DOI: https://doi.org/10.36910/6775-2524-0560-2023-51-21
УДК 621.379, 004.032.6
Обухова Катерина Олександрівна, ст. викладач,
https://orcid.org/0000-0001-8793-7055
Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна.

БЕЗПЕЧНЕ ВІДДАЛЕНЕ ПІДКЛЮЧЕННЯ ДО IP-КАМЕР ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Обухова К.О. Безпечне віддалене підключення до IP-камер через мережу Інтернет. IP-камери стали частиною нашого повсякденного життя. Власники камер відеоспостереження хочуть мати доступ до відеоканал в реальному часі на смартфонах, віддалених комп'ютерах та інших мобільних пристроях. Для цього потрібно налаштувати безпечне підключення до IP-камер через мережу Інтернет. У цій статті досліджуються різні методи підключення для захисту системи відеоспостереження в Інтернеті.
Ключові слова: IP-камери, система відеоспостереження, метод «точка-точка», переадресація портів, VPN-тунелювання

Obukhova K. Secure remote connection to IP cameras via the Internet. IP cameras have become part of our everyday life. CCTV camera owners want to have access to a real-time video feed on smartphones, remote computers and other mobile devices. To do this, you need to configure a secure connection to the IR cameras via the Internet. This article explores different connection methods for securing an Internet CCTV system.
Keywords: IP cameras, video surveillance, point-to-point, port forwarding, VPN

Постановка наукової проблеми. IP-камери стають все більш популярними. З міркувань безпеки вони активно використовуються для моніторингу будинків, робочих місць, громадських місць і доріг. Через розташування установки більшість методів доступу є віддаленим.

Компанії та домовласники все більше покладаються на камери Інтернет-протоколу (IP) для спостереження віддалено на смартфонах або інших мобільних пристроях. Занадто часто це дає їм хибне відчуття безпеки: хоча насправді зловмисники можуть не лише отримати доступ і переглянути канал камери, але й використати незахищений пристрій, щоб зламати саму мережу.

Аналіз досліджень. Нові дослідження показують експоненціальне збільшення кількості використання саме IP-камер. Так, на основі даних 28 найпопулярніших виробників, було виявлено, що 3,5 мільйона IP-камер підключено до Інтернету, що свідчить про восьмикратне збільшення за останні 2 роки [3].

Ця тенденція викликає занепокоєння, оскільки пристрої, підключені до Інтернету, можуть бути вразливими до атак – зловмисники можуть отримати доступ до прямої трансляції з камери, збирати конфіденційні дані та запускати подальші атаки в мережі.

Так, наприклад, у березні 2021 року команда хакерів зламала велику кількість IP-камер, що належать виробника Verkada. Хакери отримали доступ до трансляцій камер відеоспостереження у хмарі, які розкривають дані та інтелектуальну власність на таких підприємствах, як Tesla, школах і в'язницях [2].

Серед проаналізованих брендів всі мають принаймні деякі моделі, які дозволяють користувачам зберігати паролі за замовчуванням або не мають жодних налаштувань автентифікації.

Також за допомогою запитів до відомих виробників було виявлено понад 1 мільйон камер спостереження та понад 125 000 серверів спостереження, відкритих для Інтернету. З цих пристроїв 90 % не мають захищених порталів входу (використовують HTTP, а не HTTPS). Крім того, приблизно 8 % мають відкриті порти SSH і Telnet, 3 % мають розкриті бази даних MySQL, і принаймні 1,7 % цих пристроїв все ще вразливі до вразливості HeartBleed SSL, виявленої ще у 2012 році.

Навіть великі виробники відеоспостереження мають моделі камер відеоспостереження з незахищеним підключенням. Наприклад, на сервері CCTV від Samsung принаймні 83 тисячі пристроїв, де 86 % використовують портали входу HTTP, а 1604 мають відкриті порти SSH. Більше того, HikVision, виробник систем відеоспостереження з найбільшою на сьогодні часткою ринку в 24,7 %, має принаймні 260 тисяч пристроїв, які піддаються впливу, і лише 53 з них мають увімкнений HTTPS [1].

