Romuald Hoffmann[1], Tomasz Protasowicki[2]

Klasyczne modele rozprzestrzeniania się wirusów komputerowych w ujęciu dynamiki systemowej

1. Wstęp

Globalizacja oraz ciągły postępujący rozwój technologii ICT spowodowały lawinowy wzrost użycia wszelkiego rodzaju urządzeń komputerowych. Jako ich użytkownicy, biznesowi czy indywidualni, staliśmy się od nich uzależnieni. W tej sytuacji wszelkiego rodzaju oprogramowanie złośliwe, w tym wirusy komputerowe, jest już nie potencjalnym, ale rzeczywistym i kluczowym ryzykiem biznesowym funkcjonowania nie tylko organizacji dowolnej wielkości, ale również przeciętnego użytkownika domowego komputera lub urządzenia przenośnego. Stąd też od wielu lat badacze poszukują modeli opisujących dynamikę rozprzestrzeniania się wirusów komputerowych – teoretycznych i praktycznych. W konsekwencji w literaturze zaproponowano zaadaptowanie modeli epidemiologicznych do modelowania rozprzestrzeniania się wirusów w sieciach komputerowych.

W.H. Murray[3] jako pierwszy zasugerował związek pomiędzy epidemiologią a wirusami komputerowymi, wskazując na fakt, że wirusy komputerowe są pewną analogią wirusa biologicznego. J.O. Kephart i S.R. White[4] byli pierwszymi autorami, którzy zaproponowali przyjęcie modelu SIS (ang. *susceptible*, *infected*, *susceptible*) jako modelu rozprzestrzeniania się wirusów komputerowych. Od tego czasu modele epidemii były szeroko stosowane do modelowania dynamiki rozprzestrzenia się wirusów komputerowych.

---

[1] Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.
[2] Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.

[3] W.H. Murray, *The application of epidemiology to computer viruses*, „Computer and Security" 1988, vol. 7, s. 139–145.

[4] J.O. Kephart, S.R. White, *Directed-graph epidemiological models of computer viruses*, w: *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, 1991, s. 343–359; J.O. Kephart, S.R. White, *Measuring and modeling computer virus prevalence*, w: *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, 1993, s. 2–15.

Ogólnie rzecz ujmując, modele epidemii można podzielić na dwie kategorie – modele deterministyczne, oparte na równaniach różniczkowych, i modele stochastyczne, wykorzystujące w większości łańcuchy Markowa, procesy gałązkowe i procesy dyfuzji. W niniejszej pracy bazujemy na deterministycznych modelach epidemii. Niemniej warto wspomnieć tutaj, że stochastyczny model SIS został wprowadzony przez G.H. Weissa i M. Dishona[5], którzy zastosowali ciągły proces narodzin i śmierci do modelowania epidemii. Porównanie deterministycznych oraz stochastycznych modeli SIS i SIR (ang. *susceptible*, *infected*, *recovered*) można znaleźć w wybranych publikacjach[6]. Należy tutaj zaznaczyć, że zarówno deterministyczne, jak i stochastyczne modele odgrywają znaczącą rolę w modelowaniu dynamiki zjawisk epidemii. Wskazuje na to istniejąca bogata literatura, w większości dotycząca deterministycznych modeli epidemiologicznych rozprzestrzeniania się wirusów komputerowych. Oprócz klasycznych modeli SIS i SIR, bazujących na modelu W.O. Kermacka i A.G. McKendricka[7], w ostatnich latach zostało sformułowanych wiele nowych, takich jak np.: SEIRS[8], SEIQRS[9] i SIRA[10]. Należy odnotować, że modele omawiane w literaturze przedmiotu, które zostały zaczerpnięte z bogatego wachlarza modeli epidemiologicznych[11], w większości są oparte na równaniach różniczkowych. Modele te stanowią zatem naturalną bazę dla modeli w ujęciu dynamiki systemowej.

Modele podstawowe SIS, SIR, SIRS w ujęciu dynamiki systemowej, bazujące na modelach deterministycznych, są przedmiotem rozważań zawartych w niniejszym artykule. Dodatkowo wskazano na model SAI (ang. *susceptible*,

---

[5] G.H. Weiss, M. Dishon, *On the asymptotic behavior of the stochastic and deterministic models of an epidemic*, „Mathematical Biosciences" 1971, vol. 11, issues 3–4, s. 261–265.

