Послідовності MA, MB, MC, MD шифруються за допомогою правил ДНК шифрування і отримуються матриці DA, DB, DC, DD,значення яких змінюються за формулою 2, в наслідок чого отримується зашифроване зображення.

Процес розшифрування є зворотнім до процесу шифрування і відрізняється тільки заміною операції додавання на віднімання послідовностей ДНК [5].

Отже, розглянутий алгоритм є досить стійким і надійним серед більшості інших криптографічних алгоритмів, оскільки при такому підході ключ генерується з використанням гіперхаотичної системи рівнянь Росслера, і застосуванням алгоритму ДНК заміщення.

Список використаних джерел:

1. Patel D. K. Image Encryption Using Different Techniques: A Review / Patel D. K., Belani S.; International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol. 1, Issue 1, November 2011. – Pp. 30-34.

2. Kwok H. S. A Fast Image Encryption System based on Chaotic Maps with Finite Precision Representation 32 / Kwok H. S., Tang W. K. S.; Chaos Solitons and Fractals, 2007. – Pp. 1518–1529.

3. Soni R. An Encryption and Decryption Algorithm for Image Based on DNA / Soni R. Johar, A., Soni V.; International Conference on communication systems and network technologies (CSNT), April 2013. – Pp. 478-481,

4. Rössler O. E An equation for hyperchaos; Physics Letters A, 1979. – Pp. 155-157.

5. Niu H. Splicing model and hyper-chaotic system for image encryption / Niu H., Zhou C., Wang B., Zheng X., Zhou S.; Journal of Electrical Engineering. Volume 67, Issue 2 May 2016. – Pp. 78–86.

Даниляк В.І.
студент;
Науковий керівник: **Вовк Р.Б.**
кандидат технічних наук,
Івано-Франківський національний технічний університет нафти і газу

ОПИС ТА КЛАСИФІКАЦІЯ ОСНОВНИХ МЕРЕЖЕВИХ АТАК ТА МЕТОДІВ ЗАХИСТУ ВІД НИХ

Мережевий захист – це динамічна галузь, яка стрімко розвивається, проте, не дивлячись на це, все частіше в заголовках новин зустрічається термін «мережеві атаки». Мережеві атаки – це певні дії, метою здійснення яких є отримання контролю над комп'ютерною системою або порушення її роботи, а також захоплення даних користувача. Актуальність захисту пристроїв у мережі з плином часу лише зростає, так згідно зі статистикою Qrator Labs [1] кількість лише DDoS-атак в першій половині 2015 становила 9347 в порівнянні з 2715 у 2014 році за аналогічний період.

Існує багато видів мережевих атак і захисту від них, вибір способу захисту залежить від багатьох факторів, таких як топологія мережі, протокол з'єднання та інше. Сьогодні багато людей, незалежно від їх сфер діяльності перебувають

під ризиком атак у інтернеті, а кількість комп'ютерів заражених шкідливим програмним забезпеченням невпинно зростає. У зв'язку з цим є актуальним дослідження мережевих протоколів, шкідливих програм, технологій захисту та методів виявлення несанкціонованого доступу.

Спершу розглянемо найбільш вживані мережеві протоколи. Інтернет-протокол (Internet protocol, IP) – це незалежний протокол, що передає пакети даних від одного комп'ютера до іншого. IP версії 4 (IPv4) використовує 32-бітні IP-адреси, які часто записуються у вигляді чотирьох десяткових чисел в діапазоні від 0 до 255, наприклад 194.95.9.96. Після того як кількість можливих адрес IPv4 у 2011 році досягла 4 мільярдів, було здійснено перехід до нової версії IP-протоколу: IPv6, яка використовує 128-бітні адреси [2]. Більшість інтернет-сервісів використовують протокол керування передачею (Transmission control protocol, TCP), який забезпечує віртуальні канали. TCP розбиває потік даних в IP-пакети і повторно збирає в кінці з автоматичним перенаправленням всіх пакетів, отримання яких не підтверджується.

