DOI: 10.24427/978-83-66391-28-4_2

Stochastyczny model ogólnego cyklu życia ataku cybernetycznego

Romuald HOFFMANN[*]

1. Wprowadzenie

Bez wątpienia dzisiejszy rozwój informatyki jest jednym z najważniejszych czynników rozwoju współczesnego świata. Oddziałuje on na wiele procesów społecznych, gospodarczych i militarnych. Wpływ ten należy postrzegać zarówno w sensie pozytywnym, jak i negatywnym. Do niepożądanych efektów jego oddziaływania należy zaliczyć rosnącą cyberprzestępczość. Niestety do grona indywidualnych i zorganizowanych cyberprzestępców dołączyły państwa, dla których ataki w cyberprzestrzeni stały się elementem prowadzonej agresywnej polityki gospodarczej i militarnej, wywołując w ten sposób reakcje obronne pozostałych. Właściwie już teraz można dostrzec swoisty wyścig zbrojeń w cyberprzestrzeni, który zdaniem autora w niedalekiej przyszłości stanie się normą, prowadząc w konsekwencji do poważnych konfliktów militarnych. Nie pomylimy się, twierdząc, że rywalizacja państw w cyberprzestrzeni stała się faktem i zjawisko to obecnie bardzo szybko narasta. Analizując dotychczasowe przypadki ataków cybernetycznych, dostrzega się w nich pewną systematykę – zostały one przeprowadzone według pewnego schematu, który śmiało można określić mianem procesu cyberataku. Pomimo tego, jak często mówi się i pisze o cyberatakach, wiele organizacji odbiera atak cybernetyczny jako krótkotrwałe zdarzenie, któremu prawie nie da się przeciwstawić. W rzeczywistości atak cybernetyczny nie jest jednak aktem chwilowym, ale procesem, na który składa się zbiór czynności, które należy wykonać w odpowiedniej kolejności i które mają swoje czas i miejsce trwania [1] [10]. W zależności od celu ataku czynności te łączy się w logiczne grupy i realizuje etapowo, tworząc w ten sposób proces ataku cybernetycznego. Proces ten ma skończony czas trwania i nazywamy go cyklem życia ataku cybernetycznego (ang. *cyber attack life cycle*, *cyber kill chain*). Znajomość tego cyklu może umożliwić np. oszacowanie prawdopodobieństwa ataku, średniego czasu trwania ataku lub średniego czasu do kompromitacji systemu informatycznego (ang. *time-to-compromise*), a ostatecznie kosztów ataku. Znając te wymienione i inne charakterystyki procesu, możemy starać się odpowiedzieć na kluczowe pytania, np. o to, kiedy nastąpi prawdopodobny atak, jakiej fazie ataku podlegamy i z jakim prawdopodobieństwem.

[*] Wojskowa Akademia Techniczna

W pracy przedstawiono przywołany z [1] opis ogólnego cyklu życia ataku cybernetycznego składającego się z następujących siedmiu faz: identyfikacja i definicja potrzeb – planowanie wstępne, rozpoznanie, uzbrojenie, dostarczenie, uruchomienie i kontrola kodu złośliwego, realizacja celów, zakończenie ataku i zatarcie śladów. Wspomniany cykl modelowano w [1] z wykorzystaniem łańcuchów Markowa z ciągłym parametrem czasu. W modelu źródłowym przyjęto założenie wykładniczego rozkładu prawdopodobieństwa czasów trwania poszczególnych faz cyklu cyberataku, który może stanowić ograniczenie wykorzystania modelu w praktyce. Wobec tego w pracy zaproponowano stochastyczny model ogólnego cyklu życia ataku cybernetycznego, zakładając, że czasy trwania poszczególnych faz ataku mają dowolny ciągły rozkład prawdopodobieństwa. Ponadto w proponowanym modelu uwzględniono powtarzalność ataków cybernetycznych przejawiającą się w powtarzalności cyklu ataku cybernetycznego.

