service Data Unit);