В одному з досліджень було виявлено, що приблизно 73 000 камер безпеки в 256 країнах доступні за допомогою стандартних паролів. Ці статистичні дані підкреслюють низький рівень безпеки IP-систем відеоспостереження [4].

Метою дослідження є аналіз переваг і недоліків різних способів віддаленого підключення до системи відеоспостереження та визначення найбільш безпечного віддаленого підключення IP-камер.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Перш ніж розглянути способи віддаленого підключення до IP-камер, потрібно зазначити, що на безпеку також впливають уразливості самої системи відеоспостереження, такі як бекдори або використання стандартних паролів, які дозволяють хакерам отримати несанкціонований доступ.

Бекдор-зломи, які траплялися в минулому, відбувалися через лазівки та ліниві програмні недогляди, які призводили до експлойтів. Неякісні системи відеоспостереження зазвичай мають бекдори, які не були розглянуті через недостатні інвестиції часу та грошей у захист пристроїв. Багато скомпрометованих брендів також не надають оновлень для вирішення проблем безпеки, часто тому, що ці діри в безпеці неможливо закрити.

З незахищеною системою камер потрібно турбуватися не лише про вразливість цієї системи до злому, але й про інші пристрої в мережі, які також можуть стати вразливими. Відповідно до цієї історії в Реєстрі, системи відеоспостереження з бекдорами можуть використовуватися для атаки на інші пристрої у домашній або робочій комп'ютерній мережі та викрадення конфіденційної інформації [5].

Використання слабких паролів або паролів за замовчуванням є помилкою номер один, яка дозволяє хакеру проникнути в систему відеоспостереження в Інтернеті або будь-який пристрій IoT. Хакери використовують ботів для перевірки комбінацій відомих паролів, які використовуються виробниками пристроїв, щоб легко вгадати паролі та отримати доступ до камер або відеореєстраторів безпеки по всьому світу, підключених до Інтернету.

Є кілька різних способів віддаленого підключення до системи відеоспостереження. Кожен із методів має свої переваги та недоліки, і жодна система не застрахована від злому, якщо вона підключена до Інтернету. Нижче розглянемо різні методи доступу до системи відеоспостереження, починаючи від найпростішого та найменш безпечного віддаленого підключення до найбезпечнішого.

Метод «точка-точка»

Підключення «точка-точка» (point-to-point, P2P) або хмарне з'єднання – це спосіб з'єднання, який дозволяє використовувати мобільний пристрій за допомогою застосунку для підключення системи відеоспостереження через сервер, що знаходиться в хмарі або в чужому центрі обробки даних, безпосередньо до пристрою.

Використання цього методу для віддаленого підключення є найпростішим у налаштуванні та стає все більш популярним. Метод P2P не потребує складних мереж, таких як переадресація портів або VPN. У першу чергу пристрої, орієнтовані на домашніх споживачів, використовують P2P як спосіб віддаленого перегляду, оскільки користувачі, які не мають технічних знань, легко налаштувати за допомогою смартфона.

Принцип роботи полягає в тому, що смартфон (чи інший мобільний пристрій) та камера підключається до «хмари» або P2P-сервера виробника або сервера третьої сторони (рис. 1). Зазвичай, існує певна форма безпечної автентифікації, після чого надається доступ до відеоканалу та системи.

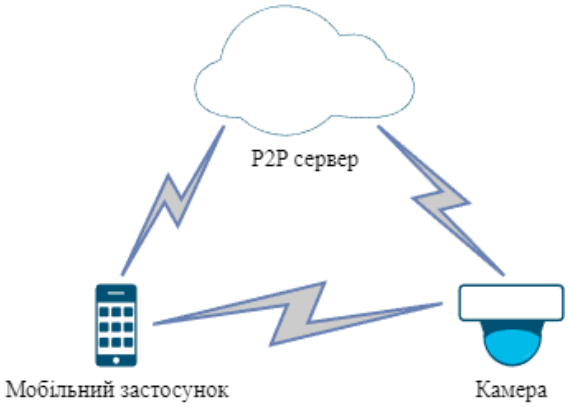

Рис. 1 – Схема підключення «точка-точка»

Оскільки дані у цьому випадку проходять через інший сервер, існує збільшена при передачі відеоданих. Для користувачів із повільним підключенням до Інтернету це може стати перешкодою для віддаленого перегляду у режимі «наживо». Для тих, хто має швидке підключення до Інтернету,

затримка може бути не такою помітною, але вона все одно є. Будь-який віддалений перегляд матиме певну затримку, але при підключені «точка-точка» вона найбільш виражена.