2. Ogólny cykl życia ataku cybernetycznego

W pracy [1] zaproponowano ogólny cykl życia ataku cybernetycznego, składający się z następujących faz: (S_1) identyfikacja i definicja celów ataku – planowanie wstępne, (S_2) rozpoznanie (ang. *reconnaissance*), (S_3) uzbrojenie (ang. *weaponization*), (S_4) dostarczenie kodu złośliwego (ang. *delivery*), (S_5) uruchomienie i kontrola kodu złośliwego (ang. *cyber execution and command & control*), (S_6) realizacja celów (ang. *action, achieve objectives*) oraz (S_7) zakończenie ataku i zatarcie śladów. Propnowany w [1] cykl życia różni się od dotychczas opisywanych w literaturze [2, 3, 4, 5, 6] dwoma dodatkowymi fazami: S_1 i S_2. Te dwie fazy uwzględniają występujące w praktyce czynności planowania i zakończenia ataku. Pozostałe fazy cyklu mają swoje odpowiedniki w literaturze, stąd też podano w nawiasach ich angielskie nazwy. Tabela 1 zawiera opis faz ogólnego cyklu życia ataku cybernetycznego [1].

TAB. 1. Fazy ogólnego cyklu życia ataku cybernetycznego [1]
TAB. 1. Phases of general cyber-attack life cycle [1]

Nazwa fazy	Opis fazy ataku cybernetycznego
Identyfikacja i definicja celów – planowanie wstępne (S_1)	Identyfikacja i określenie potrzeb agresora/atakującego, np. biznesowych, politycznych itp. Faza ta powinna wystąpić nawet wtedy, gdyby był to tylko pomysł przestępcy na przejęcie np. konta ofiary na Twitterze. Na pewno występuje wówczas, gdy np. grupa przestępcza lub jakaś organizacja planuje swoje działania, wynika z przyjętej szerszej strategii państwa dotyczącej działań w cyberprzestrzeni itp.

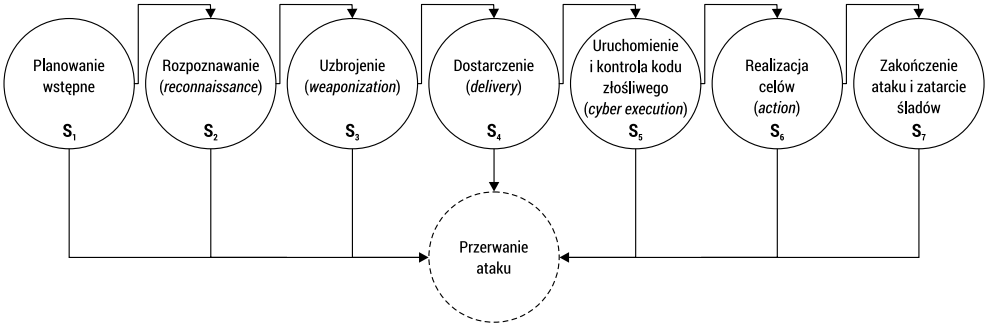
Nazwa fazy	Opis fazy ataku cybernetycznego
Rozpoznanie (ang. *reconnaissance*) (S_2)	Identyfikacja i dobór celów ataków (technicznych) poprzez rozpoznanie docelowego środowiska, np. skanowanie portów TCP, indeksowanie witryn internetowych, materiałów konferencyjnych, list adresów e-mail, sieci społecznościowych, informacji na temat stosowanych (specyficznych) technologii, socjotechniczne wyłudzenie informacji i danych itp.
Uzbrojenie (ang. *weaponization*) (S_3)	Przygotowanie cyberbroni, tzn. specjalnego oprogramowania, np. zintegrowanie koni trojańskich z innym złośliwym kodem (ang. *exploit*) w celu stworzenia możliwego do dostarczenia ładunku za pomocą automatycznego narzędzia (ang. *weaponizer*). W przypadku, gdy nie zachodzi potrzeba budowy lub skonfigurowania pakietu oprogramowania, etap ten może zostać pominięty.
Dostarczenie (ang. *delivery*) (S_4)	Skopiowanie cyberbroni do docelowego środowiska, np. wykorzystanie najbardziej rozpowszechnionych sposobów dostawy (np. w ramach ataków APT), którymi przykładowo są: zainfekowane załączniki do e-maili, spreparowane lub złośliwie zmodyfikowane oprogramowanie strony internetowej (np. aplety, linki), wstrzyknięcie kodu SQL, zainfekowane nośniki danych podłączane do portów USB.
Uruchomienie i kontrola kodu złośliwego (ang. *cyber execution*) (S_5)	1. Uruchomienie kodu złośliwego (po dostarczeniu cyberbroni do środowiska docelowego), np. w wyniku wykorzystania podatności/luki programowej w aplikacji lub systemie operacyjnym lub zmanipulowania użytkownika systemu docelowego. 2. Instalacja dodatkowego kodu złośliwego, np. koni trojańskich (ang. Remote Access Trojan, RAT), umieszczenie tylnych furtek (ang. backdoor) w systemie docelowym w celu zestawienia stałego kanału komunikacji zainfekowanego środowiska wewnętrznego ofiary z centrum (zewnętrznym środowiskiem) dowodzenia i sterowania oprogramowaniem złośliwym. 3. Kontrola i sterowanie zainfekowanego środowiska, np. eskalacja lub uzyskanie dodatkowych uprawnień, systemowych, doinstalowanie pozostałego lub dodatkowego kodu złośliwego (np. ang. backdoor/trojan/rootkit), modyfikacja system plików, przeglądanie lub modyfikacja systemowych baz danych.
Realizacja celów (*achieve objectives, action*) (S_6)	Podjęcie działań nakierowanych na osiągnięcie pierwotnych celów, np. skopiowanie danych, naruszanie integralności i/lub dostępności danych, uzyskanie dostępu do poczty elektronicznej ofiary w celu wykorzystania jej do głębszej penetracji zakatowanej infrastruktury lub wykorzystanie poczty elektronicznej do dalszego rozprzestrzenienia prowadzonego ataku. W tej fazie nie wyklucza się fizycznej destrukcji infrastruktury organizacji.
Zakończenie ataku i zatarcie śladów (S_7)	Zakończenie ataku, może być połączone z usunięciem lub zamaskowaniem śladów ataku i aktywności kodu złośliwego. Etap opcjonalny, zależny od celów i stopnia zaawansowania technologicznego agresora.

