- поява пасивних ворожих створінь увечері та їхня активізація на початку ночі;
- поведінка ворожих створінь;
- можливість ховатись у високій траві, тим самим збільшуючи шанси пережити ніч.

Список використаних джерел

1. Elite (video game). URL: https://en.wikipedia.org/wiki/Elite_(video_game)
2. What is better game engine: is Unity right for you? URL: https://www.gamesindustry.biz/articles/2020-01-16-what-is-the-best-game-engine-is-unity-the-right-game-engine-for-you

ПЕРЕВІРКА НА КОЛІЗІЙНІСТЬ ГЕШ-КОДІВ ЯКІ СФОРМОВАНО ЗА ДОПОМОГОЮ АЛГОРИТМУ UMAC НА КРИПТО-КОДОВИХ КОНСТРУКЦІЯХ

[1]***Євсеєв С. П.***, [1]***Гаврилова А. А.***
[1]*Харківський національний технічний університет «ХПІ», м. Харків*

В доповіді проведено аналіз колізійних властивостей кодів автентифікації повідомлень, отриманих за допомогою зменшеної моделі UMAC (mini-UMAC). Дані властивості пов'язані з експериментальною оцінкою розподілу кількості зіткнень (колізій) образів, що формуються. За допомогою зменшених моделей досліджено основні показники ефективності криптоалгоритму при збереженні його алгебраїчної структури [1].

Оскільки в алгоритмі UMAC на першому шарі формування геш-коду використовуються сімейства універсальних гешуючих функцій [2–4], статистичні дослідження проводилися на другому шарі при формуванні псевдовипадкової підкладки та на заключному етапі формування кодів автентифікації (після виконання підсумовування). Саме на цих етапах, за припущенням авторів [5] і порушуються властивості універсальності кодів автентифікації, що формуються.

При проведенні статистичних досліджень колізійних властивостей значень геш-кодів, що формуються, для кожного експерименту оцінювалися за математичними очікуваннями $m(n_1)$, $m(n_2)$ та $m(n_3)$ (табл. 1).

Таблиця 1

Значення математичних очікувань колізійних властивостей кодів автентифікації

Математичні очікування	MASH -1	MASH -2	mini-UMAC MASH-1	mini-UMAC MASH-2	mini-UMAC AES	mini-UMAC KKK
$\widetilde{m}(n_1)$	*7,09**	*7,14**	1,965	1,968	1,096	1,166
$\widetilde{m}(n_2)$	1,013	1,014	2,629*	2,64*	1,532	1,161
$\widetilde{m}(n_3)$	1,0008	1,0002	0,237	0,224	0,0005	0

За значеннями математичних очікувань коди, які сформовано за всіма алгоритмами, не відповідають першому критерію універсальності, оскільки кількість колізій перевищує задану межу $n_1(x_1,x_2) \le P_{кол} \cdot |H| = 1$ [1]. Так, за алгоритмами шифрування MASH-1 і MASH-2 кількість колізій перевищує теоретичну межу більш ніж у 7 разів.

Отримані експериментальним шляхом результати свідчать про те, що колізійні властивості кодів автентифікації, які сформовано з використанням алгоритмів mini-MASH-1 та mini-MASH-2, не задовольняють і другому критерію ($|H|/|B| = 1$ [1]), оскільки кількість колізій за ними перевищує теоретичну межу майже в 3 рази, а по решті алгоритмів також спостерігається перевищення допустимої кількості колізій. Отже, перший критерій суворої універсальності не виконується жодним з алгоритмів.

У відповідності до третього критерію ($n_3(x_1,x_2,y_1,y_2) \le P_{кол} \cdot |H| = 1$ [1]) отримані значення свідчать про те, що колізійні властивості кодів автентифікації, які сформовано з використанням mini-MASH-1, mini-MASH-2, mini-UMAC AES та mini-UMAC KKK задовольняють другий критерій суворої універсальності.

Таким чином, за розрахунковими значеннями, отриманими за допомогою програмного додатку виявлено, що вимогам суворо універсального класу створення геш-кодів відповідають геш-коди, які сформовано за допомогою алгоритмів mini-UMAC MASH1, mini-UMAC MASH2, mini-UMAC AES та mini-UMAC KKK.