[6] L.J.S. Allen, *An introduction to stochastic epidemic models*, w: *Lecture Notes in Mathematics*, t. 1945, Springer, Berlin 2008, s. 81–130; L.J.S. Allen, A.M. Burgin, *Comparison of deterministic and stochastic SIS and SIR models in discrete time*, „Mathematical Biosciences" 2000, vol. 163, s. 1–33; T. Britton, *Stochastic epidemic models: a survey*, „Mathematical Biosciences" 2010, vol. 225, s. 24–35; M.J. Keeling, J.V. Ross, *On methods for studying stochastic disease dynamics*, „Journal of Royal Society Interface" 2008, vol. 5, s. 171–181.

[7] W.O. Kermack, A.G. McKendrick, *A Contribution to the Mathematical Theory of Epidemics*, „Proceedings of The Royal Society" 1927, vol. 115, s. 700–721.

[8] B.K. Mishra, D.K. Saini, *SEIRS epidemic model with delay for transmission of malicious objects in computer network*, „Applied Mathematics and Computation" 2007, vol. 188, s. 1476–1482.

[9] B.K. Mishra, N. Jha, *SEIQRS model for the transmission of malicious objects in computer network*, „Applied Mathematical Modelling" 2010, vol. 34, s. 710–715.

[10] J.R.C. Piqueira, V.O. Araujo, *A modified epidemiological model for computer viruses*, „Applied Mathematics and Computation" 2009, vol. 213, s. 355–360.

[11] J.D. Murray, *Wprowadzenie do biomatematyki*, Wydawnictwo Naukowe PWN, Warszawa 2006.

antidotal, *infected*) jako uproszczoną wersję modelu SIRA[12] (ang. *susceptible*, *infected*, *removed*, *antidotal*).

2. Krótka charakterystyka metody dynamiki systemowej

Metoda dynamiki systemowej (ang. *system dynamics*) jest metodą budowy modeli symulacji ciągłej, która umożliwia modelowanie struktury oraz dynamiki złożonych systemów i procesów w nich zachodzących. Została zaproponowana w latach 60. XX w. przez J. Forrestera, który opracował jej podstawowe zasady podczas swojej pracy w Sloan School of Management i przedstawił je w licznych publikacjach[13]. Metoda dynamiki systemowej jest przeznaczona do modelowania złożonych systemów, w których występują tzw. sprzężenia zwrotne opisujące zależności przyczynowo-skutkowe pomiędzy elementami systemu[14]. W modelach matematycznych zbudowanych z wykorzystaniem metody dynamiki systemowej wyróżniamy równania: poziomów (opisane równaniami różniczkowymi pierwszego rzędu), przepływów (dane równaniami algebraicznymi) i zmiennych pomocniczych (określone jako równania algebraiczne). Z równań tych otrzymujemy układ równań różniczkowo-algebraicznych, stanowiący opis matematyczny związków przyczynowo-skutkowych występujących w modelowanym systemie. W metodzie dynamiki systemowej są stosowane równania różniczkowe zwyczajne pierwszego rzędu wyprowadzone z ogólnej postaci zagadnienia Cauchy'ego[15]. Bardzo dobrym wprowadzeniem do metod dynamiki systemowej jest praca J.D. Stermana[16].

---

12 J.R.C. Piqueira, V.O. Araujo, *A modified epidemiological model for computer viruses*, „Applied Mathematics and Computation" 2009, vol. 213, s. 355–360.

13 J.W. Forrester, *Industrial Dynamics*, MIT Press, Cambridge 1961; J.W. Forrester, *The collected papers of Jay W. Forrester*, Wright-Allen Press, Cambridge 1975; J.W. Forrester, *Urban Dynamics*, MIT Press, Cambridge 1969.