ŹRÓDŁO: opracowanie własne.
SOURCE: own elaboration.

3. Podstawowe założenia modelu

Jak już wspomniano na wstępie, podstawą proponowanego w niniejszym artykule stochastycznego modelu jest ogólny cykl życia ataku cybernetycznego (omówiony w poprzednim paragrafie; tab. 1, rys. 1). Na potrzeby prezentowanego modelu przyjmuje się, że nie ma możliwości powrotu z bieżącej fazy do faz poprzednich* oraz pominięcia której kolwiek z faz następnych. Natomiast w modelu uwzględnia się dynamikę procesu ataku, zakładając, że atak może zostać powstrzymany lub przerwany (w ostateczności zakończony) w każdej z faz i w dowolnej chwili, licząc od momentu rozpoczęcia danej fazy ataku. Na rysunku 1 zobrazowano w formie grafu skierowanego możliwe przejścia pomiędzy poszczególnymi fazami cyklu.

W praktyce na jednym cyklu ataku cybernetycznego na daną organizację (przedsiębiorstwo, instytucję, państwo) zazwyczaj się nie kończy. Ataki są powtarzane do skutku, nawet gdyby miało to trwać miesiącami. Jeżeli już atakujący uzyska oczekiwany efekt, to i tak następnie wyznacza sobie nowy cel i rozpoczyna cykl od nowa. Wobec tego zakłada się, że cyberataki mogą być powtarzane, a przerwanie bieżącego ataku skutkuje przystąpieniem przez atakującego do rozpoczęcia nowego cyklu.



RYS. 1. Graf przejść pomiędzy fazami ogólnego cyklu życia ataku cybernetycznego
FIG. 1. Graph of transitions between the phases of the general cyber-attack lifecycle

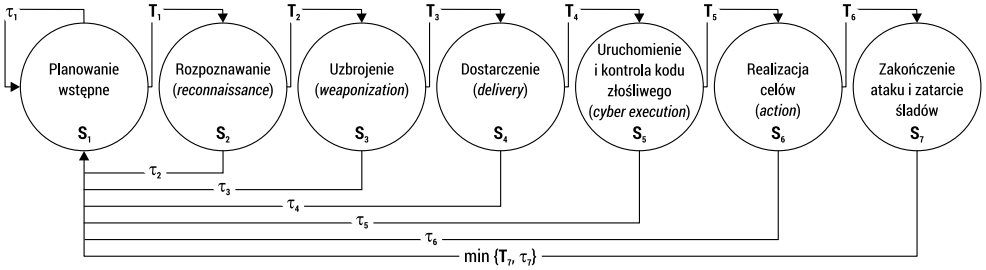
ŹRÓDŁO: opracowanie własne.
SOURCE: own elaboration.

