УДК 004.056
DOI: 10.31673/2409-7292.2021.034248

Колісник Д.Р., Ліщук І.В.

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НА БАЗІ РІШЕННЯ HIKVISION

В роботі проведено дослідження та аналіз проблеми забезпечення захисту систем відеоспостереження, встановлена сутність завдань їх захисту. Проаналізовано існуючі технології захисту систем відеоспостереження. Досліджена технологія забезпечення захисту систем відеоспостереження на базі рішення Hikvision. Визначено методи та засоби захисту складових системи відеоспостереження, які реалізовані компанією Hikvision. Встановлено основні загрози для IP-систем відеоспостереження. Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології захисту систем відеоспостереженні на підприємстві.

Ключові слова: відеоспостереження, Hikvision, кібербезпека, захист, Інтернет речей.

Вступ. На сьогодні системи відеоспостереження являються невід'ємною частиною сучасних підприємств, також вони знаходяться на важливих державних об'єктах, на вокзалах, в громадському транспорті і навіть удома. За останні кілька десятиліть технології відеоспостереження еволюціонували від аналогових систем до систем з комутацією пакетів (по мережах IPv4 і IPv6) [1]. В результаті за останні кілька років, кількість підключених пристроїв в будинку виросла в 17 разів [2]. Однак, як і очікувалося, ці системи і їх компоненти стали мішенню численних кібератак. Наприклад, вони були мішенню розподілених атак типу "відмова в обслуговуванні" (DDoS), використовуваних для вторгнення в приватне життя користувачів і навіть для майнінгу криптовалюти [3]. В одному дослідженні було виявлено, що приблизно 73 000 камер відеоспостереження в 256 країнах доступні з паролями за замовчуванням [4]. Ці статистичні дані підкреслюють поганий стан безпеки IP систем відеоспостереження.

Мета роботи – розробити варіант технології захисту системи відеоспостереження на базі рішення Hikvision.

Аналіз атак в системах відеоспостереження

У багатьох роботах були виконані комплексні огляди безпеки Інтернету речей [5–7]. Хоча системи відеоспостереження на основі IP використовують загальні мережеві елементи і спільно використовують технології з іншими системами Інтернету речей, їх поверхня атаки відрізняється з точки зору кібербезпеки. Це відбувається тому, що вони підтримують і забезпечують нашу фізичну безпеку, і, коли вони скомпрометовані, виникає загроза нашої фізичної безпеки і нашого приватного життя (вдома, на роботі і в національному сенсі). В результаті технологія, суб'єкти загроз, мотиви атак і загальна поверхня атаки відрізняються від IoT. Можна розрізнити ці відмінності наступним чином:

Суб'єкти загроз. Існує безліч зловмисників, які хочуть використовувати функціональні можливості систем відеоспостереження спеціально. Наприклад, державні діячі або злодії, які проводять розвідку над географічним районом, і злочинці, які планують шантажувати жертву відеозаписом;

Об'єкти загроз. У разі компрометації ці системи можуть надати зловмиснику особисті зображення, що призведе до прямого явного порушення конфіденційності. Ці системи також є прибутковими активами для власників ботнетів, оскільки вони зазвичай мають високу пропускну здатність (для DDoS-атак) і пристойні обчислювальні можливості (для кріптомайнінга). Особливості системи спостереження змінюють вагу цілей атакуючого і пріоритет захисника в обороні. Наприклад, в системах відеоспостереження більше уваги приділяється атакам проти DoS і MitM, ніж в інших системах [6].

Моделі розгортання систем відеоспостереження:

Існує кілька способів розгортання системи відеоспостереження на основі IP. Топологія мережі може бути централізованою (всі камери підключаються до відеореєстратора) або розподіленою (користувач підключається до кожної окремої камери). З

точки зору доступності, система може бути доступна безпосередньо через Інтернет або не доступна взагалі. У зв'язку з цим виділяємо три категорії доступності (рис. 1):

