E-mail: m.romanenko1994@gmail.com.
Orcid ID: 0000-0002-0646-2797.

Болотюк Юлія Володимирівна, ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені героїв Крут

Yuliia Bolotiuk, adjunct (postgraduate) of the Scientific and organizational department of the Military Institute of Telecommunications and Informatization named after the Heroes of Kruty.
E-mail: yuliia.bolotiuk@viti.edu.ua.
Orcid ID: 0000-0002-3805-6419.

DOI: 10.18372/2410-7840.25.17935
УДК 004.056.5

МЕТОДОЛОГІЯ МАСКУВАННЯ ТРАФІКУ У СПЕЦІАЛІЗОВАНІЙ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ

Сергій Клімович

У зв'язку зі зростаючими загрозами в кібербезпеці, існує необхідність в розробці нових підходів (нової методології) маскування трафіку для уникнення виявлення та аналізу трафіку з боку несанкціонованих осіб. Маскування трафіку дозволяє приховувати характеристики переданих даних, такі як джерело, призначення, тип та об'єм, шлях та інші метадані, що надають змогу ідентифікувати та аналізувати комунікацію. Це може бути особливо корисним у випадках, коли необхідно зберегти приватність користувачів або запобігти виявленню конфіденційної інформації. Сучасні методи аналізу трафіку постійно вдосконалюються, тому виникає потреба в розвитку нових підходів до маскування у відповідності до змін в технологіях аналізу даних. Актуальність роботи пов'язана з тим, що дії адміністратора спеціалізованої мережі щодо забезпечення безпеки її функціонування спрямовані на розв'язання двох взаємопов'язаних завдань, а саме: забезпечення скритного функціонування мережі і виявлення фактів стороннього втручання (виявлення дій сторонніх осіб). Обидва завдання суворо регламентовані керівними документами, но кінцевий результат залежить від глибини розуміння посадовою особою існуючої проблеми, ступеня володіння методологією забезпечення безпеки функціонування спеціалізованої мережі, наявних матеріальних (в тому числі фінансових) засобів та наявного часового ресурсу. В роботі проведено аналіз існуючих підходів до забезпечення маскування трафіку в мережі, наведено алгоритми (варіанти програмної реалізації) механізмів маскування та виявлення факту маскування трафіку в спеціалізованій мережі передачі даних.

Ключові слова: *маскування трафіку, конфіденційність, математичні моделі, Shadowsocks.*

ВСТУП

Забезпечення конфіденційності та безпеки переданих даних є одним із найважливіших аспектів у сучасному цифровому світі. З постійним розвитком технологій та зростаючою кількістю глобальних мереж і пристроїв, виникає все більше загроз, пов'язаних зі зловживанням та несанкціонованим доступом до інформації. Це ставить під загрозу приватність користувачів, безпеку установ, а також може мати серйозні наслідки для суспільства в цілому. Як наслідок, застосування та обмін інформацією стають все більш розповсюдженими в різних сферах життя. У цьому контексті, конфіденційність та безпека переданих даних є критичними аспектами для забезпечення довіри між користувачами, установами та системами. Зловживання та несанкціонований доступ до даних може призвести до розголошення конфіденційної інформації, що завдасть значних фінансових збитків та спричинить порушення роботи установ.

Аналіз публікацій свідчить про постійний інтерес та активні дослідження в цій галузі. Дослідники та фахівці з кібербезпеки, мережевих технологій та інформаційної безпеки присвячують значний обсяг робіт з розробки та вдосконалення методів маскування трафіку з метою забезпечення конфіденційності та безпеки передачі даних. Публікацій у цій області [1-3] присвячені вивченню різних аспектів маскування трафіку, таких як алгоритми шифрування, обфускація даних, зміна характеристик трафіку, використання тунелювання. Ці дослідження спрямовані на розробку ефективних та надійних методів, які дозволяють приховати характеристики переданих даних від зловмисників.

Водночас ряд учених присвятили свої дослідження [4-8] аналізу технік розпізнавання трафіку,

які використовуються зловмисниками для ідентифікації та аналізу комунікації. Вони пропонують нові підходи до виявлення та захисту від таких методів розпізнавання, а також вивчають вплив різних факторів, таких як обсяг даних, часові параметри, структура пакетів на результати аналізу трафіку.

Крім того, велика увага приділяється використанню машинного навчання та штучного інтелекту для вдосконалення методів маскування трафіку.