Przyjmijmy, że $T_n \in [0, +\infty))$ oznacza czas niezbędny do zakończenia z sukcesem fazy S_n ($n = 1, 2, \ldots, 7$). Dalej czasy te nazywać będziemy *niezbędnymi czasami trwania faz*. Zakładamy, że T_n jest zmienną losową o dystrybuancie $F_n(t) = \Pr\{T_n < t\}$ i skończonej wartości oczekiwanej ET_n ($ET_n = \int_0^{+\infty} t dF_n(t) < +\infty$). Niech $\tau_n \in [0, +\infty)$ będzie zmienną losową o dystrybuancie $G_n(t) = \Pr\{\tau_n < t\}$ i skończonej wartości oczekiwanej $E\tau_n$ ($E\tau_n = \int_0^{+\infty} t dG_n(t) < +\infty$) oznaczającą czas, po którym może nastąpić zatrzymanie

* Z wyjątkiem powrotu do fazy , który symbolizuje i oznacza rozpoczęcie nowego cyklu ataku.

(przerwanie) ataku, licząc od momentu rozpoczęcia fazy S_n. W tym miejscu, w celu uogólnienia, uczynimy założenie, że bieżący cykl ataku może zakończyć się również w fazie planowania wstępnego. W związku z powyższym czas przebywania w każdej fazie S_n jest równy $\beta_n = \min\{T_n, \tau_n\}$ ($n = 1, 2, \ldots, 7$).

Zgodny z przyjętymi założeniami graf przejść pomiędzy stanami przedstawiono na rysunku 2. Powrót do stanu S_1 symbolizuje rozpoczęcie nowego cyberataku – nowego cyklu ataku cybernetycznego. Łuki grafu przejść pomiędzy fazami cyklu cyberataku opisano czasami, po których może nastapić przejście do fazy następnej lub w ostateczności zakończenie lub przerwanie ataku.



RYS. 2. **Graf ogólnego cyklu życia ataku cybernetycznego z czasami przebywania w fazach**
FIG. 2. **Graph of the general cyber-attack lifecycle with staying time in phases**

ŹRÓDŁO: **opracowanie własne.**
SOURCE: **own elaboration.**

W tym miejscu dodatkowo przyjmuje się założenie, że niezbędne czasy trwania poszczególnych faz są niezależne stochastycznie, tzn. zmienne losowe $T_1, \ldots, T_7$ są niezależnymi zmiennymi losowymi. Ponadto niech zmienne losowe $\tau_1, \ldots, \tau_7$ będą również niezależnymi zmiennymi losowymi. Zakłada się również niezależność stochastyczną zmiennych losowych T_n i τ_n ($n = 1, 2, \ldots, 7$).

4. Czas trwania pojedynczego cyklu ataku cybernetycznego

Przyjmijmy, że $\alpha_n \in \{0,1\}$ dla każdego $n = 1, 2, \ldots 7$ jest binarną zmienną losową[**] – taką, że $\alpha_n = 1$, gdy zachodzi zdarzenie $\{T_n < \tau_n\}$ oraz $\alpha_n = 0$, gdy zachodzi $\{T_n \geq \tau_n\}$. Niech $\Theta \in [0, +\infty)$ oznacza czas trwania pojedynczego cyklu ataku cybernetycznego.

Wobec przyjętych oznaczeń i założeń czas trwania pojedynczego cyklu ataku cybernetycznego Θ można zapisać następująco:

$$\Theta = \beta_1 + \alpha_1 \cdot \beta_2 + \alpha_1 \cdot \alpha_2 \cdot \beta_3 + \alpha_1 \cdot \alpha_2 \cdot \alpha_3 \cdot \beta_4 + \ldots + \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_6 \cdot \beta_7 \qquad (1)$$

gdzie $\beta_n = \min\{T_n, \tau_n\}$.