Переваги хмарного з'єднання:

– проста конфігурація;

– пристрої прив'язані до одного облікового запису і ними можна легко поділитися з ким забажаєте.

Недоліки методу:

– використовує UPnP – технологію універсального автоматичного налаштування мережевих пристроїв, тому немає можливості контролювати, які порти відкриваються;

– дані проходять через сервер третьої сторони і доступ до них є у власника цієї хмари;

– при віддаленому підключенні є певна затримка, які може бути доволі критичною при нестабільному підключенні до Інтернету.

Загалом P2P є безпечним методом віддаленого перегляду, якщо нікому не передавати інформацію про віддалений перегляд, а саме серійний номер запису камери безпеки чи камери.

Однак, не всі виробники створюють якісні рішення «точка-точка» або не завжди оновлюють такі рішення, для відповідності новому програмному забезпеченню (рис. 2).

Рис. 2 – Сервіс виробника камери підтримує тільки застарілі версії браузера

Деякі з них не вимагають, щоб камера була прив'язана до одного облікового запису, тому можна легко отримати доступ до неї, якщо відомий серійний номер пристрою та параметри за замовчуванням не були змінені. Крім того, якщо ця компанія припинить свою діяльність і припинить підтримувати свій сервер, у вас не залишиться жодних засобів для підключення до вашої системи відеоспостереження, крім двох інших методів (переадресація портів або VPN).

Отже, метод дистанційного «точка-точка» призначений переважно для домашніх користувачів.

Метод переадресації портів

Переадресація портів (port forwarding) – це функція маршрутизаторів, яка дозволяє користувачеві налаштувати певні комунікаційні порти для маршрутизації до пристроїв у мережі, наприклад комп'ютера, відеореєстратора або IP-камери (рис. 3).

