УДК 004.056.55:004.056.53

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

ФАЗОВО-ЕВОЛЮЦІЙНІ КРИПТОГРАФІЧНІ СИСТЕМИ: ФОРМАЛЬНА БЕЗКЛЮЧОВА МОДЕЛЬ

У роботі розглядається формальна модель нового класу криптографічних систем – фазово-еволюційних криптографічних систем (ФЕКС), що функціонують без використання криптографічних ключів. На відміну від традиційних криптографічних моделей, де безпека визначається секретністю або складністю відновлення ключа, у ФЕКС безпека системи визначається еволюцією її внутрішнього операційного стану [1]. Така модель є фундаментальною для координатної криптографії та інших систем, у яких криптографічні властивості визначаються динамікою внутрішніх процесів системи. У класичній криптографії формування шифротексту описується відображенням виду $c = Enc(m, k)$, де m – відкрите повідомлення, а k – криптографічний ключ. Формально у ФЕКС процес формування шифрокоду можна подати як $c_t = F(m_t, n_t, \mathcal{E}_t)$, $\mathcal{E}_t$ – операційний стан системи у фазі t, m_t – компонент відкритого тексту, n_t – вектор імітаційних даних $\mathcal{NA}$, F – відображення формування шифрокоду. $\mathcal{NA}$ – це внутрішній ентропійний вектор, що використовується у випадках відсутності відкритого тексту, для маскування структури повідомлення: $n_t \sim \mathcal{D}_{\mathcal{NA}}$, де $\mathcal{D}_{\mathcal{NA}}$ – розподіл ентропійних векторів імітаційних даних [2]. Формально ФЕКС ($\mathcal{C}_{\mathcal{PE}}$) можна визначити як клас систем:

$$\mathcal{C}_{\mathcal{PE}} = \{system \mid c_t = F(m_t, n_t, \mathcal{E}_t),\ \mathcal{E}_{t+1} = \Psi(\mathcal{E}_t, c_t),\ k = \emptyset\}.$$

Це означає, що криптографічне перетворення визначається еволюцією операційного стану системи. Симетрія $\mathcal{E}_t$ та стохастична симетрична еволюція $\mathcal{E}_{t+n}$ комунікуючих систем є необхідною умовою для ФЕКС. Симетрія виникає як властивість еволюції операційного стану систем. Механізмом синхронізації комунікуючих систем є логічна безпарольна автентифікація (LPA) шифрокоду. Формально процедура описується як : $V_{\mathcal{E}_t}(c_i) \in \{0,1\}$, де результат 1 означає, що структура шифрокоду узгоджується з поточним операційним станом системи. На відміну від класичних систем автентифікації, не використовує ключі, паролі або цифрові підписи. Якщо дві системи мають симетричні операційні стани, то шифрокод, сформований однією системою, може бути коректно верифікований іншою: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow V_{\mathcal{E}_t}(c) = 1,\ \forall t.$

Симетрія операційних станів підтримується через послідовну фазову еволюцію систем, та визначається однаковими верифікованими подіями:

$$\mathcal{E}_{t+1}(A) = \Psi(\mathcal{E}_t(A), c_t),\ \mathcal{E}_{t+1}(B) = \Psi(\mathcal{E}_t(B), c_t).$$

Синхронізація систем не потребує використання криптографічних ключів - роль ключа виконує симетричний операційний стан систем.

Операційний стан $\mathcal{E}_t$ є комплексним параметром системи та включає фазові параметри еволюції, подієву пам'ять обмеженої фазової глибини

H_t, а також координатне представлення криптографічних об'єктів. Кожна подія формування або реконструкції за умови верифікації шифрокоду змінює подальшу траєкторію розвитку системи. Фундаментальною властивістю ФЕКС є унікальність фаз еволюції. Якщо позначити фазовий стан системи через Φ_t, то для будь-яких різних моментів часу виконується $\forall i \neq j$: $\Phi_i \neq \Phi_j$. Це означає, що операційний стан системи не може бути повторений. Наслідком унікальності фаз є властивість фазової антиколізійності шифрокодів. Для будь-яких двох подій виконується $m_i = m_j \Rightarrow c_i \neq c_j$ та $c_i = c_j \Rightarrow m_i \neq m_j$. Таким чином однакові повідомлення не можуть породжувати однакові шифрокоди, але однакові шифрокоди – як правило сформовані різними текстами, не залежно від їх фазової належності. Саме тому автентифікація автора шифрокоду через механізм ЛБА – виникає як логічний наслідок симетрії фазової еволюції систем, а не як результат використання криптографічних ключів, паролів чи будь-яких інших цифрових ідентифікуючих даних.

Оскільки еволюція операційного стану залежить від історії подій у декількох попередніх фазах, траєкторія еволюції має немарковський характер [1]. Поточний стан системи визначається не лише попереднім станом, а всією історією подій, накопичених у подієвій пам'яті H_t яка не збільшується за розміром, а змінює свій стан. Кожна верифікована подія фази t є безумовною, змінює стан H_t невідкладно, але не впливає на її розмір. Умовні події – навпаки, накопичується у H_t, змінюють її стан тільки після виконання умови, що пов'язана із ймовірнісним очікуванням геометричних параметрів $\mathcal{E}_{t+n}$, де n – невідома: $\exists n \in N$: умова$(\mathcal{E}_{t+n})$.

Кількість попередніх фаз $d_t = |\varphi_i : i < t|$, умови яких зберігаються у H_t обмежена її фазовою глибиною у поточній фазі та може бути змінена. Формально це можна подати як $\mathcal{E}_t = f(\mathcal{E}_{t-1}, H_t)$. Отже поведінка системи визначається накопиченою історією криптографічних подій.

Формально безпеку можна подати як функцію $\mathcal{E}_t$: $Security = f(\mathcal{E}_t) \Rightarrow$ Security $\notin KeySpace$. Криптографічна стійкість є наслідком динаміки внутрішніх процесів та симетричної еволюції операційного стану систем. Конфіденційність, автентифікація та цілісність інформації виникають як внутрішні властивості системи, а не як результат використання зовнішніх криптографічних інфраструктур: $Enc(m, key)$, $Enc(m, \mathcal{E}_t) \Rightarrow key \equiv \mathcal{E}_t$. Дешифрування: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow Dec\big(F(m_t, \mathcal{E}_t)\big) = m_t$, $\mathcal{E}_t \notin KeySpace$.

Стохастична немарковська еволюція $\mathcal{E}_t$ виконує роль динамічного криптографічного параметра, тому: $Security \not\equiv Key$, оскільки ключ формує тільки один операційний стан із всієї множини можливих.

Список використаних джерел

1. Bellare M., Rogaway P. Introduction to modern cryptography // *UCSD Notes*. – 2005.
2. Cover T. M., Thomas J. A. Elements of Information Theory. – Wiley, 2006.