УДК 004.056.55:004.056.53

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

## МЕТАДАНОНЕЙТРАЛЬНІ КАНАЛИ КОМУНІКАЦІЇ ТА КРАХ МОДЕЛІ СПОСТЕРЕЖЕННЯ

У роботі розглядається властивість метаданонейтральності каналів комунікації сформованих у межах нової криптографічної парадигми - координатної криптографії (КК). Це онтологічно замкнена модель закритої комунікації, у якій спостережувані характеристики передавання не містять інформації про факт та/або структуру інформаційного обміну між комунікуючими системи. Ця властивість є похідною від трьох структурних механізмів: послідовного обміну шифрокодами, використання імітаційних даних та логічної безпарольної автентифікації шифрокоду (LPA). Саме їх одночасна дія формує метаданонейтральні властивості каналу. На відміну від класичних систем, де первинною операцією є розшифрування повідомлення, у КК первинною операцією є логічна перевірка коректності шифрокоду відносно поточного операційного стану системи. 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 $\Pi_t^{int}$ – внутрішня (латентна) проєкція, що формує подію $e_t$ у вигляді множини бінарних

векторів, $\Pi_t^{ext}$ – 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 $\Psi_t$ – 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 $m_i = m_j \Rightarrow c_i \neq c_j$, $c_i = c_j \Rightarrow m_i \neq m_j$. Нехай $S_t \in \{UA_t, NA_t, UA_t \cup NA_t\}$ – джерело подій у системі, що визначає формування шифрокодів. Нехай $\{C_t\}_{t\in N}$ – випадковий процес шифрокодів, де $N$ – множина фаз. Тоді виконується рівність розподілів:

$$\mathcal{L}\left(\{C_t\}_{t\in N}^{(UA)}\right) = \mathcal{L}\left(\{C_t\}_{t\in N}^{(NA)}\right) = \mathcal{L}\left(\{C_t\}_{t\in N}^{(UA\cup NA)}\right),$$

де верхній індекс позначає джерело, що індукує процес. Тобто процес шифрокодів є статистично нерозрізнюваним відносно джерела їх формування [1]. Відповідно, для зовнішнього спостерігача взаємна інформація між шифрокодами та джерелом подій дорівнює нулю [2]: $I(c_t; S_t) = 0$. Закритий канал зв'язку для якого виконуються умови: нерозрізнюваність шифрокодів та інформаційна нейтральність комунікуючих сторін – є метаданонейтральним каналом зв'язку:

$$Ch_{MN} = \{\, channel \mid I(C; \{C_t\}_{t\in N}) = 0 \,\}.$$

Для зовнішнього спостерігача кожна подія формування шифрокоду $C_t$ статистично нерозрізнювана відносно спостереження [1] *Obs*, які доступні зовнішньому спостерігачу: $\forall t \in N : Pr(C_t \mid Obs) = Pr(C_t)$. Унаслідок цього спостереження каналу не дозволяє визначити, чи відбувався реальний інформаційний обмін: $Pr(C \mid \{C_t\}_{t\in N}) = Pr(C)$.

Тому для будь-якого алгоритму аналізу $A$ його перевага на основі спостереження каналу дорівнює нулю, тобто $\forall A : Adv_A(channel) = 0$. Таким чином зовнішній спостерігач не може встановити факт комунікації, її напрямок, структуру або обсяг переданої інформації. Як наслідок - модель спостереження втрачає розрізнювальну здатність, що призводить до колапсу моделі спостереження, яка фактично колапсує до тривіального випадкового процесу: $\{C_t\}_{t\in N} \sim \mathcal{L}$.

Таким чином КК формує нову криптографічну парадигму та відповідний клас каналів зв'язку – метаданонейтральні закриті канали комунікації. Метаданонейтральні властивості виникають як природний наслідок структурної організації системи. Безпека моделі не спирається на ключі чи паролі, а визначається онтологічною замкненістю системи, стохастичною природою формування шифрокодів та відсутністю спостережуваних структур, які могли б виступати об'єктами атак.

**Список використаних джерел**

1. Goldwasser S., Micali S. Probabilistic encryption // *Journal of Computer and System Sciences*. – 1984. – Vol. 28. – № 2. – P. 270–299.

2. Serjantov A., Danezis G. Towards an information theoretic metric for anonymity // Privacy Enhancing Technologies. – 2002. – P. 41–53.