Таким чином, аналіз останніх досліджень і публікацій за визначеною темою показав, що вивчення особливостей маскування трафіку дає змогу вироблення ефективних механізмів маскування та виявлення факту маскування трафіку в спеціалізованій мережі передачі даних.

ОСНОВНА ЧАСТИНА

Для забезпечення конфіденційності та безпеки переданих даних у спеціалізованій мережі використовується низка відомих організаційних та технічних рішень, а саме:

- шифрування даних як процес використання спеціальних алгоритмів, що запобігає однозначному сприйняттю противником перехопленої інформації;
- технологія VPN мережі для безпечного з'єднання віддалених вузлів через інтернет шляхом створення захищеного тунелю;
- спеціальні програми (файрволи, антивіруси) для блокування небажаного трафіку та запобігання атакам;
- процеси автентифікації користувача та його прав на доступ до певних ресурсів мережі (ідентифікація та аутентифікація);
- спеціальні сервери (проксі сервери) для приховання IP-адреси клієнта та його розташування;
- протоколи передачі гіпертексту (HTTPS) для захисту паролю та логіну при передачі конфіденційної інформації.

Кожне з зазначених рішень має свої особливості, і вибір того чи іншого рішення (комплексне їх застосування) з урахуванням наявності обов'язкових до виконання нормативних документів, рівня підготовки спеціаліста та передбачуваного значення обраного критерію оцінки функціонування системи захисту.

Одним із варіантів забезпечення безпеки в спеціалізованій мережі є метод маскування трафіку. Методологія (програми, алгоритми, методи), яка можлива до застосовування під час маскування трафіку однаково доступна як зловмисникам, так і адміністраторам мережі. Метод маскування трафіку має кілька переваг над іншими організаційно-технічними методами оскільки виконується факт приховання передачі даних між вузлами мережі. Одночасно, маскування трафіку може бути більш надійним, оскільки дозволяє приховувати інформацію про дані в умовах, коли інші методи захисту були скомпрометовані.

Однак, цей метод не є універсальним методом захисту інформації і має ряд недоліків (може бути більш складним у налаштуванні та управлінні, ніж інші методи і може вимагати більшої кількості ресурсів для його реалізації). Крім того, метод не гарантує 100% захист від атак і може бути скомпрометований за наявності відповідних інструментів та знань у зловмисників.

Одним із варіантів застосування методу маскування трафіку є його використання для обходу блокування інтернет-ресурсів, на які накладено обмеження (у певній країні чи регіоні). Користувачі можуть використовувати маскування трафіку для того, щоб приховувати свою реальну IP-адресу та отримати доступ до заблокованих ресурсів.

В умовах інтенсивного розвитку технологій штучного інтелекту (ШІ) забезпечення безпеки передачі даних у спеціалізованих мережах стає більш складною задачею, що призводить до нового рівня протиборства між захисниками та зловмисниками:

- машинне навчання для виявлення аномалій трафіку в реальному масштабі часу;
- виявлення загроз безпеки та визначення найбільш ефективних методів маскування трафіку в конкретному випадку (відкриті бібліотеки машинного навчання та аналізу даних (TensorFlow, PyTorch, Scikit-learn));
- використання генеративних моделей, таких як генеративні змагальні мережі (GAN) для генерації хибного трафіку;
- використання нейронних мереж для шифрування трафіку.

Оцінку ефективності методу маскування трафіку (вибір критерію оцінки) необхідно проводити залежно від цілей, яких планується досягти.

Якщо пріоритетним напрямком є захист конфіденційності даних, то критерій захисту конфіденційної інформації має бути переважаючим. Якщо потрібно скоротити обсяг трафіку (скоротити час активності мережі), то метрика зниження обсягу трафіку буде важливішою. Таким чином, оцінка ефективності методу маскування трафіку може проводитись за наступними критеріями:

- складність аналізу трафіку. Оцінюється складність процесу аналізу маскованого трафіку для зловмисників. Чим вище складність, тим ефективнішим вважається метод маскування. Оцінка складності може бути виконана шляхом порівняння часу та ресурсів, необхідних для аналізу маскованого та не маскованого трафіку;
- захист від розкриття особистої інформації. Оцінюється, наскільки успішно метод маскування трафіку захищає конфіденційну інформацію користувачів. Вона може бути оцінена, за допомогою тестування на проникнення, де зловмисникам дається доступ до зашифрованих даних та оцінюється їхня здатність декодувати ці дані;
- зниження обсягу трафіку. Ця метрика оцінює, наскільки успішно метод маскування трафіку може знизити обсяг трафіку, який пересилається мережею. Чим менший обсяг трафіку, тим менша ймовірність того, що зловмисник виявить конкретні дані;
- надійність та доступність. Надійність може бути виміряна шляхом оцінки ймовірності виникнення помилок під час використання методу. Доступність може бути оцінена шляхом вимірювання часу, необхідного для встановлення та налаштування методу.