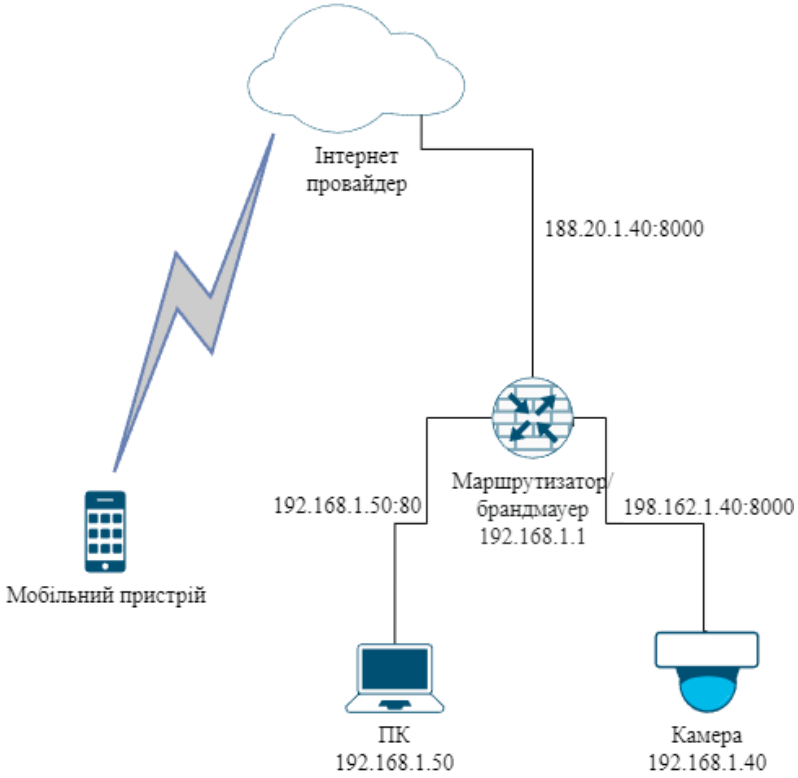

Рис. 3 – Структура схема налаштування переадресації портів

Найбільшою перешкодою для переадресації портів є вимога статичної IP-адреси. IP-адресу призначає маршрутизатору ваш Інтернет-провайдер (ISP). Більшість домашніх підключень до Інтернету періодично отримують нову IP-адресу, коли постачальник послуг виконує технічне обслуговування або вимикається електроенергія. Якщо IP-адреса зміниться, доступ до системи відеоспостереження буде заблоковано, доки не отримаєте адресу, на яку її було змінено.

Як обхідний шлях можна скористатися безкоштовною службою служби динамічних доменних імен (DDNS), вбудованою в більшість доступних на ринку маршрутизаторів, або спеціальними застосунками. Це дозволяє легко відстежувати зміну IP-адрес під час підключення до Інтернету. Маршрутизатор повертає на захищений сервер, поточну IP-адресу, тому можна використовувати зрозуміле ім'я, наприклад myhomesystem.ddns.net, щоб отримати доступ до IP-камери з Інтернету.

Перенаправлення портів безпечніше, ніж P2P, оскільки це пряме підключення до камери через маршрутизатор. Це пряме з'єднання усуває будь-яку додаткову затримку або час затримки, які зазвичай зустрічаються з хмарними з'єднанням. Поки нікому не надаєте IP-адресу/адресу DDNS, ім'я користувача або пароль, переадресація портів є кращим способом віддаленого перегляду порівняно з P2P.

Переваги переадресації портів:

– можливість контролювати, які порти відкриваються;
– доступ до повних налаштувань камери;
– через встановлення прямого з'єднання немає додаткової затримки при підключенні до камери у режимі «наживо»;
– для віддаленого доступу можна вибрати статичний IP-адресу або динамічну IP-адресу (за допомогою DDNS).

Мінуси:

– відкриті порти залишаються відкритими весь час;
– якщо немає інструментів для виявлення або запобігання вторгненню, система піддається атакам з Інтернету;
– якщо користувач має слабкий пароль, він компрометує систему.

Використання цього методу поки що є найбільш гнучким варіантом, якщо потрібен більш детальний контроль, особливо в ситуаціях, коли для доступу до системи потрібно більше ніж одній людині.

Крім того, використання служби DDNS полегшує доступ через веб-браузер без необхідності встановлення клієнта ПК/Mac, пов'язаного з системою. DDNS дозволяє використовувати «mycompany.com:80» замість фактичної IP-адреси, наприклад «188.40.100.xx:80», яка може змінюватися за бажанням і бажанням вашого провайдера.

Переадресацію портів рекомендовано для комерційного та домашнього використання для підзвітності та контрольованого доступу до системи відеоспостереження.

VPN-тунелювання

Віртуальна приватна мережа (VPN) – це технологія, за допомогою якої можна створити безпечне та зашифроване з'єднання через менш захищену мережу, наприклад публічний Інтернет. VPN працює, використовуючи спільну загальнодоступну інфраструктуру, зберігаючи конфіденційність за допомогою процедур безпеки та протоколів тунелювання. Тунелювання працює подібно до методу «точка-точка», за винятком того, що це безпечний зашифрований тунель до вашої мережі ззовні через Інтернет (рис. 4).

