УДК 004.056:007 (045)

МОДЕЛЬ КОНФЛІКТНИХ СИТУАЦІЙ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Дмитро Домарєв, Яна Милокум

Проблема управління інформаційною безпекою витікає з необхідності пошуку шляхів підвищення ефективності функціонування інформаційних систем держави в сучасних умовах. Для вибору адекватних протидій загрозам інформаційної безпеки та атакам слід застосовувати моделі взаємодії сторін конфлікту та моделі конфліктних ситуацій в умовах невизначеності. Конфліктні ситуації в управлінні інформаційною безпекою держави змодельовані за стратегічно-імовірніснім підходом. Описано процес конфлікту як перемінний процес з двома станами та відомою матрицею переходів. Наведено формули для розрахунку імовірностей інтервальних переходів між станами атак та захисту. Створено модель конфліктних ситуацій в управлінні інформаційною безпекою, яка завдяки формалізації процесу реагування системи управління інформаційною безпекою на атаки дає змогу автоматизовано прогнозувати інтервали стану безпеки та тривалості відновлення систем інформаційної безпеки після атак.

***Ключові слова**: теорія конфлікту, модель процесу конфлікту, Марківський процес, напівмарківський процес, система управління інформаційною безпекою, СУІБ.*

Актуальність. Проблема управління інформаційною безпекою витікає з необхідності пошуку шляхів підвищення ефективності функціонування інформаційних систем (ІС) держави в сучасних умовах; оцінки ефективності побудови науково-методичного апарату та функціонування систем інформаційної безпеки (ІБ) України; розробки науково-методичних основ, технологій та засобів аналізу, прогнозування й інформаційно-аналітичної підтримки процесів прийняття рішень щодо забезпечення ІБ України; розробки методик та інструментарію оцінки стану інформаційної безпеки як складової національної безпеки України.

На тлі зростання викликів і посилення загроз національній безпеці зберігається невідповідність сектору безпеки і оборони України завданням захисту національних інтересів, що характеризується нездатністю України протистояти новітнім викликам національній безпеці (явищам і тенденціям, що можуть за певних умов перетворитися на загрози національним інтересам), пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам [10].

Зосередженість на короткострокових цілях, нехтування потребами стратегічного розвитку суспільства і держави посилюють загрози національній безпеці і послаблюють спроможність України захищати свої національні інтереси [10]. Для підвищення координованості та контролю діяльності державних органів сфері ІБ держави, посилення їх інформаційно-аналітичного і організаційного забезпечення існує потреба вдосконалення системи управління інформаційною безпекою (СУІБ) держави.

Поняття «інформаційна безпека держави» витікає із поняття національної безпеки і означає захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах ІБ, захисту інформації, ІТ та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам [9]. Захист інформації представляє собою важливу частину усього комплексу заходів та методів, орієнтованих на забезпечення інформаційної безпеки держави [3].

Слід відзначити дві ключових особливості процесу протидії зловмисникам в управлінні ІБ.

По-перше, при захисті ІС іноді застосовують методи адаптації системи до зовнішніх умов, що змінюються. Такий підхід є ефективними лише для підстроювання системи під зміни параметрів зовнішніх завад та шумів природного походження, тобто при конфлікті з природним супротивником. При боротьбі з "розумним супротивником", зокрема, зі зловмисником, який провадить атаки та несанкціоновані вторгненнями в ІС держави, адаптація практично марна, тому що вона за визначенням – пасивна реакція на зміни зовнішніх умов. При адаптації під дії розумного супротивника сторона, що захищається, завжди відставатиме в інформаційній боротьбі, як мінімум, на один крок. Отже, теорія конфлікту завжди є більш доцільною для застосування, ніж теорія адаптації.

По-друге, ключовим принципом системотехніки складних систем є "на обробці інформації економити в останню чергу". Тому в рамках теорії конфлікту не треба зосереджуватись на прос-

тому нарощуванні ресурсів захисту через те, що витрати на захист від атакуючих впливів, як правило, на порядок більші, ніж витрати на їх створення. Найбільш ефективними у цьому сенсі будуть методи затягування супротивника в ескалаційну атаку, створення пасток, хибних вразливостей (так званих "медових пасток"), демонстрацій впевненості або розгубленості тощо.

Враховуючи викладене, розглянемо запропоновану модель управління інформаційною безпекою в рамках загальної теорії конфлікту.

