УДК 004.056.55:004.056.53

Соловей В. А., молодший наук. співробітник
Житомирський військовий інститут ім. С. П. Корольова

МОДЕЛЮВАННЯ ОНТОЛОГІЧНО ЗАМКНЕНИХ КАНАЛІВ ЗВ'ЯЗКУ У КООРДИНАТНІЙ КРИПТОГРАФІЇ

У роботі розглядається модель онтологічно замкненого каналу зв'язку, сформованого у межах нової криптографічної парадигми – координатної криптографії (КК). На відміну від традиційних криптографічних систем, де основні функції безпеки реалізуються через зовнішні інфраструктури (ключі, центри сертифікації, цифрові підписи, хеш-механізми тощо), у КК базові властивості захищеної комунікації виникають як внутрішні властивості самої системи. У результаті система формує канал зв'язку, структурно замкнений відносно власних механізмів функціонування. Онтологічна замкненість означає, що система не потребує зовнішніх довірених інфраструктур для забезпечення конфіденційності, автентифікації та контролю цілісності інформації. Усі ці властивості виникають у парадигмі КК як наслідок фазової еволюції операційного стану системи та симетрії його розвитку у комунікуючих сторін. Шифрокод формується як координатне відображення об'єктів g_i у внутрішньому віртуальному просторі та виступає навігаційною інструкцією, реконструкція якої дозволяє знайти той самий об'єкт g_i у координатному просторі системи. Будь-якої іншої семантики, крім необхідної для реконструкції координатної події шифрокод не містить. Координатний простір є компонентом операційного стану системи $\mathcal{E}_t$. Він формується з об'єднання активної $\mathcal{A}_t$ та пасивної $\mathcal{P}_t$ множин об'єктів: $\mathcal{A}_t \cap \mathcal{P}_t = \emptyset,\ GIS_t = \mathcal{A}_t \cup \mathcal{P}_t$, при цьому обов'язково: $|\mathcal{A}_t| \ll |\mathcal{P}_t|$. Кожен об'єкт $g_i \in \mathcal{A}_t \cup \mathcal{P}_t$ має унікальні координатні параметри. Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом, який верифікується як «свій» (інакше – «чужий») тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0,1\}, \quad V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція LPA, а значення 1 відповідає прийняттю («свій»). LPA не потребує знання семантики відкритого тексту і базується виключно на логічній узгодженості структури шифрокоду з параметрами фазової симетрії системи. Шифрокод може бути верифікований лише системами з симетричним операційним станом: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow V_{S_t}(c) = accept$, що дозволяє зробити логічний висновок про автора шифрокоду. Нехай UA_t – компонент відкритого тексту, NA_t – внутрішній ентропійний вектор імітаційних даних, що використовується у випадках відсутності відкритого тексту та визначається розподілом $\mathcal{D}_{\mathcal{NA}}$, що забезпечує маскування структури повідомлення: $NA_t \sim \mathcal{D}_{\mathcal{NA}}$. Внутрішній вектор e_t та зовнішній вектор c_t однієї і тієї ж криптографічної події задаються відображеннями: $e_t = \Pi_t^{int}(UA_t, NA_t, \mathcal{E}_t), \quad c_t = \Pi_t^{ext}(UA_t, NA_t, \mathcal{E}_t)$, де Π_t^{int} – внутрішня

(латентна) проєкція, що формує подію e_t у вигляді множини бінарних векторів, Π_t^{ext} – зовнішня проєкція, що формує шифрокод c_t як спостережуване представлення криптографічного процесу. Еволюція $\mathcal{E}_t$ відображається: $\mathcal{E}_{t+1} = \Psi_t(\mathcal{E}_t, c_t)$, де Ψ_t – фазово-залежне стохастичне відображення, c_t – верифікований шифрокод (подія). Фазова еволюція незворотна та унікальна для кожної фази: $\forall i \neq j: \Phi_i \neq \Phi_j$. Звідси виникає фундаментальна властивість фазової антиколізійності шифрокодів, яка може бути записана у вигляді $m_i = m_j \Rightarrow c_i \neq c_j$, $c_i = c_j \Rightarrow m_i \neq m_j$. Цілісність відкритого тексту m також виникає як внутрішня властивість системи. Механізм верифікації цілісності тексту здійснюється у наступній події через LPA шифрокоду.

$Event_1 \subseteq$ {Боб відправив Алісі c_1 $B \to A : c_1$; A: $V_{S_1}(c_1) \in accept$; $c_1 \Rightarrow m_1$}. $Event_2 \subseteq$ {*Аліса*: $h_{m_1} = H(m_1)$; $c_2 = c_{r-1}(m_2) \oplus h_{m_1} \Rightarrow c_2 = F(m_2, n_2, S_2)$; $A \to B : c_2$; B: $V_{S_2}(c_2) \in accept$; $c_2 \Rightarrow m_2$}.

$Event_3 \subseteq$ {B: $h_{m_2} = H(m_2)$; $c_3 = c_{r-1}(m_3) \oplus h_{m_2} \Rightarrow c_3 = F(m_3, n_3, S_3)$; $Bob \to Alice : c_3$; Аліса : $V_{S_3}(c_3) \in$ accept; $c_3 \Rightarrow m_3$ }.

У події №3 – c_3 верифікований як «від Боба», враховуючи, що Аліса виконувала $h_{m_1} = H(m_1)$ та храповий механізм формування c_3, робиться логічний висновок, що $\big(receive(m_1) \wedge integrity(m_1)\big) \Rightarrow read(m_1)$.

Будь-яка модифікація шифрокоду порушує фазову симетрію систем та виявляється під час LPA. Контроль цілісності реалізується без використання зовнішніх механізмів на кшталт цифрових підписів або хеш-функцій. У загальному вигляді безпека такої системи визначається виключно еволюцією її внутрішнього стану: $Security = f(S_t)$.

Це означає, що безпека системи не залежить від зовнішніх криптографічних інфраструктур [1]. Формально цю властивість можна подати як незалежність безпеки від зовнішніх механізмів довіри:

$I(Security; ExternalInfrastructure) = 0$, де I(·;·) – взаємна інформація. Відповідно канал зв'язку, сформований у межах такої системи, можна визначити як онтологічно замкнений канал:

$$Ch_OC = \{C: Security(C) = f(S_t)\} \to I(Security; PKI) = 0.$$

Таким чином конфіденційність, автентифікація та контроль цілісності не потребують зовнішніх криптографічних артефактів і виникають як наслідок внутрішньої структури системи. Модель демонструє онтологічно замкнені канали зв'язку у яких безпека визначається не зовнішньою інфраструктурою довіри, а стохастичною еволюцією операційного стану. Системи безпеки, які ґрунтуються на онтологічно замкнених парадигмах комунікації є структурно стійкими до атак.

Список використаних джерел

1. Canetti R. Universally composable security: A new paradigm for cryptographic protocols // *FOCS*. – 2001. – P. 136–145.

2. Shannon C. A mathematical theory of communication // *Bell System Technical Journal*. – 1948. – Vol. 27. – P. 379–423.