14 R. Hoffmann, T. Protasowicki, *Metoda dynamiki systemowej w modelowaniu złożonych systemów i procesów*, „Biuletyn Instytutu Systemów Informatycznych" 2013, nr 12, s. 19–28; R. Hoffmann, T. Protasowicki, *Modelowanie pola walki z zastosowaniem koncepcji dynamiki systemowej*, „Biuletyn Instytutu Systemów Informatycznych" 2013, nr 12, s. 29–34.

15 E. Kasperska, *Dynamika systemowa. Symulacja i optymalizacja*, Wydawnictwo Politechniki Śląskiej, Gliwice 2005.

16 J.D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill, NewYork 2000.

3. Modele SIR (*susceptible*, *infected*, *recovered*)

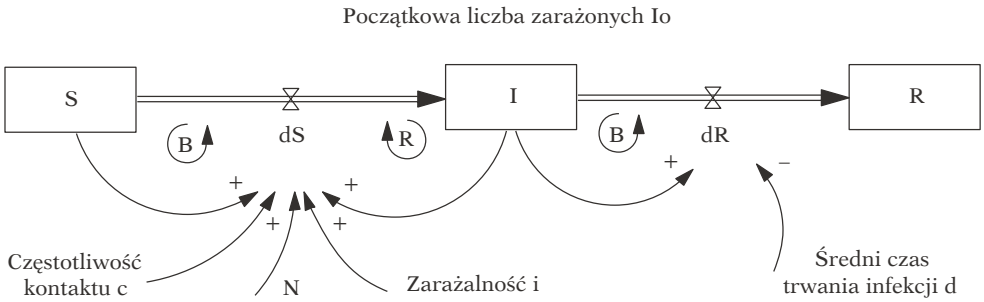
W modelach SIR przyjęto założenie, że rozprzestrzenianie się kodu złośliwego prowadzi do podziału populacji komputerów na trzy grupy urządzeń:

- podatne ($S(t)$, $t \geq 0$) – takie, które mogą zostać zainfekowane;
- zainfekowane ($I(t)$, $t \geq 0$) oraz
- wyleczone ($R(t)$, $t \geq 0$).

Do grupy wyleczonych zaliczamy takie komputery, z których kod złośliwy został usunięty i oprogramowanie zostało zaktualizowane i zyskało tym samym odporność na infekcję. Do tej grupy zaliczają się również urządzenia, które są jeszcze zainfekowane, ale zostały odłączone od sieci lub wyłączone z eksploatacji. Podstawowym modelem tutaj jest klasyczny model Kermacka–McKendricka, opisany poniższym układem zwykłych równań różniczkowych:

$$\begin{aligned} \frac{d}{dt}S(t) &= -a \cdot S(t) \cdot I(t), \\ \frac{d}{dt}I(t) &= a \cdot S(t) \cdot I(t) - b \cdot I(t), \\ \frac{d}{dt}R(t) &= b \cdot I(t), \end{aligned} \tag{1}$$

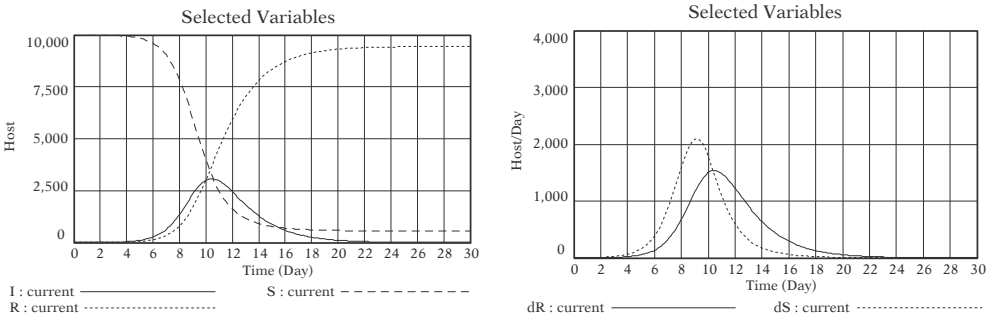
gdzie dane są warunki początkowe: $S(0) = S_0 > 0$, $I(0) = I_0 > 0$ oraz $R(0) = 0$; $a > 0$ oznacza współczynnik (tempo) rozprzestrzeniania się wirusa komputerowego, $b > 0$ jest współczynnikiem (tempem) usuwania kodu złośliwego. Zauważmy, że założenie stałej wielkości populacji komputerów jest już wbudowane w układ równań (1), tzn. $S(t) + I(t) + R(t) = const = N$.