Запропонована модель. Для вибору адекватних протидій загрозам ІБ та атакам слід застосовувати моделі взаємодії сторін конфлікту та моделі конфліктних ситуацій в умовах невизначеності. Конфліктні ситуації в управлінні ІБ держави змодельовані за стратегічно-імовірніснім підходом, описаним в [8].

Для ІС держави, які є дискретними системами із запізнюванням, процеси протиборства між сторонами, одна з яких атакує, а інша – захищається, в загальному випадку (1) описуються рівняннями з аргументами, що відхиляються або диференціально-різницевими рівняннями [6]. Математично сторони представлені системами S_{att} (та, що атакує) і S_{pro} (СУІБ держави).

$$\begin{cases} Y'_{pro}(t) = f_{pro}\left(t, Y_{pro}(t), Y_{pro}(t-\tau_{pro}), U_{pro}(t), y_{att}(t-\tau_{att}), Z_{pro}(t)\right); \\ Y'_{att}(t) = f_{att}\left(t, Y_{att}(t), Y_{att}(t-\tau_{att}), U_{att}(t-\tau_{att}), y_{pro}(t), Z_{att}(t)\right), \end{cases} \quad (1)$$

де Y_{pro} і Y_{att} – вектори стану систем S_{pro} і S_{att} відповідно; τ_{pro} і τ_{att} – запізнювання в S_{pro} і S_{att} відповідно; $U_{pro}(t)$ і $U_{att}(t)$ – вектори управлінь в S_{pro} і S_{att} відповідно; $y_{pro}(t)$ – вектор впливів S_{pro} на S_{att}; $y_{att}(t)$ – вектор впливів S_{att} на S_{pro}; $Z_{pro}(t)$ і $Z_{att}(t)$ – вектори випадкових збурень, що діють на S_{pro} і S_{att} відповідно.

Мета СУІБ держави – максимізувати власну ефективність та знизити ефективність протилежної сторони. На інтервалі спостереження $t\in[0;t^*]$ СУІБ держави доступні лише про стратегію поведінки супротивника і дані про поточний стан Y_{pro} і Y_{att}, спираючись на які можна виробляти найкращі управління $U_{pro}(t)$, впливи $y_{pro}(t)$ і прогнозувати кінцевий результат. Необхідно вирішувати задачу конфлікту з додатковим критерієм мінімізації долі ресурсу, що відводиться на захист, або з обмеженням на допустиму витрату цієї долі ресурсу. В (1) виділення частини ресурсу на заходи захисту або контратаки представлене функцією $y_{pro}(t)$. Результат обраної стратегії та поведінки стане відомий лише у момент часу t^*.

Ефективності систем S_{pro} та S_{att} на інтервалі спостереження $t\in[0;t^*]$ (E_{pro} та E_{att} відповідно) в загальному випадку є нелінійними функціоналами станів Y_{pro}, Y_{att} і векторів $Z_{pro}(t)$ і $Z_{att}(t)$ відповідно. Як випливає з (1), вони взаємопов'язані.

Для розв'язання рівнянь (1) слід застосовувати метод апроксимації Гауса в малій околиці точок екстремумів E_{pro} і E_{att} з урахуванням чинника нормалізації випадкових процесів у великих системах [1]. Вирази ефективності в такому випадку мають вигляд (2).

$$E_{pro} = \int_0^{t^*} Y_{ids}(t)dt; \qquad E_{pro} \to \max y_{pro}; \qquad (2)$$

$$E_{att} = \int_0^{t^*} Y_{att}(t)dt; \qquad E_{att} \to \max y_{att}.$$

Розглянемо процес окремої конфліктної ситуації, наприклад, спроби дезінформації. Нехай перша подія конфлікту відбувається у момент часу $t_1=\tau_1$, i-а подія – у момент часу $t_i=\tau_1+\tau_2+\ldots+\tau_i$, де τ_i ($i\in\{1, 2, \ldots\}$) – незалежні невід'ємні безперервні випадкові величини. τ_i при $i\geq 2$ мають однакову щільність імовірності $h_2(t)=h_3(t)=\ldots=h_i(t)=h(t)$, а τ_1 може мати іншу щільність імовірності $h_1(t)$.

Існують три часткові види процесу відновлення системи, що атакується в залежності від вибору початку відліку часу [2].