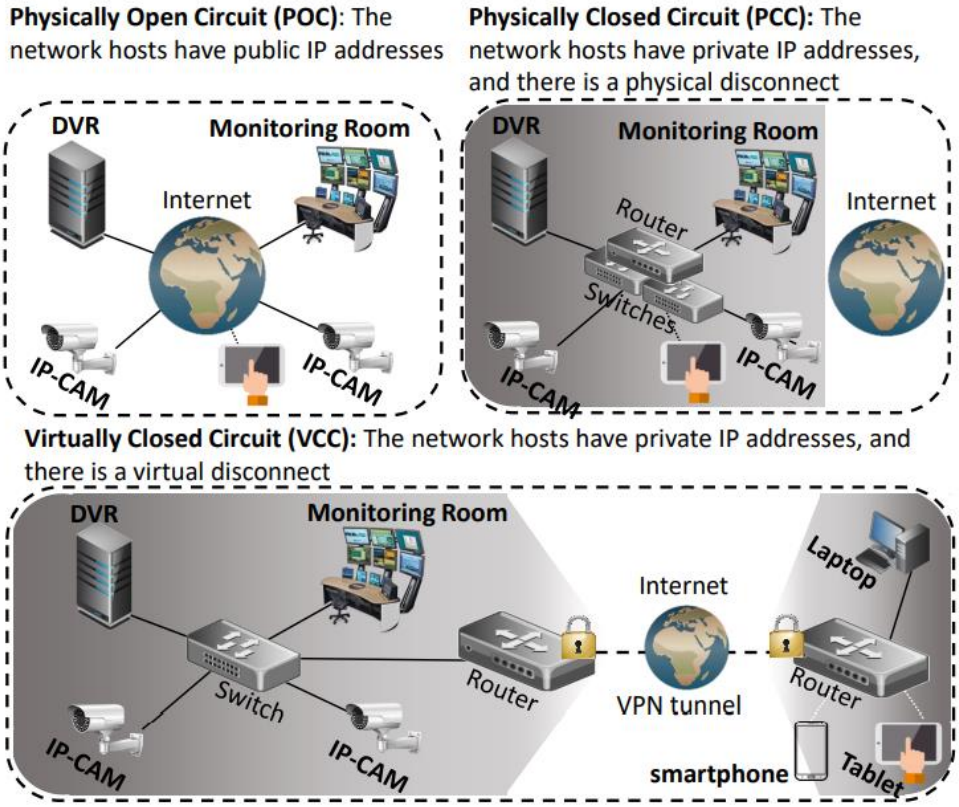

Рис. 1. Доступні моделі для розгортання системи відеоспостереження [6]

фізично відкритий контур (POC), коли мережеві хости в системі (камери, відеореєстратори тощо) мають публічні IP-адреси. Це означає, що будь-який користувач Інтернету може відправляти пакети на пристрої;

фізично замкнутий контур (PCC), коли мережеві хости в системі мають приватні IP-адреси, і немає інфраструктури, яка з'єднує мережу з Інтернетом. Це означає, що ніхто з Інтернету не може відправляти пакети безпосередньо на пристрої. Ці системи також називаються air-gapped networks [7];

практично замкнутий контур (VCC), коли мережеві хости в системі мають приватні IP-адреси, а мережа підключається через Інтернет за допомогою VPN. Це означає, що ніхто з Інтернету не може відправляти пакети на пристрої безпосередньо, якщо тільки вони не відправляють пакети через VPN.

З точки зору життєвого циклу безпеки даних Hikvision формулює відповідні політики управління безпекою даних відповідно до кожної фази життєвого циклу, включаючи генерацію, зберігання, передачу і знищення даних, щоб забезпечити наскрізну безпеку даних.

End-to-End Data Encryption. Витік конфіденційної інформації, такої як ім'я користувача, пароль, особисте ім'я, номер телефону, Адреса електронної пошти та адреса, дозволить зловмиснику вкрасти користувацьку інформацію за власним бажанням протягом тривалого часу без відома користувача. Щоб уникнути витоку конфіденційних даних, пристрій може безпечно зберігати конфіденційні дані. Пристрій зберігає конфіденційні дані за допомогою шифрування, щоб запобігти отримання зловмисниками конфіденційної інформації шляхом отримання документів за допомогою статичного аналізу прошивки і входу в систему пристрою.

Шифрування даних протягом усього процесу, включаючи генерацію, передачу, зберігання та застосування даних, забезпечує максимальну безпеку даних. Після

високоміцного шифрування дані передаються з терміналу на серверне сховище або платформну систему і зберігаються безпосередньо у вигляді зашифрованих даних на платформі. При наявності запиту бізнес-запиту дані як і раніше відправляються Клієнту в зашифрованому вигляді і відображаються після локальної розшифровки на клієнті. Дані знаходяться в зашифрованому стані протягом усього курсу, що може ефективно запобігти витоку даних.