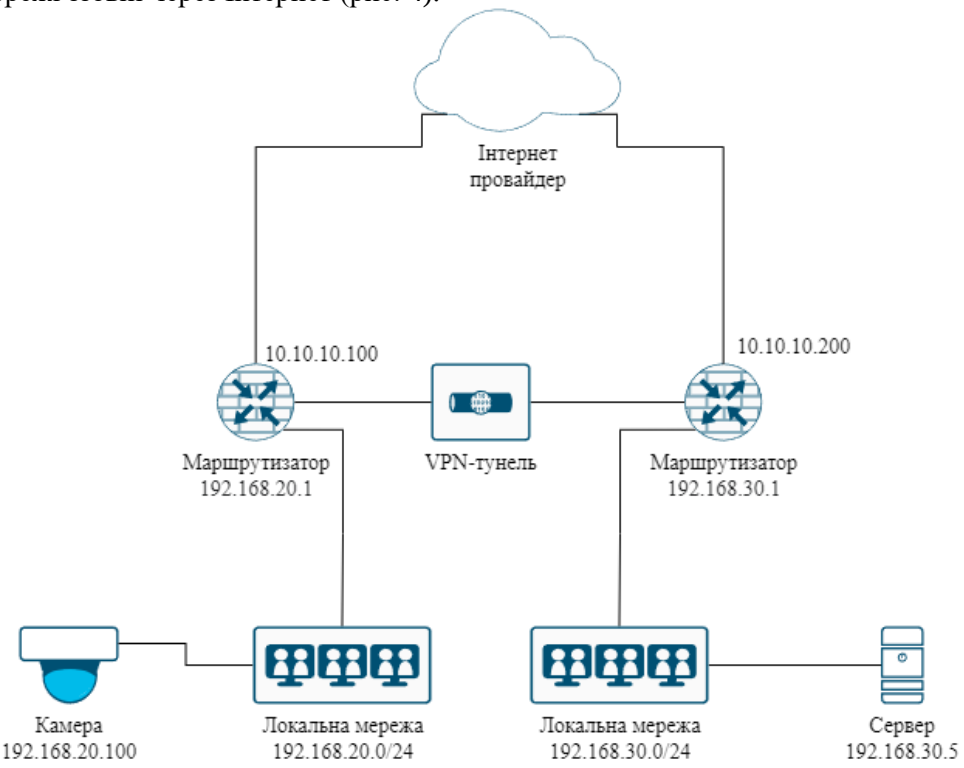

Рис. 4 – Структура схема встановлення VPN-тунелювання

Використання VPN або віртуальної приватної мережі є одним із найбезпечніших способів віддаленого доступу до системи відеоспостереження. VPN дозволяє безпосередньо підключатися до домашньої мережі з будь-якої точки світу. Прямі з'єднання, такі як VPN або переадресація портів, безпечніші, ніж використання P2P. Після встановлення VPN-з'єднання з домашньою мережею можна робити все, що завгодно, із системою відеоспостереження.

VPN відносно легко налаштувати на більшості домашніх маршрутизаторів, і його можна використовувати на ПК з будь-якою операційної системою, а також на мобільних пристроях під Android чи iOS.

Важливо зауважити, що не всі VPN однакові. Маршрутизатори матимуть різні можливості VPN, доступні для налаштування. Залежно від того, скільки камер потрібно підключити, знадобиться маршрутизатор із достатньо потужним процесором для розміщення VPN. Також знадобиться достатньо потужне підключення до Інтернету, щоб розмістити VPN із відеоданими. Слід враховувати також, що деякі маршрутизатори мають сильніше VPN-з'єднання, якщо вони з'єднані з притроями однієї марки та моделі.

VPN уразливі, лише якщо вони загальнодоступні або, якщо комусь надано інформацію про VPN. Більшість програмного забезпечення VPN потрібує щомісячну оплату, яка може бути значно високою.

Переваги тунелювання:

– даний метод пропонує більшу безпеку під час підключення з віддалених місць;
– можна використовувати для безпечного моніторингу третьою стороною;

– не потребує DDNS;

– немає необхідності відкривати порти системи та маршрутизатора для Інтернету та ризикувати відкритими атаками.

Недоліки використання VPN:

– швидкість з'єднання може бути нижчою через витрати VPN, які використовуються для шифрування трафіку;

– для підключення необхідно виконувати додаткові кроки, що зменшує простоту налаштування;

– кращі VPN мають доволі високу помісячну оплату.

Технологія VPN є дуже безпечним способом моніторингу системи відеоспостереження, але вона рідко використовується користувачами у домашніх мережах через складність налаштування VPN та високу вартість послуг.

Отже, VPN-тунелювання рекомендовано для використання в професійних, охоронних і корпоративних системах відеоспостереження.