Якщо $h_1(t)=h(t)$, має місце *простий процес відновлення*, де усі випадкові величини τ_i мають однакову щільність імовірності $h(t)$. Стратегія захисту в такому випадку є простою і представляє собою періодичну псевдовипадкову зміну методів захисту (наприклад, контратака і блокування атакуючих дій).

Якщо $h_1(t)$ і $h(t)$ не обов'язково однакові, має місце *загальний (модифікований) процес відновлення*, де виконані усі умови простого процесу відновлення, за винятком того, що тривалість від початку спостереження до першої атаки має розподіл, відмінний від решти штатної роботи. Стратегія захисту в такому випадку є аналогічною.

Якщо $h_1(t)$ має вигляд (3), має місце *стаціонарний процес відновлення*, який можна розглядати як простий процес відновлення, в якому конфлікт почався задовго до початку спостереження ($t\to-\infty$), а спостереження процесу починається у момент $t=0$.

$$h_1(t) = \frac{1 - F(\tau)}{m_\tau}, \qquad (3)$$

де $F(\tau)$ – функція розподілу (4), яка визначає імовірність того, що атака відбулась до моменту τ; m_τ – середній час безвідмовної роботи.

$$F(\tau) = P\{\tau_i < \tau\} = \int_0^\tau h(t)dt. \qquad (4)$$

Загальний вплив процесу конфлікту на СУІБ держави розглядається як сума незалежних елементарних випадкових впливів, в якому. При цьому кожен з доданків чинить малий вплив на суму і характер сумарного потоку атакуючих дій є пуассонівським [2].

Нехай потік атак описується законом Пуассона з параметром інтенсивності λ як потік вимог на обслуговування. Розглянемо один з елементів СУІБ – простий апаратний чи програмний засіб.

Спочатку елемент СУІБ вільний. Загроза або атака (заявка на обслуговування) з'являється після випадкового інтервалу часу $\tau^{att}{}_1$, експоненційно розподіленого з параметром λ. Елемент СУІБ у відповідь негайно починає захист або контратаку (обслуговування), через що блокується протягом часу обслуговування $\tau^{pro}{}_2$, і нові заявки на обслуговування не приймаються. Коли елемент звільняється, приймає чергову заявку на обслуговування, що з'явилася після інтервалу часу $\tau^{att}{}_2$ і т.д.

Тип процесу відновлення системи, що захищається, залежить від статистичних характеристик послідовностей випадкових величин $\tau^{att}{}_i$ і $\tau^{pro}{}_j$, ($i,j \in \{1, 2, \ldots\}$). Виходячи з припущення про пуассонівський характер потоку заявок, обидві послідовності випадкових величин взаємно незалежні. Випадкові величини $\tau^{att}{}_i$ – незалежні і однаково експоненційно розподілені з параметром λ. Інтервали блокування $\tau^{pro}{}_j$ – також незалежні і однаково розподілені з щільністю імовірності $h^{pro}(t)$.

З точки зору ІБ держави, найбільший інтерес представляють прийняті заявки, тобто точковий процес. За викладених вище умов утворюється загальний (модифікований) процес відновлення, в якому інтервал до першої події $\tau_1 = \tau^{att}{}_1$ експоненційно розподілений з параметром λ, а інтервали до наступних подій $\tau_2 = \tau^{pro}{}_2 + \tau^{att}{}_2$, $\tau_3 = \tau^{pro}{}_3 + \tau^{att}{}_3$ і т. д. мають однакову щільність імовірності у вигляді згортки $h^{pro}(t)$ відносно експоненційного розподілу інтервалів атак.

На рівні СУІБ держави розглядаються дві взаємно незалежних послідовності невід'ємних безперервних випадкових величин: моментів атакуючих дій і моментів захисних дій (чи контратак) – відповідно $\tau^{att}{}_i$ і $\tau^{pro}{}_j$ ($i, j \in \{1, 2, \ldots\}$). Випадкові величини в межах кожної з цих послідовностей також незалежні між собою і мають однакові щільності імовірності $h^{att}(t)$ і $h^{pro}(t)$ відповідно. Чергування випадкових величин з двох послідовностей (інтервалів двох типів) утворюють перемінний точковий процес відновлення (рис. 1).