Digital Watermarking. Цифрові водяні знаки-це технологія стеганографії, основна концепція якої полягає в захисті авторських прав на цифрові продукти, доказі автентичності продуктів і відстеженні піратства або наданої додаткової інформації про продукти шляхом вбудовування секретної інформації в цифрові продукти, такі як цифрові зображення, аудіо-та відеоконтент. Ця технологія дозволяє приховати цифрову інформацію, яка потім стає невидимою у вихідному файлі і може бути прочитана тільки за допомогою спеціальних зчитувачів. Таким чином, додавання цифрових водяних знаків у відеопотік є ідеальним рішенням для атак на відео-саботаж. Стан прихованих водяних знаків може вказувати на те, чи була відеоінформація підроблена чи ні.

Audio and Video Data Security. Оскільки дані піддаються несанкціонованому втручанню або перегляду на рівні сприйняття, транспортному рівні або прикладному рівні, безпека аудіо-та відеоданих є пріоритетом систем відеоспостереження. Відповідно, пристрої Hikvision підтримують захист безпеки на етапах кодування і передачі.

Encoding. Аудіо та відеодані шифруються в процесі кодування, потім передаються і зберігаються в зашифрованому тексті, що ефективно запобігає несанкціонованому доступу до даних. Цифровий підпис аудіо-та відеоданих на етапі кодування підтримується, а дані передаються і зберігаються за допомогою цифрового підпису, ефективно запобігаючи несанкціонованому втручанню.

Transfer. HTTPS / TLS підтримується для передачі аудіо-та відеоданих по мережі, ефективно захищаючи від усіх видів кібератак.

Підписання коду програми. Після завантаження ядро пристрою визначить, які призначені для користувача процеси і додатки можуть бути запущені. Щоб гарантувати, що всі додатки взяті з затверджених відомих джерел і не були підроблені, всі виконувані коди повинні бути підписані сертифікатами, визнаними Hikvision. Цей обов'язковий підпис коду розширює концепцію ланцюжка довіри від операційної системи до рівня програми, ефективно запобігаючи запуску несанкціонованих додатків.

За допомогою підпису коду він гарантує, що всі виконувані коди авторизовані, запобігаючи запуску шкідливих кодів. На відміну від технології підписання коду через Інтернет, технологія в IoT може бути застосована не тільки на рівні додатків, але і на рівні мікропрограмного забезпечення. Коди, що працюють у кожному важливому пристрої (включаючи датчик, перемикач, тощо), повинні бути підписані, інакше вони не будуть виконані. Враховуючи обмежені ресурси деяких вбудованих пристроїв IoT, наприклад обмежену потужність процесора, комунікаційну ємність і обсяг пам'яті, Hikvision створила набір механізмів підпису коду, які адаптуються до характеристик IoT, балансуючи безпеку, ефективність і продуктивність.

Реалізація технологій Hikvision для захисту від атак. У перші дні існування IoT, пристрої та мережі були в основному призначені для роботи в ізольованому середовищі, а механізм безпеки був відносно незрілим. З швидким розвитком IoT ці пристрої і мережі поступово стали підключатися до Інтернету, що вводить нові проблеми безпеки. На додаток до вбудованого механізму безпеки, який захищає збережені данні в пристроях, існує також ряд заходів мережевої безпеки, доступних для забезпечення безпеки і точності інформації при передачі на пристрій і з нього.

Anti-ARP Spoofing Technology: ARP-спуфінг відноситься до безперервної відправки пакетів ARP-спуфинга для впровадження підроблених зіставлень IP-MAC в мережеві пристрої або хости, тим самим перехоплюючи дані, відправлені цільовому хосту (рис. 2).