Rysunek 1. Model SIR opisany równaniami (1) w języku dynamiki systemowej

Źródło: opracowanie własne na podstawie: J.D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill, Boston 2000, s. 304.

W tym miejscu rozważań przyjmiemy, że w modelu SIR w języku dynamiki systemowej będziemy $S(t)$, $I(t)$, $R(t)$ oznaczać odpowiednio S, I, R. Konwencja ta będzie odnosić się również do pozostałych modeli.



Rysunek 2. Model SIR – wynik symulacji: liczba komputerów $N = 10\,000$; czas symulacji 30; $c = 6$; $d = 2$; $i = 25/100$; $I_0 = 1$

Źródło: opracowanie własne.

Wszystkie modele przedstawione w niniejszym artykule zostały zaimplementowane przy pomocy pakietu Vensim® ver. 5, autorstwa Ventana Systems Inc.

Na rysunku 1 przedstawiono model SIR w języku dynamiki systemowej odpowiadający równaniom (1). W modelu przyjęto następujące parametry: $a = c \cdot i / N > 0$, $b = 1/d > 0$. Wyniki przykładowej symulacji dla modelu SIS w języku dynamiki systemowej przedstawiono na rysunku 2.

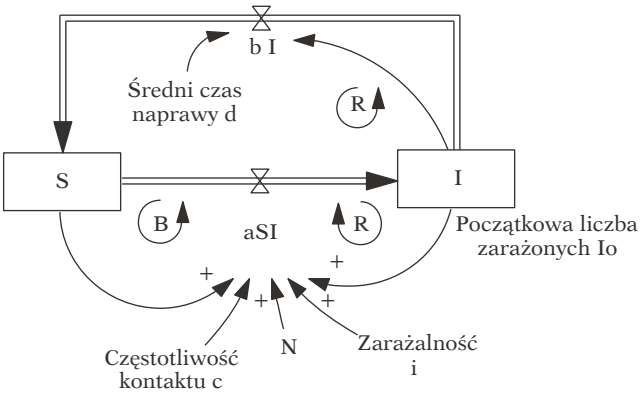
4. Model SIS (*susceptible*, *infected*, *susceptible*)

Model SIS opisuje następujący układ równań różniczkowych:

$$\begin{aligned} \frac{d}{dt}S(t) &= -a \cdot S(t) \cdot I(t) + b \cdot I(t), \\ \frac{d}{dt}I(t) &= a \cdot S(t) \cdot I(t) - b \cdot I(t), \end{aligned} \tag{2}$$

gdzie, podobnie jak w modelu SIR, przyjęto następujące oznaczenia: $S(t)$, $t \geq 0$, oznacza populację urządzeń podatnych na infekcję w chwili t oraz $I(t)$, $t \geq 0$, oznacza populację urządzeń zainfekowanych w chwili t.

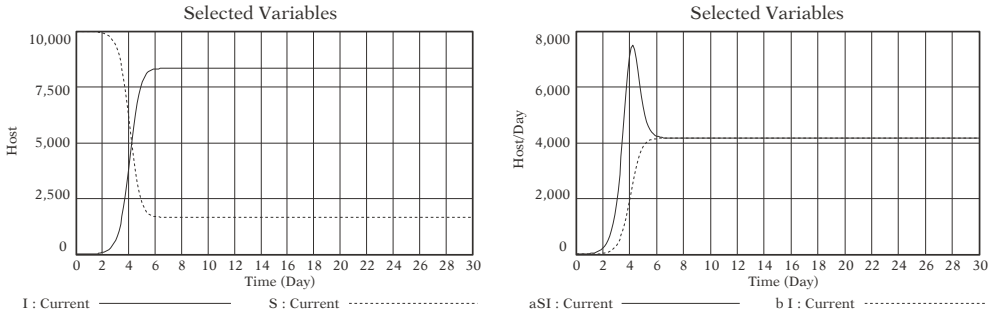
Ponadto dane są warunki początkowe: $S(0) = S_0 > 0$, $I(0) = I_0 > 0$. Parametry $a > 0$ i $b > 0$ przyjęto tak jak w modelu SIR.