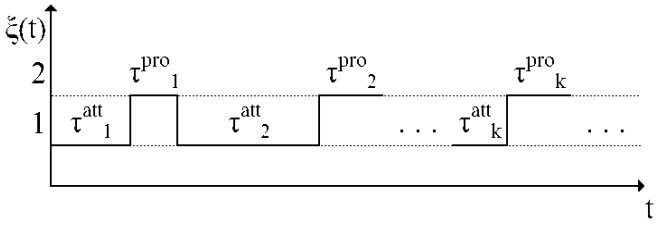

Рис. 1. Перемінний процес відновлення, який відображає процес конфлікту

Процес починається з інтервалу першого типу ($\tau^{att}{}_1$), в кінці якого відбувається подія першого типу (атака). За ним йде інтервал другого типу ($\tau^{pro}{}_1$), що закінчується подією другого типу (захист) у момент часу $\tau^{att}{}_1 + \tau^{pro}{}_1$. Далі цикл повторюється.

Подія першого типу (атака) під номером $(2k-1)$ відбувається у момент часу $\tau^{att}{}_1 + \ldots + \tau^{att}{}_k + \tau^{pro}{}_1 + \ldots + \tau^{pro}{}_{k-1}$, а подія другого типу (захист) під номером $(2k)$ відбувається у момент часу $\tau^{att}{}_1 + \ldots + \tau^{att}{}_k + \tau^{pro}{}_1 + \ldots + \tau^{pro}{}_k$.

Для спрощення представлення зроблено припущення, що період блокування (захисту) починається при $t = 0$, а час блокування елемента СУІБ ототожнено з часом виведення його з ладу і вважається постійним ($\tau^{pro}{}_2 = \tau^{pro}{}_3 \ldots = \tau_0 = \text{const}$). Тоді описаний процес буде простим процесом відновлення, а інтервали між обслуженими заявками матимуть зміщений експоненційний розподіл $\lambda e^{-\lambda(\tau - \tau 0)}$, $\tau \geq \tau_0$.

Нехай щільності імовірності атак і захисту є експоненційними з параметрами λ_1 і λ_2, які є відповідно узагальненою інтенсивністю атак і узагальненою інтенсивністю захисних дій. У найзагальнішому випадку вони є змінними параметрами, які залежать від часу.

Такий процес є нестаціонарним процесом Пуассона [2], а зміна станів (типів інтервалів) процесу конфлікту між атакуючим суб'єктом і СУІБ держави описується напівмарківським процесом, тобто ланцюгом Маркова з двома станами і відомою матрицею переходів. Праці [4, 5] присвячені опису стану СУІБ як напівмарківського процесу.

Напівмарківський процес [7, 11] – це Марківський процес з випадковими інтервалами між переходами. Кожного разу, коли процес входить у певний стан, обираються наступний стан і тривалість затримки відповідно до імовірностей переходів і функцій щільності розподілу тривалості затримок. Після затримки в стані i на час τ_{ij}, процес переходить в стан j, а потім процедура повторюється.

Остаточно напівмарківський процес описується матрицею імовірностей інтервальних переходів (5).

$$\Phi^e(s) = [I - P \square H^e(s)]^{-1} \,^{cc} W^e(s), \tag{5}$$

де I – одинична матриця, □ – поелементне множення, $^e(s)$ – матриця перетворень Лапласа (6).

$$f^e(s) = \int_0^\infty f(t) e^{-\delta t} dt. \tag{6}$$

Стани позначено ξ_1 і ξ_2, а матриця імовірностей переходів має вигляд (7).

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{7}$$

Переходи системи в один і той самий стан не розглядаються ($p_{11} = p_{22} = 0$). Стан ξ1 неодмінно змінюється станом ξ2 і навпаки. Нехай h12(t) і h21(t) – задані щільності імовірності відповідних затримок. Імовірності інтервальних переходів ϕij(t), i, j ∈ [1;2] розраховані за формулою (8) на основі рівняння (5) [8].

$$\begin{aligned} \Phi^e(s) &= \left(I - P \times \begin{pmatrix} 0 & h_{12}^e(s) \\ h_{21}^e(s) & 0 \end{pmatrix} \right)^{-1} \times \begin{pmatrix} 1 - h_{12}^e(s) & 0 \\ 0 & 1 - h_{21}^e(s) \end{pmatrix} = \\ &= \frac{1}{s\left(1 - h_{12}^e(s) h_{21}^e(s)\right)} \begin{pmatrix} 1 - h_{12}^e(s) & h_{12}^e(s)\left(1 - h_{21}^e(s)\right) \\ h_{21}^e(s)\left(1 - h_{12}^e(s)\right) & 1 - h_{21}^e(s) \end{pmatrix}. \end{aligned} \tag{8}$$