Мережеві протоколи щодня піддаються атакам з боку зловмисників, одними з яких є:

- DoS (denial-of-service) атаки, суть яких полягає у надсиланні зловмисниками великої кількості SYN-запитів на пристрій «жертви». SYN-запити – це запити, які передаються по протоколу TCP, а у відповідь, сервер чекає ACK (acknowledge), тобто підтвердження від зловмисник. Відповідно він, просто, ігнорує ці запити і цими діями переповняє на сервері чергу на підключення. Таким способом, клієнти цього сервера не зможуть встановити з ним зв'язок або встановлять з суттєвою затримкою.
- Розподілена Dos або DDos-атака (Distributed Denial-of-service) – це атака для здійснення якої зловмиснику необхідно попередньо заразити велику кількість комп'ютерів шкідливим програмним забезпеченням. Після цього він може дати повідомлення зараженим комп'ютерам дял надсилання запитів на певну комп'ютерну систему чи сервер. Найчастіше цілями DDos-атак є великі корпорації.
- IP спуфінг (IP Spoofing) – можливість отримання несанкціонованого доступу до комп'ютера, суть якого полягає в тому, що зловмисник змінює значення поля source в IP-пакеті, що маскує його фізичний адрес. Переважно, IP спуфінг застосовується перед більш суттєвими атаками.

Досить розповсюдженими також є мережеві атаки на локальну мережу. У випадку контролювання зловмисниками хоча б одного з комп'ютерів у локальній мережі, вони можуть отримати доступ до різного роду конфіденційної інформації, наприклад, до користувацьких паролей, особистих даних працівників компанії і т.п.. Для цього можуть використовуватися сніффери, тобто програмне забезпечення, яке застосовується для діагностики мережі. Завданням сніфферів є аналіз всього трафіку, який проходить через локальну мережу.

Найбільш поширеним способом захисту протоколів від атак є мережевий екран або фаєрвол (Firewall) – спеціалізоване програмне забезпечення, яке призначене для фільтрації трафіку, що проходить між локальною мережею та Інтернетом. Таким чином, шкідливі пакети викидаються або модифікуються до

безпечного стану. В залежності від виду фільтрації, розрізняють наступні основні 3 типи фаєрволи:

1. Пакетні фільтри (Packet Filtering) – фільтрують пакети адрес і номери портів, і практично не впливають на маршрутизацію, тобто не зменшують продуктивність маршрутизатора.

2. Шлюз сеансового рівня (Circuit Gateways) – працює на рівні TCP, відслідковуючи процес встановлення TCP-зв'язку, що дозволяє з'ясувати, чи поточний сеанс є авторизованим. До переваг даного типу відноситься несуттєвий вплив на швидкість маршрутизації, проте шлюзи сеансового рівня не можуть фільтрувати окремі пакети.

3. Шлюз прикладного рівня (Application Relays) – виступає в якості проксі-сервера. Прикладами є поштові фільтри, які відсіюють спам або веб-проксі сервери, які блокують або видаляють небажаний контент. Фаєрволи такого типу забезпечують більш якісний захист мережі, проте негативно впливають на швидкість маршрутизації.

Таким чином, у даному дослідженні розглянуто основні види мережевих протоколів, атак та способів захисту від них.

Список використаних джерел:

1. Вебсайт xakep [Електронний ресурс]. – Режим доступу: https://xakep.ru/2015/09/14/ddos-runet/

2. Ross J. Anderson – University of Cambridge, 2008. – 1080 pages. – (Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition).

Дегтярёв А.Г.

студент;

Яшков И.О.

кандидат технических наук, доцент,

Харьковский национальный университет радиоэлектроники

ЗАКОН МУРА КАК ВЕКТОР РАЗВИТИЯ ПОЛУПРОВОДНИКОВОЙ ПРОМЫШЛЕННОСТИ

Закон Мура – эмпирическое наблюдение, сделанное Гордоном Муром (Gordon Moore), согласно которому количество транзисторов, располагающихся на одном кристалле интегральной схемы, увеличивается в два раза каждые 2 года (24 месяца) [1].

Актуальность данного закона наблюдалась более 40 лет. В 2007 году Мур заявил о том, что закон перестанет действовать из-за атомарного происхождения веществ, а также ограничение скорости света. Основным физическим ограничением для миниатюризации электронных схем является Принцип Ландауэра, который гласит, что в любой вычислительной системе, независимо от её физической реализации, при потере 1 бита информации выделяется теплота в количестве по крайней мере W джоулей:

$$W = k_B T \ln 2,$$