Rysunek 3. Model SIS opisany równaniami (2) w języku dynamiki systemowej

Źródło: opracowanie własne.

Na rysunkach 3 i 4 przedstawiono odpowiednio model SIS w języku dynamiki systemowej i wyniki przykładowej symulacji.

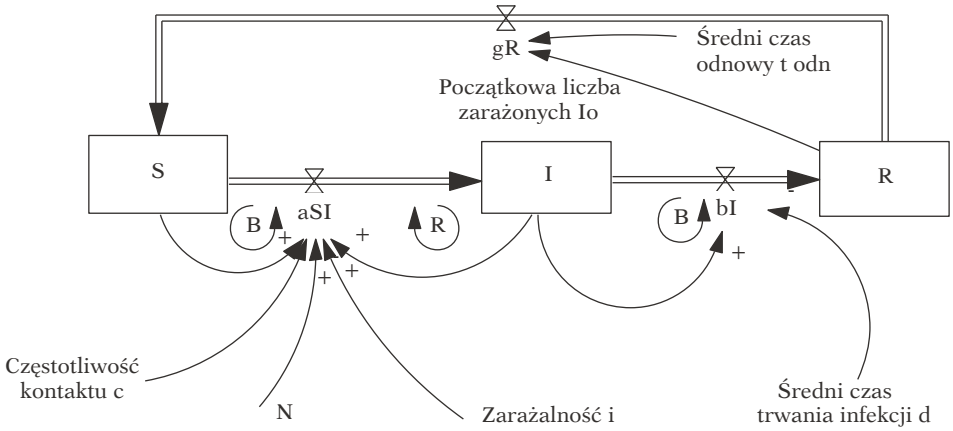


Rysunek 4. Model SIS – wynik symulacji: liczba komputerów N = 10 000; czas symulacji 30; c = 6; d = 2; i = 0,5; I_0 = 1

Źródło: opracowanie własne.

5. Model SIRS (*susceptible*, *infected*, *recovered*, *susceptible*)

Modyfikacją modelu SIR jest model SIRS, którego opis w języku dynamiki systemowej przedstawiono na rysunku 5. Podobnie jak w modelu SIS zakłada się, że urządzenia po usunięciu kodu złośliwego i aktualizacji lub ponownej instalacji (odnowy) oprogramowania wracają do puli komputerów podatnych. Jak zauważymy, w modelu tym występuje dodatkowy przepływ opisany jako $g \cdot R = R/t_{odn}$, oznaczający liczbę komputerów powracających do puli komputerów podatnych.



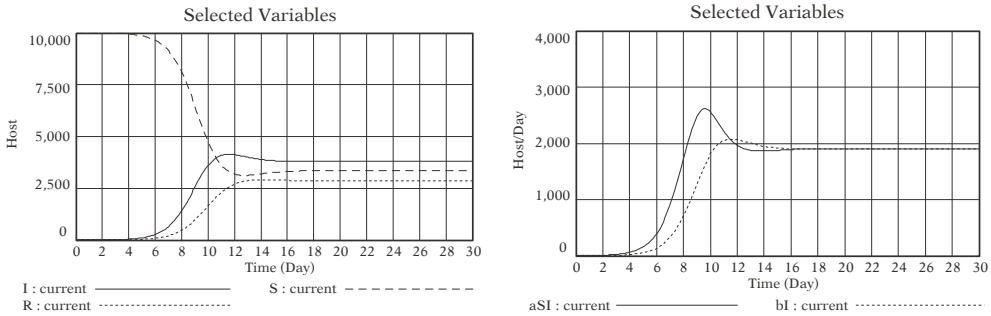
Rysunek 5. Model SIRS w języku dynamiki systemowej

Źródło: opracowanie własne.

