УДК 004.056.5(043)

Б.Є. Журиленко, к.ф.-м.н., К.І. Ніколаєв, Л.В. Рябова
(Національний Авіаційний Університет, Україна)

Математична модель можливого фізичного процесу зламу технічного захисту інформації

Математична модель базується на роботах Б.Журиленка, в яких використано: вкладене в захист інформації фінансування, коефіцієнт ефективності захисту і напрямок процесу зламу. Математична модель будується з врахуванням розподілу Пуассона, яке використовується в теорії масового обслуговування. Розподіл Пуассона дозволяє врахувати ймовірність появлення тієї або іншої спроби та час зламу захисту інформації.

Рішення проблеми.

Вираз для розподілу ймовірності зламу без урахування спроб їх виникнення матиме вигляд

$$P_{взл} = \{ P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m_c,t_c)}{t_c}} \cdot [\frac{t}{f(m,t)+t}] \}^{\gamma}, \quad (1)$$

та вираз для розподілу максимумів ймовірності зламу

$$P_{взл} = \{ P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m,t)}{t}} \cdot [\frac{t}{f(m,t)+t}] \}^{\gamma}, \quad (1a)$$

де $f_i(m,t), f_i(m_c,t_c)$ – функції, які властиві даній системі захисту, що визначають її захисні властивості залежно від напряму зламу (спроб) m_1, t_1, m_2, t_2 та поточних координат m,t. $X=x/H$ – наведене вкладене у захист фінансування; x – величина вкладеного у захист фінансування (наприклад, у грошових одиницях); H – фінансові втрати без технічного захисту інформації (ТЗІ) (у таких же грошових одиницях); $P_m(X)$ – ймовірність зламу від вкладеного у захист фінансування.

$$P_m(X) = \frac{X^X}{(1+X)^{1+X}}. \quad (2)$$

Коефіцієнт ефективності (γ) побудованого захисту матиме вигляд

$$\gamma = \frac{x}{x+H} = \frac{X}{1+X}. \quad (3)$$

Самі ж функції для розподілу ймовірності зламу в залежності від напрямку часу спроби, що виражені через параметри конкретних спроб, для максимуму ймовірності, наприклад, в координатах $m=m_c$, $t=t_c$, мають вигляд:

$$f(m_c,t_c) = [(m_1-1) + \frac{m_2-m_1}{t_2-t_1} \cdot (t_c-t_1)] \cdot t_c, \quad (4)$$

те саме для розподілу ймовірності в залежності від напрямку спроб зламу:

$$f(m_c, t_c) = [t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m_c - m_1)] \cdot (m_c - 1) \ , \tag{4a}$$

і, відповідно, залежності функції у тому же обраному напрямку від поточних координат t и m:

$$f(t) = f(m,t) = [(m_1 - 1) + \frac{m_2 - m_1}{t_2 - t_1} \cdot (t - t_1)] \cdot t \ , \tag{5}$$

$$f(m) = f(m,t) = [t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m - m_1)] \cdot (m - 1) \ . \tag{5a}$$

Зв'язок між координатами спроби зламу m і часом цієї спроби зламу t визначається виразами, якщо m_1=1 и t_1=0 (не є початкові умови, коли перша спроба зламу починається за нульовим часом), де залежність часу зламу від її спроби матиме вигляд

$$t(m) = \frac{\sqrt{A^2 + \frac{4}{\omega} \cdot f(m)}}{2} - \frac{A}{4}, \quad \text{де} \quad A = t_1 + \frac{m_1 - 1}{\omega}, \quad \omega = \frac{m_2 - m_1}{t_2 - t_1} \tag{6}$$

і залежність спроби зламу від його часу

$$m(t) = \frac{\sqrt{B^2 + 4 \cdot \omega \cdot f(t)}}{2} - \frac{B}{2} + 1, \quad \text{де} \quad B = \omega \cdot t_1 - (m_1 - 1) \cdot \tag{6a}$$

Як зазначалося раніше, вирази (1) і (1а) описують залежності ймовірності зламу від вкладеного у захист фінансування та її ефективності, напряму зламу, але ці вирази не дають значення ймовірності зламу без ТЗІ. За відсутності ТЗІ коефіцієнт ефективності захисту дорівнює нулю та ймовірності зламу стають рівними одиниці, що вказує на можливий злам з першої спроби. У реальних умовах цього не має. В цьому випадку процес зламу стає випадковою подією і ймовірність зламу стає випадковою величиною. Отже, ці вирази, крім перелічених параметрів, повинні ще враховувати ймовірність виникнення самих спроб зламу в залежності від їх інтенсивності або параметра λ – частоти появи події зламу, яка в теорії масового обслуговування називається «інтенсивністю вимог або заявок». Інтенсивність спроб зламу λ – це середня кількість подій, що надходить до системи масового обслуговування в одиницю часу при зламі ТЗІ, незалежно від наявності вкладеного у захист фінансування. Іншими словами, в координатах m и t, λ вказує на інтенсивність можливого процесу зламу, що йде, на відміну від інтенсивності спроб зламу ω (6), яке визначає напрям запроектованого або запланованого процесу зламу. Їх значення можуть співпадати λ=ω, якщо реальний процес зламу йде у запроектованому напрямку.