В частковому випадку (9) вираз (8) приймає спрощений вигляд.

$$\begin{aligned} &h_{12}(t) = \lambda_2 e^{-\lambda_2 t}; \qquad h_{21}(t) = \lambda_1 e^{-\lambda_1 t}; \\ &h_{12}(s) = \frac{\lambda_2}{s + \lambda_2}; \qquad h_{21}(s) = \frac{\lambda_1}{s + \lambda_1}; \\ &\Phi^e(s) = \frac{1}{s\left(s + \lambda_1 + \lambda_2\right)} \begin{pmatrix} s + \lambda_1 & \lambda_2 \\ \lambda_1 & s + \lambda_2 \end{pmatrix}. \end{aligned} \tag{9}$$

Матриця імовірностей інтервальних переходів (10) знаходиться оберненим перетворенням Лапласа (6):

$$\Phi(t) = \frac{1}{\lambda_1 + \lambda_2} \begin{pmatrix} \lambda_1 + \lambda_2 e^{-(\lambda_1 + \lambda_2)t} & \lambda_2\left(1 - e^{-(\lambda_1 + \lambda_2)t}\right) \\ \lambda_1\left(1 - e^{-(\lambda_1 + \lambda_2)t}\right) & \lambda_2 + \lambda_1 e^{-(\lambda_1 + \lambda_2)t} \end{pmatrix}. \tag{10}$$

При $t = 0$, $\Phi(0) = P$. При $t \to \infty$ має місце (11).

$$\lim_{t \to \infty} \Phi(t) = \frac{1}{\lambda_1 + \lambda_2} \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_1 & \lambda_2 \end{pmatrix}. \tag{11}$$

Висновки. Створено модель конфліктних ситуацій в управлінні інформаційною безпекою, яка завдяки формалізації процесу реагування СУІБ на атаки дає змогу автоматизовано прогнозувати інтервали стану безпеки та тривалості відновлення систем ІБ після атак.

Отриманий результат може бути використаний у виборі структур систем реагування на загрози та заходів із забезпечення ІБ держави. Визначення набору необхідних функцій СУІБ, а також структура взаємозв'язків між складовими розроблюваного методу управління ІБ повинна відбуватись з урахуванням викладеної моделі.

ЛИТЕРАТУРА

[1]. Вентцель Е.С. Исследование операций Е.С. Вентцель – М.: Советское радио, 1972. – 552 с.

[2]. Гнеденко Б.В. Введение в теорию массового обслуживания. 2-е изд. [Текст] / Б.В. Гнеденко, И.Н. Коваленко – М.: Наука, 1987. – 336 с.

[3]. Домарев В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – К.: ООО «ТИД «ДС», 2004. – 992 с.

[4]. Домарев Д.В. Применение полумарковских процессов в разработке и описании состояния систем защиты информации [Текст] / Д.В. Домарев // Системи обробки інформації: Зб. наук. пр. – Х.: ФОП «Азамаєва В.П.», 2009. – Вип. 7(79). – С. 19-24.

[5]. Домарев Д.В. Математическое описание процессов атак на компьютерные сети [Текст] / Д.В. Домарев // Проблеми інформатизації та управління: Зб. наук. пр. – К.: НАУ, 2010. – Вип. 1(29). – С. 50 – 54.

[6]. Дружинин В.В. Введение в теорию конфликта [Текст] / В.В. Дружинин, Д.С. Конторов, М.Д. Конторов. – М.: Радио и связь, 1989. – 288 с.

[7]. Дынкин Е.Б., Управляемые Марковские процессы и их приложения [Текст] / Е.Б. Дынкин, А.А. Юшкевич. – М.: «Наука», 1975. – 341 с.

[8]. Милокум Я.В. Моделі та методи забезпечення якості обслуговування у захищених комп'ютерних

мережах [Текст]: дис. … канд. техн. наук / Я.В. Милокум. – К., 2009. – 154 с.
[9]. Про основи національної безпеки України [Текст]: закон України від 19 червня 2003 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – С. 351.
[10]. Стратегія національної безпеки України [Текст]: офіц.текст: за станом на 8 червня 2012 р. // Офіційний вісник України – 2012. – 22 червня. – С. 104.
[11]. Howard R.A. System analysis of semi-Markov processes [Текст] / R.A. Howard // IEEE Transactions on Military Electronics – New York: Institute of Electrical and Electronics Engineers, 1964. – Issue 2, vol. 8. – P. 114–124.