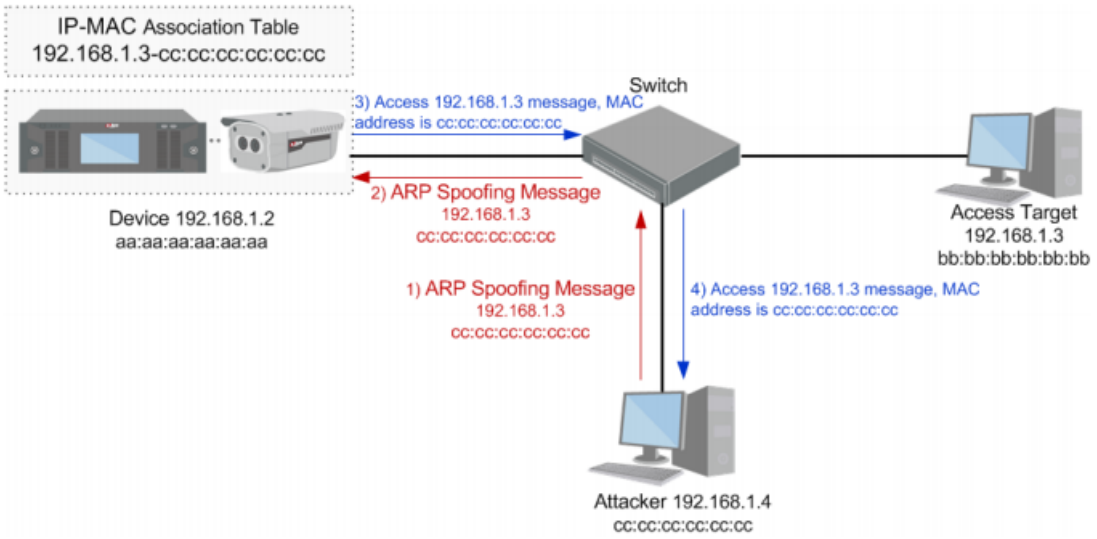

Рис. 2. Технологія Anti-ARP Spoofing

Підроблене зіставлення IP-MAC відноситься до відносин зіставлення, що складається з IP-адреси цільового хоста атаки і MAC-адреси атакуючого хоста. Технологія Anti-ARP spoofing використовується для зміцнення списку зіставлення IP-MAC вихідного хоста, блокування повідомлень ARP spoofing і запобігання імплантації підроблених відносин зіставлення IP-MAC.

Anti-DoS Attack Technology: Dos-атака означає, що зловмисник вичерпує службові ресурси цільового хоста, відправляючи шкідливі мережеві пакети, так що цільовий хост не може надавати звичайні послуги законним користувачам.

Пристрій Dahua надає захисні технології для наступних DoS атак:

ICMP Flood, відправляючи велику кількість пакетів повідомлень ICMP на пристрій, пристрій не може відповідати на законні запити обслуговування;

Syn Flood, який являє собою атаку на НАПІВЗ'ЄДНАННЯ TCP. Безперервно посилаючи підроблені запити на TCP-з'єднання, зловмисник змушує пристрій створювати велику кількість ресурсів TCP semi-connection, тим самим виснажуючи стек протоколів TCP і реалізуючи DoS-атаки.

Anti-DoS Attack Technology: Dos-атака означає, що зловмисник вичерпує службові ресурси цільового хоста, відправляючи шкідливі мережеві пакети, так що цільовий хост не може надавати звичайні послуги законним користувачам. Пристрій Dahua надає захисні технології для наступних DoS атак:

ICMP Flood, відправляючи велику кількість пакетів повідомлень ICMP на пристрій, пристрій не може відповідати на законні запити обслуговування;

Syn Flood, який являє собою атаку на НАПІВЗ'ЄДНАННЯ TCP. Безперервно посилаючи підроблені запити на TCP-з'єднання, зловмисник змушує пристрій створювати велику кількість ресурсів TCP semi-connection, тим самим виснажуючи стек протоколів TCP і реалізуючи DoS-атаки.

Password Anti-cracking Technology: Атака на злом пароля відноситься до використання високопродуктивного хоста для виконання високочастотних вгадувань пароля на цільовому пристрої до тих пір, поки пристрій не буде успішно увійшло в систему, щоб отримати правильний пароль для пристрою входу в систему.

Варіант системи відеоспостереження на базі рішення Hikvision

Варіант системи відеоспостереження розроблений на реальному досвіді проектування та побудови системи відеоспостереження в м. Виноградів з компанією Bezpeka Universal. IP-камери приймають відео в цифровому форматі, відстежують рух, без участі людського

фактора, самостійно можуть підключатися до веб-сервера. IP - камери можна налаштовувати з браузера та ПЗ. При необхідності, камери зможуть передати отримане відео миттєво на центральний сервер. Цифрові відеореєстратори (NVR) забезпечують зберігання архіву відео. Можна додати додатково камери відеоспостереження і збільшити масив зберігання даних. Передбачена резервна система зберігання інформації. Цифрові реєстратори можуть працювати з розгалуженою кількістю об'єктів, передаючи дані на центральний пункт. Програмне забезпечення дозволяє управляти настройками і адмініструвати камери та інше обладнання, аналізувати дані відеопотоку, одночасно записувати і переглядати відео. Передбачає великий арсенал засобів відеоаналітики.

Для реалізації проекту було розроблено план схему розміщення камер відеоспостереження в сквері міста Виноградів (рис. 3).