Кількісно, оцінити ефективність застосованого методу можна через показник:

- успішної передачі даних (Successful Delivery Ratio, SDR), який є відношенням числа успішно доставлених пакетів до загального числа переданих пакетів в мережі:

$$SDR = N_{у} / N_{з},$$

де $N_{у}$ – число успішно доставлених пакетів, $N_{з}$ – загальна кількість переданих пакетів;

- ймовірності виявлення трафіку ($P_{і}$):

$$P_{і} = N_{в} / N_{з},$$

де $N_{в}$ – число виявлених пакетів, $N_{з}$ – загальна кількість переданих пакетів.

При функціонуванні мережі в умовах обмеження часу на прийняття рішень (обмеження часу існування актуальної інформації), на перше місце виходить критерій часу.

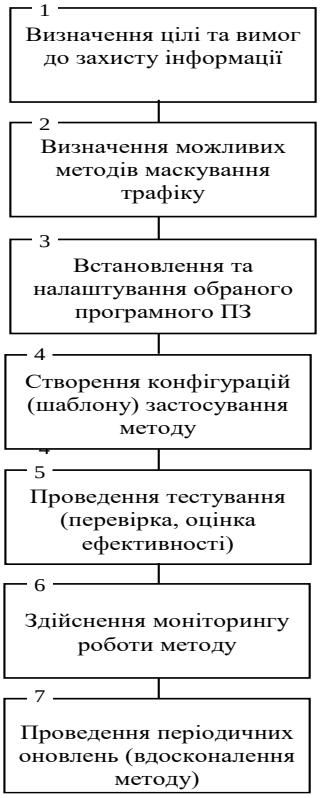

Рис. 1. Алгоритм дій адміністратора мережі для реалізації методу маскування трафіку

На сьогодні відомі наступні математичні моделі оцінки ефективності методу маскування трафіку:

- модель оцінки безпеки мережі з урахуванням теорії інформації. У цій моделі мірою ефективності методу маскування трафіку є кількість інформації, яку зловмисник може отримати із зашифрованого трафіку. Міра може бути виражена через ентропію трафіку;
- модель оцінки складності аналізу трафіку з урахуванням методів машинного навчання. У цій моделі мірою ефективності є складність алгоритму, який буде необхідний для аналізу маскованого трафіку. Для оцінки складності можуть використовуватися методи машинного навчання, такі як класифікація та кластеризація;
- модель оцінки часу, необхідного для злому системи. У цій моделі мірою ефективності є час, необхідний зловмиснику для злому системи, захи-

щеної методом маскування трафіку. Для оцінки часу можна використовувати методи аналізу тимчасової складності алгоритмів.

Алгоритм дій адміністратора мережі для реалізації методу маскування трафіку може мати наступний вид (рис. 1).

На сьогодні відоме та широко використовується наступне програмне забезпечення для вирішення завдання маскування трафіку:

- Tor – безкоштовне та відкрите програмне забезпечення для анонімної передачі даних в Інтернеті;
- VPN-клієнти (NordVPN, ExpressVPN, CyberGhost) дозволяють приховувати реальну IP-адресу користувача та шифрувати трафік між пристроєм користувача та сервером VPN;
- proxy-сервери (Squid, Tinyproxy) дозволяють перенаправляти трафік через проміжний сервер, приховуючи реальну IP-адресу користувача;
- програмне забезпечення (ПЗ) для налаштування маршрутизаторів (OpenWrt, DD-WRT) дозволяє налаштувати VPN-сервер безпосередньо на маршрутизаторі для захисту всіх пристроїв, підключених до мережі;
- ПЗ для налаштування брандмауерів (iptables, nftables) дозволяє налаштувати правила маскування трафіку на рівні операційної системи;
- ПЗ (Shadowsocks, SSH-тунелі) дозволяє маскувати трафік шляхом створення зашифрованих тунелів між пристроями.