[**] Indykatorem zdarzenia.

Ze wzoru (1) wynika, że czas trwania pojedynczego cyklu życia ataku cybernetycznego Θ jest sumą zależnych zmiennych losowych – czasów przebywania w poszczególnych fazach cyklu ataku zależnych od zachowania się procesu ataku w fazach poprzedzających daną fazę.

Niech $\overline{F_n}(t) = 1 - F_n(t)$ oraz $\overline{G_n}(t) = 1 - G_n(t)$. Zatem, na podstawie przyjętych założeń o niezależności zmiennych losowych T_n i τ_n, dystrybuanta zmiennej losowej $\beta_n = \min\{T_n, \tau_n\}$ wyraża się wzorem:

$$B_n(t) = \Pr\{\beta_n < t\} = Pr\{\min\{T_n, \tau_n\} < t\} = 1 - \overline{F_n}(t) \cdot \overline{G_n}(t) \tag{2}$$

Wobec tego wartość oczekiwana zmiennej losowej β_n przyjmuje postać:

$$E\beta_n = \int_0^{+\infty} \overline{F_n}(t) \cdot \overline{G_n}(t)\, dt \tag{3}$$

Wartość oczekiwana zmiennej losowej α_n wynosi:

$$E\alpha_n = 1 \cdot Pr\{T_n < \tau_n\} + 0 \cdot Pr\{T_n \geq \tau_n\}$$

Stąd ostatecznie:

$$E\alpha_n = \int_0^{+\infty} F_n(t)\, dG_n(t) = \int_0^{+\infty} \overline{G_n}(t)\, dF_n(t) \tag{4}$$

Z własności wartości oczekiwanej zmiennej losowej [8] wynika, że wartość oczekiwana czasu trwania cyklu ataku cybernetycznego Θ przyjmuje postać:

$$E\Theta = E\beta_1 + E\alpha_1\beta_2 + E\alpha_1\alpha_2\beta_3 + ... + E\alpha_1\alpha_2 \cdot ... \cdot \alpha_6\beta_7$$

Na podstawie przyjętych założeń o niezależności zmiennych losowych T_n i τ_n wartość oczekiwanej długości cyklu ataku cybernetycznego Θ ostatecznie możemy zapisać jako:

$$E\Theta = E\beta_1 + E\alpha_1 \cdot E\beta_2 + E\alpha_1 \cdot E\alpha_2 \cdot E\beta_3 + ... + E\alpha_1 \cdot E\alpha_2 \cdot ... \cdot E\alpha_6 \cdot E\beta_7 \tag{5}$$

gdzie $E\beta_n (n = 1, 2, ..., 7)$ dla dane jest wzorem (3), a dla $E\alpha_n$ – wzorem (4).

5. Proces ataku jako stochastyczny proces regenerujący się

Załóżmy, że $\{X(t), t \in [0, +\infty\}$ jest procesem stochastycznym przyjmującym wartości ze zbioru $\mathbf{S} = \{1, 2, ..., 7\}$, którego kolejne elementy są numerami faz pojedynczego cyklu ataku – odpowiednio: $S_1, S_2, ..., S_7$. Stąd też, długość Θ czasu trwania pojedynczego cyklu ataku cybernetycznego jest chwilą zatrzymania procesu $\{X(t), t \leq \Theta\}$.

W celu dalszych rozważań oznaczmy przez Θ_k, $k = 1, 2, ...$ następujące po sobie cykle ataku cybernetycznego zdefiniowane wzorem (1), a przez $X_k(t)$ – odpowiadający każdemu cyklowi o numerze k proces $X(t)$.