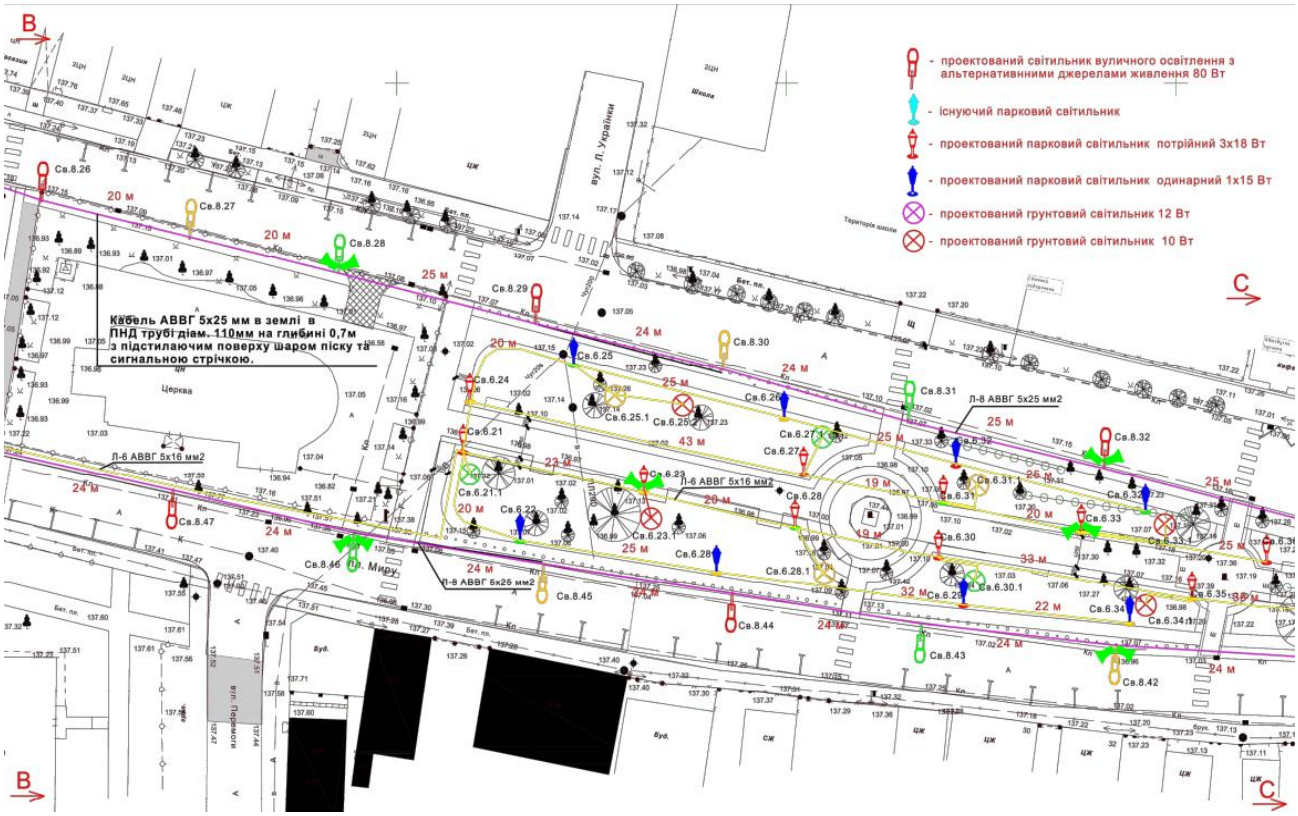

Рис. 3. Схема розміщення камер відеоспостереження

Нижче в табл. 1, наведена специфікація основного обладнання, яке використовувалось при побудові системи відеоспостереження та розробці технології застосування методів захисту систем відеоспостереження на базі рішення Hikvision. Після підключення камер відеоспостереження, було вирішено провести тестування робочих станцій з програмним комплексом IVMS 4200, для підбору оптимальної конфігурації, яка буде використана в робочих станціях операторів. Після тестування було виділено основні параметри які істотно впливають на ефективність робочих станцій, та було створено рекомендації щодо робочої станції оператора (табл. 2).