Список використаних джерел

1. Hryshchuk R., Yevseiev S., Shmatko, A. Construction methodology of information security system of banking information in automated banking systems: monograph. – Vienna.: Premier Publishing s. r. o., 2018. – 284 p.

2. Кузнецов А.А., Король О.Г., Босько В.В. Модель формирования кодов аутентификации сообщений с использованием универсальных хеширующих функций // Збірник наукових праць «Системи обробки інформації». Харків: Харк. нац. ун-т Повітр. Сил ім. Івана Кожедуба, 2011. № 3 (93). С. 117 – 125.

3. Евсеев С.П., Король О.Г., Огурцов В.В. Усовершенствованный алгоритм UMAC на основе модулярных преобразований // Восточно-Европейский журнал передовых технологий. Харьков, 2014. № 1/9 (67). С. 16 – 23.

4. Король О.Г. Использование коллизионных свойств кодов аутентификации сообщений UMAC // VIII Міжнародна науково-практичної конференції «Проблеми і перспективи розвитку ІТ-індустрії». Харків: Харк. нац. ун-т Повітр. Сил ім. Івана Кожедуба, 2010. № 7 (88), С. 221.
5. Король О.Г., Кузнецов А.А., Евсеев С.П. Исследование коллизионных свойств кодов аутентификации сообщений UMAC // Науч.-техн. журнал «Прикладная радиоэлектроника». Харків: ХНУРЕ, 2012. Т. 11, № 2, С. 171–183.

КОНЦЕПЦІЯ ФОРМУВАННЯ СОЦІОКІБЕРФІЗИЧНИХ СИСТЕМ

[1]***Євсеєв С. П.***, [1]***Король О. Г.,*** [1]***Воропай Н. І. ,*** [2]***Бондаренко К. О.***
[1] Національний технічний університет "Харківський політехнічний інститут", м. Харків
[2]*Харківський національний економічний університет ім. С. Кузнеця, м. Харків*

В умовах стрімкого зростання обчислювальних можливостей мобільних технологій та створення на їх базі бездротових Mesh-, сенсорних-мереж, технологій Інтернет-речей, smart-технологій актуальною проблемою стає забезпечення безпеки інформації. При цьому виникає необхідність розгляду безпеки у двох контурах внутрішньому (безпосередньо всередині інфраструктури мережі) та зовнішньому (хмарних технологіях). У таких умовах необхідно комплексувати загрози як на внутрішній контур безпеки, так і на зовнішній контур. Це дозволяє не лише враховувати гібридність та синергізм сучасних цільових загроз, але й враховувати рівень значущості (ступінь секретності) інформаційних потоків та інформації, що циркулює як у внутрішньому, так і зовнішньому контурі безпеки [1–3].

Для забезпечення безпеки сучасних бездротових мереж та систем, заснованих на їх інфраструктурі, необхідно враховувати комплексування внутрішньої інфраструктури елементів мережі (внутрішній контур) та зовнішньої інфраструктури управління, що базується на хмарних платформах.

Синтез внутрішнього та зовнішнього контурів забезпечує оперативність, енергомісткість та відносну безпеку (кожен контур будує безпеку на своїх механізмах та принципах), з одного боку. З іншого боку, відсутні можливості контролю не лише механізмів безпеки, що використовуються, а й оцінки поточного стану захищеності інформаційних потоків, що циркулюють та зберігаються в контурі [4].

Системи безпеки соціокіберфізичних систем у більшості випадків орієнтовані на об'єкти критичної інфраструктури (банківсько-фінансовий сектор, паливно-енергетичний комплекс, мережі життєзабезпечення, телекомунікації та мережі зв'язку, комплекс безпеки та оборони тощо). Для забезпечення безпеки таких систем необхідно враховувати два класи загроз. Перший клас – це загрози та їхнє комплексування з методами соціальної інженерії внутрішньої інфраструктури (внутрішній контур безпеки). Другий клас – загрози зовнішнього контуру (хмарні технології, які забезпечують не тільки управління