Formalnie model SIRS, z przyjętymi warunkami początkowymi jak w modelu SIR, jest opisany następującymi równaniami różniczkowymi:

$$\frac{d}{dt}S(t) = -a \cdot S(t) \cdot I(t) + g \cdot R(t),$$
$$\frac{d}{dt}I(t) = a \cdot S(t) \cdot I(t) - b \cdot I(t),$$
$$\frac{d}{dt}R(t) = b \cdot I(t) - g \cdot R(t),$$

gdzie dane są warunki początkowe: $S(0) = S_0 > 0$, $I(0) = I_0 > 0$ oraz $R(0) = 0$. Pozostałe parametry przyjęto analogicznie jak w modelu SIR: $a = c \cdot i / N > 0$, $b = 1/d > 0$.



Rysunek 6. Model SIRS – wynik symulacji: liczba komputerów $N = 10\,000$; czas symulacji 30; $c = 6$; d = 2; $i = 0{,}25$; $I_0 = 1$, $t_{odn} = 1{,}5$

Źródło: opracowanie własne.

Model SIRS w języku dynamiki systemowej przedstawiono na rysunku 5, natomiast wyniki przykładowej symulacji – na rysunku 6.

6. Model SAI (*susceptible*, *antidotal*, *infected*)

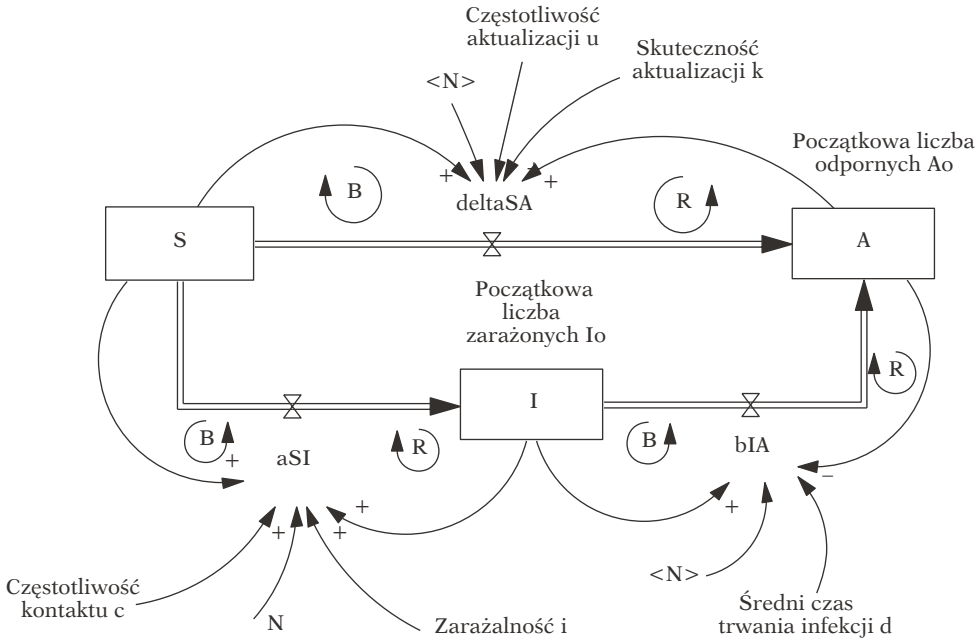
Model SAI[17] jest opisany następującym układem równań różniczkowych:

$$\begin{aligned} \frac{d}{dt}S(t) &= -a \cdot S(t) \cdot I(t) - \delta \cdot S(t) \cdot A(t), \\ \frac{d}{dt}I(t) &= a \cdot S(t) \cdot I(t) - b \cdot I(t) \cdot A(t), \\ \frac{d}{dt}A(t) &= \delta \cdot S(t) \cdot A(t) + b \cdot I(t) \cdot A(t), \end{aligned} \tag{3}$$

gdzie przyjęto oznaczenia: $S(t)$, $I(t)$, $t \geq 0$ – jak w modelu SIR, $A(t)$ – populacja komputerów uodpornionych w wyniku usunięcia podatności i aktualizacji oprogramowania. Wymagane warunki początkowe: $S(0) = S_0 > 0$, $I(0) = I_0 > 0$. Parametry $a > 0$ i $b > 0$ przyjęto tak jak w modelu SIR. Parametr $\delta > 0$ oznacza współczynnik skuteczności usunięcia podatności lub aktualizacji oprogramowania. Na rysunku 7 przedstawiono model SAI w języku dynamiki systemowej.