Z wcześniej poczynionych założeń wynika, że ciąg zmiennych losowych $\{\Theta_k\}_{k\geq 1}$ możemy uważać za ciąg niezależnych zmiennych losowych. Przyjmując założenie, że Θ_k mają jednakowy rozkład prawdopodobieństwa z wartością oczekiwana równą $E\Theta$, daną wzorem (5) możemy przyjąć, że pary $(X_k(t), \Theta_k)$, k ∈ {1, 2, ...} są niezależne i o jednakowym rozkładzie. Niech $Y(t)$, $t \in [0, +\infty)$ będzie procesem stochastycznym przyjmującym wartości ze zbioru ***S*** i zdefiniowanym następująco:

$$Y(t) = X_k(t - t_k),\ t_{k-1} \leq t < t_k,\ t_k = \Theta_1 + \Theta_2 + ... + \Theta_k,\ t_0 = 0,\ k \geq 1 \tag{6}$$

Tak zdefiniowany proces $Y(t)$ jest procesem regenerującym się [9], a chwile t_k są momentami regeneracji, w których rozpoczyna się nowy cykl ataku cybernetycznego. W tym przypadku przedziały $[t_{k-1}, t_k)$ są okresami regeneracji procesu (6).

Biorąc pod uwagę założenie powtarzalności (cykli) ataków cybernetycznych, będziemy dalej rozpatrywać ciąg cykli $\{(X_k(t), \Theta_k)\}_{k\geq 1}$ jako model cyklicznego ataku cybernetycznego – ciągłego ataku powtarzanego wg. przyjętego cyklu życia ataku cybernetycznego. Rozpatrywane tutaj cykle $(X_k(t), \Theta_k)$ na podstawie wcześniej przyjętych założeń są stochastycznie niezależne oraz mają rozkłady prawdopodobieństwa stochastycznie równoważne zmiennej losowej Θ. Należy tutaj zauważyć, że z założeń o możliwości przerwania ataku cybernetycznego w dowolnej fazie i, w konsekwencji tego, z konstrukcji czasu Θ trwania pojedynczego cyklu ataku cybernetycznego (1) wynika, że proces $Y(t)$ nie zawsze będzie przechodził przez wszystkie numery faz[***].

6. Stacjonarny rozkład prawdopodobieństwa procesu ataku

Naszym podstawowym zadaniem będzie znalezienie rozkładu stacjonarnego stochastycznego procesu regenerującego się $\{Y(t) \in \{1, 2, ..., 7\}, t \geq 0\}$ określonego przez (6), sprowadzające się do wyznaczenia granic:

$$\lim_{t\to\infty} Pr\{Y(t) = n\} = P_n \tag{7}$$

gdzie n jest numerem fazy S_n ($n = 1, 2, ..., 7$) ataku cybernetycznego.

Z węzłowego twierdzenia odnowy oraz twierdzenia Smitha [7], [9] wynika, że granicę (7) można wyznaczyć z zależności:

$$\lim_{t\to\infty} Pr\{Y(t) = n\} = \frac{1}{E\Theta}\int_0^{+\infty} Pr\left\{\left\{Y(t) = n\right\} \cap \left\{\Theta \geq t\right\}\right\} dt \tag{8}$$

W tym celu w pierwszej kolejności musimy wyznaczyć prawdopodobieństwo tego, że w chwili $t \geq 0$ proces ataku cybernetycznego jest w fazie S_n oraz że atak nie zakończył się do chwili t, tzn. $\Pr\left\{\left\{Y(t) = n\right\} \cap \left\{\Theta \geq t\right\}\right\}$. Zauważmy, że prawdopodobieństwo to jest następujące:

[***] Wszystkie fazy cyklu ataku.

$$
\begin{aligned}
Pr\left\{\left\{Y(t)=n\right\}\cap\left\{\Theta\geq t\right\}\right\} &= Pr\left\{\left\{\sum_{i=1}^{n-1}d_i<t\right\}\cap\left\{\sum_{i=1}^{n}d_i\geq t\right\}\right\}= \\
&= 1-Pr\left\{\left\{\sum_{i=1}^{n-1}d_i\geq t\right\}\cup\left\{\sum_{i=1}^{n}d_i<t\right\}\right\}= \\
&= 1-Pr\left\{\sum_{i=1}^{n}d_i<t\right\}-Pr\left\{\sum_{i=1}^{n-1}d_i\geq t\right\}= \\
&= Pr\left\{\sum_{i=1}^{n}d_i\geq t\right\}-Pr\left\{\sum_{i=1}^{n-1}d_i\geq t\right\}
\end{aligned}
\tag{9}
$$

gdzie $\Theta = d_1 + ... + d_7$, $d_1 = \beta_1$, $d_i = \alpha_1 \cdot ... \cdot \alpha_{i-1} \cdot \beta_i$ dla $i = 2, ..., 7$.

