УДК 004.056

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ СТОРОННЬОГО ДОСТУПУ ТА ЗАХИСТУ IP КАМЕР

Веселовський О.Г.
Науковий керівник – ст. викладач кафедри БІТ Данилов А.Д.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
тел.: +38(099)-441-96-64, e-mail: oleksii.veselovskyi@nure.ua

The paper provides a comprehensive analysis of methods for detecting and protecting IP cameras from unauthorized access. Focusing on the use of intrusion detection systems and artificial intelligence algorithms, the author examine their effectiveness and limitations in the context of modern cyber threats. In addition, they analyze security measures such as the use of strong passwords, encryption, and virtual private networks. The paper highlights the need for further research and development in this area to effectively counter the ever-increasing cyber threats to IP camera security.

З поширенням IP-камер в сферах громадської безпеки, домашньої безпеки і промислового відеоспостереження, забезпечення їх захисту від несанкціонованого доступу стало важливим завданням. IP-камери відіграють важливу роль у системах відеоспостереження, забезпечуючи можливість моніторингу та запису в режимі реального часу, також пропонують розширені функціональні можливості, такі як віддалений моніторинг і хмарне зберігання, проте мають свої вразливості, якими можуть скористатися зловмисники. Несанкціонований доступ до цих камер не тільки ставить під загрозу приватність осіб, а й створює значні ризики для безпеки організації.

В роботі проведено аналіз методів виявлення несанкціонованого доступу та захисту IP-камер. У сучасному світі, де кіберзагрози продовжують розвиватися, вкрай важливо вживати надійних заходів безпеки для захисту цілісності та конфіденційності відеозаписів з камер. Вивчаючи існуючі методи і нові технології, ми маємо на меті дати уявлення про ефективність, обмеження і потенційні можливості вдосконалення існуючих механізмів безпеки, розгорнутих в системах IP-камер.

Одним з основних методів виявлення стороннього доступу є використання систем виявлення вторгнень (СВВ). Ці системи відстежують мережевий трафік на предмет підозрілих дій і видають сповіщення, коли такі дії виявляються. Незважаючи на те, що СВВ ефективні у виявленні відомих загроз, вони можуть бути не настільки ефективними у виявленні нових, невідомих загроз [1].

Іншим методом виявлення стороннього доступу є використання алгоритмів штучного інтелекту (ШІ) та машинного навчання (МН). Ці алгоритми можуть аналізувати закономірності мережевого трафіку та виявляти аномалії, які можуть свідчити про стороннє вторгнення. Перевага алгоритмів ШІ та МН полягає в тому, що вони здатні адаптуватися і вчитися на нових загрозах, що робить їх потенційно більш ефективними, ніж традиційні СВВ [2].

Що стосується методів захисту IP-камер, то одним із поширених підходів є використання надійних, унікальних паролів і регулярне оновлення паролів. Це може запобігти несанкціонованому доступу до каналу IP-камери. Крім того, використання шифрування може захистити дані, що передаються з IP-камери, запобігаючи їх перехопленню та перегляду третіми особами [1].

Використання віртуальних приватних мереж (VPN) може забезпечити додатковий рівень безпеки. VPN створюють безпечне, зашифроване з'єднання через Інтернет, яке може захистити канал IP-камери від перехоплення [2].

Ще одним ефективним методом захисту IP-камер є використання систем виявлення та запобігання вторгнень. Ці системи можуть виявляти і запобігати поширенню шкідливих програм на терміналах користувачів і цифрових відеореєстраторах [3].

Шифрування даних також є важливим аспектом захисту IP-камер. Всі відеопотоки, а також така інформація, як імена користувачів і паролі, повинні бути зашифровані, щоб захистити дані, що передаються, особливо якщо вони проходять через Інтернет. Найпоширеніші варіанти шифрування включають SSL/TLS для інформації про користувача та IPsec або MACsec для даних. Належне шифрування допомагає запобігти підслуховуванню та маніпуляціям з пакетами, які можуть відбуватися під час атак типу "людина посередині" (MitM) [3].

У роботі проведено аналіз методів виявлення та захисту IP-камер від несанкціонованого доступу. Подальше вдосконалення і застосування методів захисту може значно підвищити безпеку систем відеоспостереження з використанням IP-камер.

Список використаних джерел:

1. Biondi P., Bognanni S., & Giampaolo B. Vulnerability Assessment and Penetration Testing on IP cameras. *Universita di Catania.* 2022

2. Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. The Security of IP-Based Video Surveillance Systems. *Sensors.* 2020

3. 5 Ways to Protect IP Video Surveillance Systems. Allied Telesis : вебсайт URL: https://www.alliedtelesis.com/be/en/blog/5-ways-protect-ip-video-surveillance-systems (дата звернення: 04.03.2024)