Дотримуючись теорії масового обслуговування λ можна визначити наступним чином

$$\lambda = \frac{m^*_2 - m^*_1}{t^*_2 - t^*_1}, \tag{7}$$

де m^*_1, t^*_1, m^*_2, t^*_2 – визначаються середнім числом випадкових подій чи можливих спроб зламу.

У нашому випадку процес зламу є стаціонарним, тобто λ не залежить від часу, але процес зламу випадковий. Оскільки процес зламу є стаціонарним, ординарним і без наслідків, то такий процес може бути описаний розподілом Пуассона, який повністю відповідає можливому фізичному процесу зламу ТЗІ. Оскільки процес зламу починається з m=1, то розподіл Пуассона для спроб зламу можна записати у вигляді

$$P_m(t) = \frac{(\lambda \cdot t)^{m-1}}{(m-1)!} \cdot e^{-\lambda \cdot t}. \qquad (8)$$

Оскільки процеси подій, що описуються виразами (1), (1а) и (8), є незалежними, то сам процес зламу ТЗІ може бути представлений формулами:

для розподілу ймовірності зламу

$$P_{взл} = \{P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m_c,t_c)}{t_c}} \cdot [\frac{t}{f(m,t)+t}]\}^{\gamma} \cdot P_m(t), \qquad (9)$$

для розподілу максимумів ймовірності зламу

$$P_{взл} = \{P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m,t)}{t}} \cdot [\frac{t}{f(m,t)+t}]\}^{\gamma} \cdot P_m(t) \cdot \qquad (9а)$$

Вирази (9), (9а) є складовими математичної моделі можливого процесу зламу та дозволяють описати його, спираючись на основні параметри, від яких він залежить.

Розглянемо умову, коли немає вкладеного в захист фінансування. У цьому випадку коефіцієнт ефективності захисту γ (3) дорівнює нулю, отже, вирази (9) і (9а) у фігурних дужках, рівні одиниці, тобто ймовірності (9) і (9а) будуть визначатися тільки розподілом Пуассона в напрямку можливого зламу. Якщо запроектований процес зламу вибрати з параметрами m_1=1, t_1=0 и m_2=9, t_2=9; ω=0,889, який співпадає з напрямком можливого зламу, тоді розподіл ймовірності зламу буде визначатися не тільки розподілом Пуассона, а ймовірностями (9) та (9а) .

Розглянемо наступний випадок, коли при тих самих вхідних запланованих параметрах ймовірностей зламу (1), (1а), напрямок можливого зламу відбувається в напрямку лінії 2 (Рис. 1) с параметрами m_{21}=1, t_{21}=0; m_{22}=9, t_{22}=4; λ1=2 (7). У цьому випадку виникнення спроб зламу та їх часу описуватиметься розподілом Пуассона с заявками λ1

$$P1_m(t) = \frac{(\lambda 1 \cdot t)^{m-1}}{(m-1)!} \cdot e^{-\lambda 1 \cdot t}. \qquad (10)$$

а розподіл ймовірностей і максимумів ймовірностей зламу добутком виразів (1) на (10) та (1а) на (10) відповідно. Отже, ймовірності можливого зламу будуть визначатися відповідними виразами

$$P_{взл}1(m,t) = P_{взл}(m,t) \cdot P1_m(t), \qquad (11)$$

де $P_{взл}(m,t)$ – це вираз (1), або (1а).

Вибір такого розподілу (11) пов'язано з тим, що $P_{взл}(m,t)$, в основному, залежить від вкладеного у захист фінансування, його ефективності, напряму спроби та її часу зламу, тобто залежить від параметрів запроектованого технічного захисту. А вираз $P1_m(t)$ описує виникнення розподілів ймовірностей тієї чи іншої спроби та її часу в залежності від можливого напрямку зламу, тобто від інтенсивності появи можливих вимог спроб зламу $\lambda 1$. Цим вираз (11) відрізняється від виразів (9) и (9а), де напрямок зламу йде в запроектованому напрямку $P_m(t)$.