Ці методи найчастіше використовуються, коли йдеться про підключення до систем відеоспостереження, але який метод потрібно обрати визначається потребами локальної мережі.

Висновки та перспективи подальшого дослідження. Хмарні з'єднання є загалом безпечним методом віддаленого доступу до IP-камери, але не всі виробники створюють високоякісні рішення. Деякі з них не вимагають прив'язувати камери до одного облікового запису або не використовують захищені протоколи при передачі даних. Також, завжди є ризик що до конференційних даних отримає доступ третя сторона, наприклад, власних хмарного серверу.

Використання методу переадресації портів є найбільш гнучким варіантом серед усіх розглянутих, особливо якщо потрібен більш тонкий контроль над налаштуваннями камери, наприклад, якщо доступ до системи має більше однієї людини. І хоча для переадресації портів потрібно мати статичну IP-адресу, є велика кількість сервісів, що надають послугу DDNS, яка дозволяє використовувати цей метод підключення навіть з динамічною IP-адресою.

Використання віртуальної приватної мережі є найбільш безпечним способом моніторингу систем відеоспостереження, але рідко використовується користувачами домашніх мереж через складність налаштування VPN і високу вартість послуги.

Отже, метод «точка-точка» в першу чергу орієнтованих на домашніх системи відеоспостереження. Переадресація портів рекомендується вже як для комерційного використання, так і приватного, а також, якщо потрібно надавати контрольований доступ до систем відеоспостереження. Використання VPN рекомендується для використання в професійних, охоронних і корпоративних системах відеоспостереження.

Список бібліографічного опису

1. Дел Кастільо М., Хермоса Х., Астілло П., Чудхарі Г., Драгоні Н. Програмно-визначена мережева безпечна система відеоспостереження з підтримкою Інтернету. Застосування інформаційної безпеки, 2023. С. 89-101. DOI:10.1007/978-3-031-25659-2_7.
2. Альшалаві Р., Хозіум О. Практичний приклад перевірки трафіку моніторингу IP-камери. Міжнародний журнал передових досліджень, 2020. Т. 8(12):1-11. DOI:10.23956/IJARCSSE.V8I12.924.
3. Калбо Н., Мирський Ю., Шабтай А., Еловіч Ю. Безпека IP-систем відеоспостереження. Датчики, 2020. Т. 20(17):4806. DOI: 10.3390/s20174806.
4. Сью К.-Л., Ву Т.-Ю. Нове керування віддаленим доступом до потокових даних IP-камер у реальному часі. Міжнародний журнал систем управління базами даних (IJDMS), 2020. Т 12, № 2. DOI: 10.5121/ijdms.2020.12201.
5. Ельхаррус О., Алмаадід Н., Аль-Маадід С. Огляд систем відеоспостереження. Журнал візуальної комунікації та представлення зображень, 2021. Том. 77. DOI: 10.1016/j.jvcir.2021.103116.

References

1. Del Castillo M., Hermosa H., Astillo P., Choudhary G., Dragoni N. Software-Defined Network Based Secure Internet-Enabled Video Surveillance System. Information Security Applications, 2023. pp. 89-101. DOI:10.1007/978-3-031-25659-2_7.
2. Alshalawi R., Khozium O. A Case Study of IP Camera Monitoring Traffic Verification. International Journal of Advanced Research, 2020. Vol. 8(12):1-11. DOI:10.23956/IJARCSSE.V8I12.924.
3. Kalbo N, Mirsky Y, Shabtai A, Elovici Y. The Security of IP-Based Video Surveillance Systems. Sensors (Basel), 2020. Vol. 20(17):4806. DOI: 10.3390/s20174806.
4. Sue K.-L., Wu T.-Y. A novel remote access control for the real-time streaming data of IP cameras. International Journal of Database Management Systems (IJDMS), 2020. Vol.12, No.2. DOI : 10.5121/ijdms.2020.12201.
5. Elharrouss O., Almaadeed N., Al-Maadeed S. A review of video surveillance systems. Journal of Visual Communication and Image Representation, 2021. Vol. 77. DOI: 10.1016/j.jvcir.2021.103116.