Розглянемо детальніше етапи застосування програми Shadowsocks:

1. Встановлення та налаштування сервера. На сервері, до якого будуть підключатися клієнти, встановлюється Shadowsocks-сервер та налаштовується його файл конфігурації. У файлі конфігурації задаються параметри сервера, такі як IP-адреса, порт і метод шифрування;

2. Встановлення та налаштування клієнта: на кінцевих електронно-обчислювальних машинах (ЕОМ), які підключатимуться до сервера, встановлюється Shadowsocks-клієнт та налаштовується його конфігураційний файл. У конфігураційному файлі задаються параметри клієнта, такі як IP-адреса та порт сервера, а також метод шифрування;

3. Підключення клієнта до сервера: після налаштування клієнта та сервера, клієнт підключається до сервера за допомогою програми Shadowsocks. Для цього користувач запускає клієнтську програму, вводить IP-адресу та порт сервера, а також облікові дані;

4. Шифрування та передача даних: після встановлення з'єднання між клієнтом і сервером, всі передані дані шифруються методом, заданим у конфігураційному файлі сервера та клієнта. Захищений трафік відправляється від клієнта до сервера, де він дешифрується та відправляється на кінцеву адресу;

5. Розрив з'єднання. Закривши клієнтську програму, після завершення роботи користувач може розірвати з'єднання із сервером.

Нижче наведено приклад клієнтської частини програми Shadowsocks (мова програмування Python), для демонстрації процедур шифрування, передачі на сервер та дешифрування. Як підсумок, Shadowsocks працює за принципом "проксі-сервера", який забезпечує шифрування та маскування трафіку перед його передачею.

```
import socket
import encrypt
import decrypt
# встановлення з'єднання з сервером
def establish_connection():
    server_addr = ("example.com", 8000)
    sock = socket.socket(socket.AF_INET,
socket.SOCK_STREAM)
    sock.connect(server_addr)
    return sock
# надсилання даних на сервер
def send_data(sock, data):
    sock.sendall(encrypt(data))  # дані
шифруються перед відправкою на сервер
# отримання даних від сервера
def recv_data(sock):
    data = sock.recv(1024)
    return decrypt(data)  # отримані дані
розшифровуються
# основний цикл роботи клієнта
def main():
    sock = establish_connection()
    while True:
        data_to_send = input("введіть дані для
надсилання на сервер: ")
        send_data(sock, data_to_send)
        received_data = recv_data(sock)
        print(: ", received_data)
if __name__ == "__main__":
    main()
```

Для роботи програми необхідні також модулі encrypt та decrypt, які містять відповідні функції для шифрування та розшифровування даних.

Виявлення факту маскування трафіку в мережі може бути складним процесом, який потребує детального аналізу трафіку. Застосування для цього програмних рішень може давати помилкові спрацьовування (може виявити не всі випадки маскування трафіку), тому програмні продукти використовуються лише як додатковий інструмент у комплексі заходів із безпеки мережі.

Існує кілька підходів, які можуть допомогти виявити факт маскування:

- моніторинг: адміністратор мережі може використовувати інструменти моніторингу трафіку (Wireshark, tcpdump і т.д.);
- використання інструментів виявлення аномалій (Snort, Suricata, Bro);
- аналіз журналів системи: деякі методи маскування трафіку можуть використовувати спеціальні програми чи скрипти для реалізації. Тому адміністратори мереж можуть проаналізувати журнали системи, щоб виявити незвичайну активність або запуск невідомих програм.

Серед алгоритмів аналізу можливо виділіти наступні:

- алгоритми машинного навчання (Random Forest) для класифікації трафіку на шифрований та не шифрований;
- алгоритми методу опорних векторів (SVM) (для класифікації мережевого трафіку на різні категорії);
- алгоритми на основі статистичних методів, таких як метод кореляції;
- алгоритми аналізу частотного спектра, виявлення змін у розмірі пакетів та тривалості пакетів, інтервалів між пакетами, розподілу пакетів за протоколами.

Послідовність дій з виявлення факту маскування трафіку в мережі можливо представити алгоритмом рис. 2.