На рис.1 представлено поверхні, розраховані за формулами (1), (1а) помножені на (8) – темні поверхні по лінії 1. Поверхні розраховані за формулами (1), (1а) помножені на (10) – темні поверхні по лінії 2. Ймовірності зламу реального процесу зламу представлені на рис.1 світлою поверхнею $\boldsymbol{P_{взл}=1/m}$. На рис.1а представлені розподіли ймовірностей зламу проектованого (лінія 1) і можливого (лінія 2) напрямків. На рис.1б представлені розподіли максимумів ймовірностей зламу запроектованого (лінія 1) і можливого (лінія 2) напрямків.

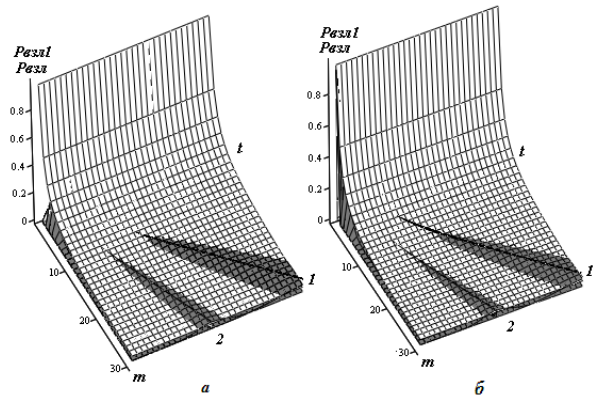

Рис.1 Поверхні з параметрами для обраного випадку: ***а*** **–** запланованого, можливого напрямів зламів (темні поверхні по лініям 1 и 2 відповідно) і реального (світла поверхня) розподілу ймовірності зламу; ***б*** – ті ж позначення для максимумів ймовірностей зламів

З рис.1 видно, що в розглянутих координатах область зламу по запроектованому напрямку (темна поверхня по лінії 1) більша, ніж за напрямком можливого зламу, що йде, (темна поверхня по лінії 2), отже, злам ТЗІ в запроектованому напрямку більш ймовірний, ніж у іншому напрямку. Слід зауважити, що при можливих спробах зламу, чим ближче відбуватиметься процес зламу до координатних осей m, t, тим область можливого зламу буде менша. З рисунка 1 можемо визначити мінімальні координати за напрямом можливого процесу зламу (лінія 2). Наприклад, з рис.1а ці координати будуть: $m_{2взл}=12$, $t_{2взл}=5$.

Таким чином, вираз (11) описує розподіл ймовірності зламу ТЗІ від параметрів: вкладеного фінансування в захист інформації, ефективності вкладеного фінансування, напряму зламу та його інтенсивності, а також ймовірності появи тієї чи іншої спроби зламу.

Щоб отримати математичну модель можливого фізичного процесу зламу технічного захисту інформації, необхідно ще врахувати ймовірність зламу самого захисту. Якщо захист визначається цифровим кодом, необхідно враховувати ймовірність виникнення цього коду. Наприклад, щоб визначити кількість можливих кодів, скористуємося формулою кількості розміщень $A^m{}_n=n^m$. У разі, коли з n цифр необхідно вибрати один код, то необхідно зробити $A^n{}_n=n^n$ разів можливих спроб зламу. Ймовірність вгадати один необхідний код буде $P(n)=(A^n{}_n)^{-1}=(n^n)^{-1}$.

Отже, математична модель можливого фізичного процесу зламу технічного захисту інформації запроектованим напрямком і цифровим кодом матиме вигляд

$$P_{взл}(m,t,n) = P_{взл}(m,t) \cdot P_m(t) \cdot P(n) \cdot \qquad (12)$$

Таким чином, якщо замінити вираз розподілу Пуассона в запроектованому напрямку на напрямок зламу того, що відбувається, то цей вираз математичної моделі (12) може використовуватися для розрахунку ймовірності можливого процесу зламу, що відбувається. У випадку, якщо ймовірність зламу самого захисту не визначається цифровим кодом $P(n)$, її необхідно замінити ймовірністю зламу передбачуваної ТЗІ. Введення в розрахунок коду одного із двох чисел суттєво підвищує ймовірність захищеності ТЗІ. У разі відсутності вкладеного у захист фінансування ймовірність зламу ТЗІ визначатиметься добутком розподілу Пуассона ($P_m(t)$) на ймовірність зламу передбачуваної ТЗІ ($P(n)$).

Висновки.

В результаті виконаної роботи отримано математичну модель можливого фізичного процесу зламу технічного захисту інформації, яка описується такими параметрами: вкладеним у захист фінансуванням, її ефективністю, напрямом спроб зламу та їх інтенсивністю, ймовірністю появи тієї чи іншої спроби зламу та ймовірністю зламу передбачуваної ТЗІ.