REFERENCES

[1]. Venttsel Ye.S. *Issledovanyye operatsyy* [Analysis of operations]. Moscow: "Sovetskoye radio", 1972. 552 p.
[2]. Gnedenko B.V., Kovalenko I.N. *Vvedeniye v teoriyu massovogo obsluzhivaniya* [Introduction to mass servicing theory. 2-nd edition]. Moscow: "Nauka", 1987. 336 p.
[3]. Domarev V.V. *Bezopasnost ynformatsyonnykh tekhnologyy. Systemnyy podkhod* [IT security. The system approach]. Kyyiv: OOO "TID DS", 2004. 992 p.
[4]. Domarev D.V. Application of semi-Markov processes in design and state description of information security systems. *Systemy obrobky informatsiyi*. 2009; 7(79): 19-24.
[5]. Domarev D.V. Mathematical description of computer network attacking processes. *Problemy informatyzatsiyi ta upravlinnya*. 2010; 1(29): 50-54.
[6]. Druzhinin V.V., Kontorov D.S., Kontorov M.D. *Vvedeniye v teoriyu konflikta* [Introduction to conflict theory]. Moscow: "Radio i svyaz", 1989. 288 p.
[7]. Dynkin Ye.B., Yushkyevych A.A. *Upravlyayemiye Markovskiye protsessy i ikh prilozheniya* [Controlled Markov processes and their applications]. Moscow: "Nauka", 1975. 341 p.
[8]. Mylokum Ya.V. *Modeli ta metody zabezpechennya yakosti obslugovuvannya u zakhyschenykh kompyuternykh merezhah* [Models and methods for providing the quality of service in protected computer networks]: dissertation for Candidate of Technical Science (PhD) degree. Kyiv, 2009. 154 p.
[9]. *Pro osnovy natsionalnoyi bezpeky Ukrayiny* [About the basis of Ukraine's national security]: law of Ukraine of 19 June 2003. #964-IV
[10]. *Strategiya natsionalnoyi bezpeky Ukrayiny* [Strategy of Ukraine's national security]: official text of 8 June 2012.
[11]. Howard R.A. System analysis of semi-Markov processes. *IEEE Transactions on Military Electronics*. 1964; vol. 8, issue 2: 114-124.

МОДЕЛЬ КОНФЛИКТНЫХ СИТУАЦИЙ В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Проблема управления информационной безопасностью вытекает из необходимости поиска путей повышения эффективности функционирования информационных систем государства в современных условиях. Для выбора адекватных противодействий угрозам информационной безопасности и атакам следует применять модели взаимодействия сторон конфликта и модели конфликтных ситуаций в условиях неопределенности. Конфликтные ситуации в управлении информационной безопасностью государства смоделированы с применением стратегически-вероятностного подхода. Описан процесс конфликта как переменный процесс с двумя состояниями и известной матрицей переходов. Приведены формулы для расчета вероятностей интервальных переходов между состояниями атаки и защиты. Создана модель конфликтных ситуаций в управлении информационной безопасностью, которая благодаря формализации процесса реагирования системы управления информационной безопасностью на атаки дает возможность автоматизировано прогнозировать интервалы состояния безопасности и длительности возобновления систем информационной безопасности после атак.
Ключевые слова: теория конфликта, процесс конфликта, Марковский процесс, полумарковский процесс, система управления информационной безопасностью, СУИБ.

MODEL OF A CONFLICT SITUATION IN INFORMATION SECURITY MANAGEMENT

The problem of information security management emerged from the necessity to search for the ways to increase the efficiency of the state information systems functioning in modern conditions. To choose the adequate counteractions to the information security threats and attacks, it was recommended to apply the models of conflict parties' interaction and the models of conflict situations in the conditions of vagueness. Conflict situations in the information security management of the state were modelled using strategically-probabilistic approach. The process of conflict was described as a variable process with two states and known transition matrix. Formulas were derived to calculate the interval transition probabilities between the states of attack and defence. The model of conflict situations in information security management was created. Due to formalization of the process of information security management system reaction to attacks, the automated forecasting was achieved for the intervals of safety and information security recovery duration after attacks.
Keywords: conflict theory, conflict process, Markov process, semi-Markov process, information security management system, ISMS.