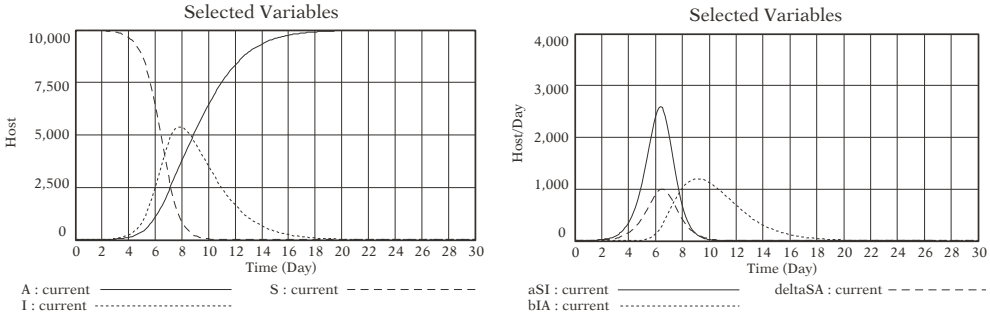
[17] J.R.C. Piqueira, A.A. de Vasconcelos, C.E.C.J. Gabriel, V.O. Araujo, *Dynamic models for computer viruses*, „Computers and Security" 2008, vol. 27, s. 355–359.

W modelu tym przyjęto $\delta = u \cdot k / N$, pozostałe parametry jak w modelu SIR. Wyniki przykładowej symulacji modelu SAI zostały przedstawione na rysunku 8.



Rysunek 7. Model SAI opisany układem równań (3) w języku dynamiki systemowej

Źródło: opracowanie własne.



Rysunek 8. Model SAI – wynik symulacji: liczba komputerów N = 10 000; czas symulacji 30; c = 6; d = 2; i = 0,25; u = 2; k = 0,65; I_0 = 1; A_0 = 1

Źródło: opracowanie własne.

7. Podsumowanie i kierunki dalszych badań

Przedstawione ujęcie klasycznych modeli rozprzestrzeniania się kodu złośliwego w języku dynamiki systemowej stanowi przykład transformowania zapisu formalizmu matematycznego w graficzny język symulacji numerycznej. W artykule zachowano oznaczenia formalne, aby wskazać związek zapisu układu równań różniczkowych z językiem dynamiki systemowej. Oczywiście w praktyce opisy poziomów, przepływów i zmiennych mogą przyjmować formę samodokumentującą znacznie odbiegającą od zapisu symbolicznego. Budowa rozbudowanych i skomplikowanych modeli zatem praktycznie nie sprawia większych problemów.

Opisane w niniejszym artykule modele dynamiki systemowej są tylko modelami generycznymi, a ich praktyczne wykorzystanie wymaga kalibracji na danych rzeczywistych. Niemniej jednak mogą stanowić bazę do budowy bardziej złożonych modeli, np. SIC[18], SEIRS[19], SEIQRS[20], uwzględniających złożoność środowiska informatycznego współczesnej organizacji, wynikającą z wykorzystywania różnorakich urządzeń: począwszy od telefonów komórkowych i smartfonów, poprzez odtwarzacze mp[3], tablety, laptopy, PC, na dużych centrach danych skończywszy.

Połączenie nakreślonych tutaj modeli z dynamicznymi modelami cyklu życia oprogramowania, opisanymi w książce *Software Process Dynamics*[21], oraz modelami zarządzania bezpieczeństwem danych i informacji może stanowić skuteczną metodę predykcji kosztów, a także skutków niezachowania właściwych zasad i polityk bezpieczeństwa.

---

[18] Q. Zhu, X. Yang, L.X. Yang et al., *A mixing propagation model of computer viruses and countermeasures*, „Nonlinear Dynamics" 2013, vol. 73, issue 3, s. 1433–1441.