Приклад програми виявлення факту маскування трафіку в мережі:

```
import scapy.all as scapy
def detect_covert_traffic(packet):
    # Перевірка наявності опції в заголовку IP-пакета з номером 252
    if packet.haslayer('IP') and packet.haslayer('IPOption'):
        ip_options = packet['IPOption'].copy()
        for opt in ip_options:
            if opt[0] == 252:
                print("[+] Covert channel detected from " + packet['IP'].src + " to " + packet['IP'].dst)
    # Запускаємо захоплення мережевого трафіку з допомогою Scapy
    sniff(filter='ip', prn=detect_covert_traffic, store=0)
```

Рис. 2. Послідовність дій з виявлення факту маскування трафіку в мережі

Цей модуль використовує бібліотеку Scapy для захоплення мережевого трафіку і фільтрує тільки IP-пакети. Потім перевіряє наявність опції (номер 252 у заголовку IP-пакета) і виводить повідомлення у разі виявлення прихованого каналу передачі даних.

Для виявлення фактів маскування трафіку в мережі можливо використовувати наступне програмне забезпечення: Wireshark, Network Miner, Bro/Zeek. Це інструменти для аналізу мережевого трафіку, які дозволяють виявляти шифрований трафік и провести його дешифрування за наявність ключів.

Для виявлення фактів маскування трафіку в мережі можна використовувати: програмне забезпечення Wireshark, Network Miner, Bro/Zeek; бібліотеку Scapy, tcpdump та інші для аналізу трафіку; алгоритми та методи визначення змін у розмірах пакетів та затримках передачі даних для виявлення факту використання VPN-з'єднання.

ВИСНОВКИ

Необхідність дослідження процедури маскування трафіку у мережі передачі даних пов'язана з тими обставинами, що для вирішення задач приховування трафіку і виявлення факту цих дій застосовуються однакові (загально відомі) програмні засоби. Ефективність обох процедур залежить від вмінь та навичок оператора (адміністратора).

Маскування трафіку не є універсальним методом захисту інформації, та його ефективність може бути знижена у разі використання сучасних методів аналізу. Також використання алгоритмів маскування може уповільнити швидкість передачі даних і вимагати додаткових ресурсів для його реалізації.

Загалом, метод маскування трафіку може бути використаний у поєднанні з іншими методами захисту інформації, такими як шифрування, автентифікація та контроль доступу, для досягнення максимального рівня безпеки мережі.

ЛІТЕРАТУРА

[1] Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.

[2] Заплотинський Б.А. Основи інформаційної безпеки: конспект лекцій. КПВіП НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

[3] Захист інформації в комп'ютерних системах: підручник / укладачі О.М. Гапак, С.І. Балога. Ужгород: ПП "АУТДОР-ШАРК, 2021. 184 с.

[4] Гнатушенко В.В., Владимирська Н.О. Аналіз статистичних характеристик комунікаційної інформації в комп'ютерних мережах // Штучний інтелект. 2015. № 1-2. С. 20-26.

[5] Бабкін А.А., Кудін О.В. Огляд нейромережевих моделей систем виявлення вторгнень // Вчені записки Таврійського національного університету імені В.І. Вернадського Серія: Технічні науки. 2020. Том 31 (70) Ч. 1 № 3. С. 77-82

[6] Ільєнко А.В., Ільєнко С.С., Вертиполох О.О. Метод захисту трафіку від втручання dpi систем на базі використання DOH та DOT протоколів // Кібербезпека: освіта, наука, техніка. 2020. Том 2 № 10. С. 75-87.

[7] Сохін Н. Л., Гученко М.І., Кирса А.О. Моделі та методи прогнозування мережевого трафіку в реальному часі // Вісник КрНУ імені Михайла Остроградського. 2019. Випуск 4. С. 90-98.

[8] A. Iacovazzi, A. Baiocchi. Internet Traffic Privacy Enhancement with Masking: Optimization and Tradeoffs // IEEE Transactions on Parallel and Distributed Systems, 2014. Vol. 25(2). pp.353-362.

METHODOLOGY OF TRAFFIC MASKING IN A SPECIALIZED DATA TRANSMISSION NETWORK

In connection with the growing threats in cyber security, there is a need to develop new approaches and methodologies for masking traffic to avoid detection and analysis of traffic by unauthorized persons. Traffic masking allows you to hide the characteristics of the transmitted data, such as source, destination, type and volume, path, and other metadata that make it possible to identify and analyze the communication. This can be particularly useful in cases where it is necessary to preserve the privacy of users or to prevent disclosure of sensitive information. Modern methods of traffic analysis are constantly being improved, so there is a need to develop new approaches to masking in accordance with changes in data analysis technologies. The relevance of the work is related to the fact that the actions of the administrator of a specialized network to ensure the security of its operation are aimed at solving two interrelated tasks, namely: ensuring the hidden functioning of the network and detecting facts of third-party intervention (detecting the actions of outsiders). Both tasks are strictly regulated by the governing documents, but the final result depends on the official's depth of understanding of the existing problem, the degree of mastery of the methodology for ensuring the security of the functioning of a specialized network, the available material (including financial) means and the available time resource. The paper analyzes the existing approaches to ensuring traffic masking in the network, provides algorithms (software implementation options) of masking mechanisms and detection of the fact of traffic masking in a specialized data transmission network.