Домарєв Дмитро Валерійович, аспірант, Національний авіаційний університет,
E-mail: dimavsesvit@yahoo.com.
Домарев Дмитрий Валериевич, аспирант, Национальный авиационный університет.

Domarev Dmitry, postgraduate student of the National aviation university by speciality 21.05.01 «Information security of the State».

Милокум Яна Валеріївна, к.т.н., доцент, Національний авіаційний університет,

E-mail: Yana.Mylokum@gmail.com

Милокум Яна Валериевна, к.т.н., доцент, Национальный авиационный университет.

Mylokum Yana, PhD in technical sciences, Assossiate Professor, National aviation university.

UDC 621.391:519.7

ON THE COMPUTATIONAL SECURITY OF RANDOMIZED STREAM CIPHERS PROPOSED BY MIHALJEVIĆ AND IMAI

Anton Alekseychuk, Sergey Gryshakov

This paper yields a (computational) security analysis for a generic class of randomized stream ciphers based on joint employment of encryption, error-correction coding, and dedicated random coding. We show that the security of these ciphers can be considerably less than their designers claim. In contrast to the approach for security evaluation used before, our technique is significantly simpler and allows us to find out the code-theoretic sense of parameters that determine the security of these ciphers. We also propose another possible solution (based on nonlinear random coding) for design of randomized stream ciphers with enhanced security.

Keywords: *symmetric cryptography, randomized encryption, stream cipher, random coding, wiretap channel, LPN problem, correlation attack.*

1. Introduction

M. J. Mihaljević and H. Imai [8, 9, 11, 12] proposed a general approach for design of randomized stream ciphers based on joint employment of encryption, error-correction coding, and dedicated random (or homophonic) coding. One of the goals of designing such ciphers is to increase the security (without substantial performance reducing) of stream ciphers currently used in wireless communication systems, particularly, in the GSM standard. Another reason is to construct symmetric encryption schemes, whose security can be reduced to the hardness of some known mathematical problem such as the *Learning from Parity with Noise* (LPN) problem. Recall (see [6], for example) that this problem consists in solving a system of linear Boolean equations with equiprobable random coefficient matrix and the right-hand side corrupted by independent random variables taking values 0 and 1 with probabilities $1-\theta$ and θ, respectively, $\theta \in (0,1/2)$. In this case, we say that θ is the *noise level* in the right-hand side of the given system of linear equations.

In what follows, we focus our attention on the versions of randomized stream ciphers defined in [11, 12] and studied in detail in [10, 11, 13].

Let's denote by V_n the set of all n-dimensional Boolean vectors, by $F_{m\times n}$ the set of $m\times n$-matrices over the field $F=\mathbf{GF}(2)$, and by $F^*_{m\times m}$ the group of all invertible matrices of order m over this field.

According to [11, 12], the initial objects for a randomized stream cipher with parameters $l, m, n \in \mathbf{N}$, $p \in (0,1/2)$, where $l<m<n$, and a key space K are matrices $G_1 \in F_{m\times n}$, $G_2 \in F^*_{m\times m}$, and a keystream generator that produces a sequence $f_0(k), f_1(k), \ldots$ of n-dimensional Boolean vectors determined by a key $k \in K$. It is assumed that the functions $f_i : K \to V_n$, $i=0,1,\ldots$, can depend on some public parameters, for example, on initialization vectors (IV's). It is also assumed that G_1 is a generator matrix of a binary linear $[n,m]$-code C_1 with an efficient decoding algorithm, which is guaranteed to correct errors in the binary symmetric channel with crossover probability p.

To encrypt a plaintext $s_0, s_1, \ldots, s_t$, where $s_i \in V_l$, $i=0,1,\ldots,t$, with a key $k \in K$ the sender generates a sequence of independent random vectors $u_0, v_0, u_1, v_1, \ldots, u_t, v_t$, where u_i is uniformly distributed on the set V_{m-l}, and v_i is distributed according to Bernoulli's law with parameters (n,p), and computes the ciphertext $z_0, z_1, \ldots, z_t$ as follows:

$$z_i = (s_i, u_i)G_2G_1 \oplus f_i(k) \oplus v_i,\ i=0,1,\ldots,t. \quad (1)$$