Zauważmy, że na podstawie wzoru (8) otrzymujemy:

$$
\int_0^{+\infty} Pr\left\{\left\{Y(t)=n\right\}\cap\left\{\Theta\geq t\right\}\right\} = \int_0^{+\infty} Pr\left\{\sum_{i=1}^{n}d_i\geq t\right\}-Pr\left\{\sum_{i=1}^{n-1}d_i\geq t\right\}dt
$$

gdzie $\Theta = d_1 + ... + d_7$, $d_1 = \beta_1$, $d_i = \alpha_1 \cdot ... \cdot \alpha_{i-1} \cdot \beta_i$ dla $i = 2, ..., 7$.

W powyższym wyrażeniu całka $\int_0^{+\infty} Pr\left\{\sum_{i=1}^{n}d_i\geq t\right\}dt$ określa nam wartość oczekiwaną [7] sumy zmiennych losowych $\sum_{i=1}^{n}d_i$. Z własności wartości oczekiwanych [8] wynika natomiast, że $E\left\{\sum_{i=1}^{n}d_i\right\} = \sum_{i=1}^{n}Ed_i$. Stąd też możemy zapisać:

$$
\int_0^{+\infty} Pr\left\{\left\{Y(t)=n\right\}\cap\left\{\Theta\geq t\right\}\right\} = E\left\{\sum_{i=1}^{n}d_i\geq t\right\}-E\left\{\sum_{i=1}^{n-1}d_i\geq t\right\} = Ed_n
$$

gdzie $Ed_1 = E\beta_1$, $Ed_n = E\alpha_1 \cdot ... \cdot \alpha_{n-1} \cdot \beta_n$ dla $n \geq 2$.

Wobec powyższego oraz na podstawie (5) granica ostatecznie (9) jest następująca dla każdego $n = 1, 2, ..., 7$:

$$
\lim_{t\to\infty} Pr\{Y(t)=n\} = P_n = \frac{Ed_n}{E\Theta} = \frac{E\alpha_1 \cdot \ldots \cdot E\alpha_{n-1} \cdot E\beta_n}{E\Theta}
\tag{10}
$$

gdzie $E\alpha_1$, $E\alpha_{n-1}$, $E\beta_n$, $E\Theta$ są określone odpowiednio wzorami (3), (4) i (5).

7. Podsumowanie

Przedstawiony w pracy stochastyczny model ogólnego cyklu życia ataku cybernetycznego bazuje na opisie ataku z [1], wyróżniającego się na tle innych publikowanych w literaturze [2, 3, 4, 5, 6] definicji cyklu życia ataku cybernetycznego dodanymi dwoma fazami: identyfikacji i definicji celów, które traktowane są jako planowanie

wstępne ataku oraz zakończenie ataku połączone z zatarciem śladów aktywności agresora. Należy tutaj wskazać także, że w odróżnieniu od dotychczasowego ujęcia problemu, prezentowanego przez innych badaczy [2, 3, 4, 5, 6], w przyjętym w pracy [1] cyklu życia ataku czynności takie, jak: uruchomienie, ewentualna instalacja kodu złośliwego oraz dowodzenie, kierowanie i sterowanie występują jako jedna faza.

Z uwagi na to, że do tej pory w dostępnych źródłach [1, 10, 11] nie publikowano stochastycznego modelu cyklu życia ataku przy założeniu dowolnego ciągłego rozkładu prawdopodobieństwa przebywania cyklu ataku w poszczególnych fazach, w pracy wypełnia się tę lukę, bazując na ogólnym cyklu życia ataku. Podobnie jak w pracach [10, 11] zakłada się możliwość przerwania ataku w trakcie przebywania agresora w dowolnej fazie ataku. W praktyce przerwanie ataku może nastąpić nie tylko z woli cyberprzestępcy, ale również, a może przede wszystkim, z powodu działającego systemu cyberobrony.