[19] B.K. Mishra, D.K. Saini, *SEIRS epidemic model with delay for transmission of malicious objects in computer network*, „Applied Mathematics and Computation" 2007, vol. 188, s. 1476–1482.

[20] B.K. Mishra, N. Jha, *SEIQRS model for the transmission of malicious objects in computer network*, „Applied Mathematical Modelling" 2010, vol. 34, s. 710–715.

[21] R.J. Madachy, *Software Process Dynamics*, IEEE Press, Wiley, Hoboken 2007.

Bibliografia

Allen L.J.S., Burgin A.M., *Comparison of deterministic and stochastic SIS and SIR models in discrete time*, „Mathematical Biosciences" 2000, vol. 163, s. 1–33.

Forrester J.W., *Industrial Dynamics*, MIT Press, Cambridge 1961.

Forrester J.W., *Urban Dynamics*, MIT Press, Cambridge 1969.

Forrester J.W., *The collected papers of Jay W. Forrester*, Wright-Allen Press, Cambridge 1975.

Handbook of Software Reliability Engineering, red. M.R. Lyu, McGraw-Hill, New York 1995.

Hoffmann R., Protasowicki T., *Metoda dynamiki systemowej w modelowaniu złożonych systemów i procesów*, „Biuletyn Instytutu Systemów Informatycznych" 2013, nr 12, s. 19–28.

Hoffmann R., Protasowicki T., *Modelowanie pola walki z zastosowaniem koncepcji dynamiki systemowej*, „Biuletyn Instytutu Systemów Informatycznych" 2013, vol. 12, s. 29–34.

Kasperska E., *Dynamika systemowa. Symulacja i optymalizacja*, Wydawnictwo Politechniki Śląskiej, Gliwice 2005.

Kephart J.O., White S.R., *Directed-graph epidemiological models of computer viruses*, w: *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, 1991, s. 343–359.

Kephart J.O., White S.R., *Measuring and modeling computer virus prevalence*, w: *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, 1993, s. 2–15.

Kermack W.O., McKendrick A.G., *A Contribution to the Mathematical Theory of Epidemics*, „Proceedings of The Royal Society" 1927, vol. 115, s. 700–721.

Madachy R.J., *Software Process Dynamics*, IEEE Press, Wiley, Hoboken 2007.

Mishra B.K., Jha N., *SEIQRS model for the transmission of malicious objects in computer network*, „Applied Mathematical Modeling" 2010, vol. 34, s. 710–715.

Mishra B.K., Saini D.K., *SEIRS epidemic model with delay for transmission of malicious objects in computer network*, „Applied Mathematics and Computation" 2007, vol. 188, s. 1476–1482.

Murray W.H., *The application of epidemiology to computer viruses*, „Computer and Security" 1988, vol. 7, s. 139–145.

Piqueira J.R.C., Araujo V.O., *A modified epidemiological model for computer viruses*, „Applied Mathematics and Computation" 2009, vol. 213, s. 355–360.

Piqueira J.R.C., Vasconcelos A.A. de, Gabriel C.E.C.J., Araujo V.O., *Dynamic models for computer viruses*, „Computers and Security" 2008, vol. 27, s. 355–359.

Sterman J.D., *Business Dynamics. Systems Thinking and Modeling for a Complex World*, McGraw-Hill, Boston 2000.

Weiss G.H., Dishon M., *On the asymptotic behavior of the stochastic and deterministic models of an epidemic*, „Mathematical Biosciences" 1971, vol. 11, issues 3–4, s. 261–265.

Zhu Q., Yang X., Yang L.X. et al., *A mixing propagation model of computer viruses and countermeasures*, „Nonlinear Dynamics" 2013, vol. 73, issue 3, s. 1433–1441.

* * *

Classical Propagation Models of Computer Viruses in Terms of System Dynamics

Abstract

Computer viruses are an important risk to computational systems of all size corporations or of personal computers used for domestic applications. Classical epidemiological models for computer virus propagation such as SIR, SIS, SIRS are presented in terms of system dynamics. SAI models (Susceptible, Antidotal, Infectious) are shown as a system dynamic model as well.

Keywords: computer virus, system dynamics, computer virus propagation model, SIR, SIRS, SIS and SAI models, system dynamics model