Keywords: masking, privacy, mathematical models, Shadowsocks.

Клімович Сергій Олегович, кандидат технічних наук, начальник кафедри захисту інформації в телекомунікаційних системах та мережах Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Serhii Klimovych, candidate of technical sciences, Head of Department of Information Protection in Telecommunication Systems and Networks, Military Institute of Telecommunication and Information technologies named after the Heroes of Kruty.
E-mail: robota_ks@ukr.net.
Orcid ID: 0000-0001-7209-2176.

DOI: 10.18372/2410-7840.25.17936
УДК 004.49

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ БЕЗПЕКИ В ХМАРНИХ СЕРЕДОВИЩАХ ТА ВИРІШЕННЯ З ЗАСТОСУВАННЯМ ПІДХОДУ "БЕЗПЕКА ЯК КОД"

Олександр Вахула, Іван Опірський

"Безпека як код"- це підхід організації безпеки в хмарних середовищах, який полягає на методі інтеграції контролів безпеки, політик та кращих практик безпосередньо в процеси розробки та розгортання програмного забезпечення. Процес інтеграції включає трансформацію вимог безпеки та конфігурацій в програмний код, який в свою чергу вважається невід'ємною частиною повного життєвого циклу розробки програмного забезпечення. Вбудовуванням мір безпеки в код, скріпти, шаблони та автоматизовані робочі процеси, організація забезпечує, що є чітко визначені контролі безпеки, які консистентно та примусово будуть застосовані на всіх операційних фазах створення програмного забезпечення (розробка, тестування, впровадження, підтримка). В даній статті розглянуто основні проблеми побудови безпеки в хмарних середовищах та їх причини, також розглядає складові та принципи підходу «Безпека як код", приклад реалізації з поясненням, переваги даного підходу, а також роль DevSecOps. Ця стаття має на меті допомогти читачам зрозуміти важливість підходу "Безпека як код", як одного з найефективніших методів організації безпеки в хмарних середовищах. Так, як хмарні середовища продовжують розвиватися та поширюватися, а загрози стають все більш складними, підхід "Безпека як код" являє собою основну стратегію для про-активного захисту цифрових активів. Ця публікація слугує посібником для розуміння, впровадження та отримання переваг від підходу "Безпеки як код", надаючи уявлення про майбутній ландшафт безпеки хмарних середовищ та важливу роль автоматизації та інтеграції у вирішенні сучасних викликів безпеки. Для підтримки дослідження було проведена широкий аналіз літератури та статей, які надають інформацію про підхід "Безпека як код" та його застосування.

Ключові слова: *Безпека як код, Інфраструктура як код, DevSecOps, DevOps, хмарні середовища, цикл розробки програмного забезпечення, загрози безпеки.*

ВСТУП

У хмарних обчисленнях, які постійно розвиваються, де гнучкість та інновації поєднуються, неможливо переоцінити важливість надійних заходів безпеки. Оскільки організації продовжують використовувати трансформаційний потенціал хмарних технологій, необхідність захисту цифрових активів від постійно зростаючого спектру загроз стає не просто пріоритетом, а стратегічним імперативом.

«Безпека як код», народжена на стику кібербезпеки та розробки програмного забезпечення, являє собою зміну парадигми того, як організації концептуалізують, впроваджують і підтримують свої стратегії безпеки в хмарних середовищах. Цей підхід інкапсулює злиття принципів і методів безпеки в код, створюючи про-активну, автоматизовану та інтегровану екосистему безпеки, яка бездоганно узгоджується з сучасними методологіями розробки.

В даній статті автори розглядають основні проблеми безпеки, з якими стикаються споживачі хмарних сервісів. Кореневими причинами яких можна вважати нерозуміння моделі спільної відповідальності, яка є фундаментальною; динамічність і масштабованість середовища на відміну від наземної інфраструктури до якої звикли; недостатня видимість ресурсів або "тіньове" IT; недооцінка ризиків пов'язаних з API; складність навігації даних в розподіленому середовищі, в тому числі