Na bazie przedstawionego modelu wyliczone charakterystyki probabilistyczne, takie jak stacjonarne prawdopodobieństwa przebywania procesu ataku w poszczególnych fazach czy wartości oczekiwane czasów trwania poszczególnych faz można wykorzystać na potrzeby procesu szacowania ryzyka i zarządzania bezpieczeństwem organizacji i świadczonych e-usług.

Należy tutaj wskazać, że z praktycznego punktu widzenia do oszacowania ww. charakterystyk potrzeba i wystarcza znajomość wartości oczekiwanych poszczególnych czasów oraz oszacowanie prawdopodobieństwa sukcesu zakończenia poszczególnych faz cyklu ataku.

Literatura

1. Hoffmann R. Ogólny cykl życia ataku cybernetycznego i jego markowowski model. *Ekonomiczne Problemy Usług*. 2018; vol. 1, 2/2018(131): 121-130.
2. Coleman KGJ. *Aggression in Cyberspace*. In: Jasper S, ed. *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*. Washington DC: Georgetown University Press; 2012; 105-119.
3. Hahn A, Thomas RK, Lozano I, Cardenas A. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection*. 2015; 11: 39-50.
4. Hutchins EM, Cloppert MJ, Amin RM. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. In Ryan J, ed. *Leading Issues in Information Warfare and Security Research*, vol. 1. Reading, UK: Academic Publishing International Ltd; 2011; 78-104.
5. Khan MS, Siddiqui S, Ferens K. *A Cognitive and Concurrent Cyber Kill Chain Model*. In: Daimi K, ed. *Computer and Network Security Essentials*. Cham, Switzerland: Springer; 2018; 585-602.
6. Spring JM, Hatleback E. Thinking about intrusion kill chains as mechanisms. *Journal of Cybersecurity*. 2017; 3(3): 185-197.

7. Klimow GP. *Procesy obsługi masowej*. Warszawa: WNT; 1979.
8. Beichelt F. *Stochastic Processes in Science, Engineering and Finance*. New York: Taylor & Francis Group, LLC; 2006.
9. Kowalenko IN, Kuzniecow NJ, Szurienkow WM. *Procesy stochastyczne. Poradnik*. Warszawa: PWN; 1989.
10. Hoffmann R. Markowowskie modele cykli życia ataku cybernetycznego. *Roczniki Kolegium Analiz Ekonomicznych SGH*. 2019; 54: 303-317.
11. Hoffmann R. *Markov Models of Cyber Kill Chains with Iterations*. Materiały z: International Conference on Military Communications and Information Systems – ICMCIS 2019, Montenegro, Budva 2019.

Streszczenie

W pracy oparto się na opublikowanym w literaturze ogólnym cyklu życia ataku cybernetycznego składającym się z następujących faz: identyfikacja i definicja celów ataku – planowanie wstępne, rozpoznanie, uzbrojenie, dostarczenie, uruchomienie i kontrola kodu złośliwego, realizacja celów, zakończenie ataku i zatarcie śladów. W odróżnieniu od modelu źródłowego przyjęto założenie dowolnych ciągłych rozkładów prawdopodobieństwa czasów trwania poszczególnych faz cyklu życia ataku. Ponadto w modelu uwzględniono powtarzalność ataków cybernetycznych. Na tej podstawie wyznaczono stacjonarne prawdopodobieństwa przebywania procesu ataku w poszczególnych fazach.

Słowa kluczowe: atak cybernetyczny, cykl życia ataku cybernetycznego, stochastyczny proces regenerujący się, stochastyczny model, proces ataku, prawdopodobieństwo stacjonarne

Summary
Stochastic model of the general cyber-attack life cycle

The proposed model bases on the description of the general cyber-attack life cycle already published in the literature which consist of the following phases: identification and definition of attack targets and goals – initial planning, reconnaissance, weaponization, delivery, cyber execution and command & control, achieve objectives, ending a cyber-attack and removing traces attacker's activities.

The presented model is distinguishable from the source model by the assumption of any continuous probability distribution of the durations of the cyber-attack life cycle phases was assumed. Additionally, the presented model includes the assumption of the repeatability of cyber-attacks. On this basis, the stationary probabilities of staying of the attack process in individual phases were determined.

Keywords: cyber-attack, stochastic model, cyber-attack life cycle, regenerative stochastic process, attack process, stationary probability