Рекомендації щодо застосування технологій захисту систем відеоспостереження

Системи виявлення та запобігання вторгнень. Основи кіберзахисту повинні враховуватися в кожній комп'ютерній мережі. Наприклад, для виявлення і запобігання зараження шкідливими програмами на терміналах користувачів і відеореєстраторах має бути встановлено антивірусне програмне забезпечення. У не розподілених топологіях POC повинен бути розгорнутий суворий брандмауер для передачі мінімального мережевого

трафіку, необхідного для використання системи (наприклад, блок telnet, пакети ICMP 'ping' і т.д.). У випадку, якщо противник ухиляється від брандмауера, система виявлення мережевих вторгнень (NIDS) може бути використана для виявлення шкідливих шаблонів трафіку. У цьому випадку можна використовувати безкоштовні засновані на правилах NiD, такі як Snort і Suricata, або комерційне програмне забезпечення.

Таблиця 1

Специфікація обладнання

Назва	Модель	Од. вимірювання	К-сть.
32-канальний 4K мережевий відеореєстратор	DS-7732NI-I4 (B)	шт.	2
4Мп IP відеокамера Hikvision с детектором облич і Smart функціями	DS-2CD2646G2-IZS	шт.	10
4 Мп IP відеокамера Hikvision	DS-2CD2T43G0-I8	шт.	24
Комутаційний бокс	DS-1260ZJ	шт.	24
4 Мп ColorVu IP відеокамера Hikvision	DS-2CD2347G2-LU	шт.	2
Настінний кронштейн	DS-1273ZJ-140	шт.	2
2Мп IP ColorVu камера Hikvision	DS-2CD1027G0-L	шт.	19
Комутаційний бокс	DS-1280ZJ-XS	шт.	19
Кронштейн для кріплення на стовп	DS-1275ZJ-SUS	шт.	17

Таблиця 2

Рекомендації щодо робочої станції оператора

Параметр	Рекомендації
Операційна система	Microsoft® Windows 10 64-bit
CPU	Intel® Core™ i5 Processor або кращий
GPU	Nvidia GTX1050Ti або кращий
Memory	8 GB або більше
Resolution	1920×1080

Конфігурації та шифрування. Слід уважно вивчити конфігурацію камер, маршрутизаторів, терміналів і відеореєстраторів. Наприклад, слабкі або стандартні паролі повинні бути змінені, і різні паролі повинні використовуватися серед різних пристроїв, якщо це можливо. Крім того, API та інші подібні функції повинні бути відключені, якщо вони не потрібні. Слід також періодично перевіряти наявність нових CVE, щоб програмне забезпечення/прошивка всіх пристроїв були актуальними [8]. Це пов'язано з тим, що зловмисник все одно зможе перехопити відеопотік (наприклад, перенаправити або призупинити відео в потоці RTSP) або скомпрометувати відеореєстратор за допомогою витоку облікових даних. Деякі виробники програмного забезпечення DVR використовують самопідписані SSL-сертифікати (звичайна настройка за замовчуванням). Це значний ризик, оскільки він дозволяє зловмиснику виконати атаку SSL man in the middle redirection [9].

Обмеження фізичного доступу. Найголовніша захист периметра полягає в обмеженні фізичного доступу до активів системи. Якщо це можливо, проводка не повинна проходити через громадські зони, все мережеве обладнання (комутатори, маршрутизатори і т. д.) має бути захищене замком і ключем, а доступ до системи повинен управлятися, реєструватися і контролюватися.

Захист від DoS-атак. Існує безліч протоколів і вразливостей, які можуть бути використані для виконання DoS-атаки. В результаті виникає безліч різних захисних механізмів, які можуть бути задіяні. Хороший захист включає в себе наступні кроки: (1) виявлення ініціації атаки, (2) Вибір шкідливих/шкідливих пакетів і (3) фільтрація/реєстрація виявлених пакетів. Для виявлення атак можна використовувати машинне навчання і статистичні методи, такі як полегшене виявлення аномалій і багато іншого.

Захист від атак MitM. Правильне шифрування повинно використовуватися для запобігання підслуховування і маніпулювання пакетами (наприклад, ін'єкції відео) в

результаті атаки MitM. Однак іноді в протоколах шифрування виявляються уразливості, і системи можуть бути неправильно налаштовані. Тому в якості додаткової лінії оборони можуть бути розгорнуті додаткові методи. Для виявлення фальсифікації (відеоін'єкції) можна відрахувати час по тіньових позиціях. Однак цей метод працює тільки в обмежених обставинах. Інший варіант полягає у вимірюванні сигналів частоти електричної мережі (ENF) як природної часової мітки в закритих приміщеннях [10]. Більш поширеним підходом до перевірки цілісності зображення є водяні знаки [11].

Навчання. Просунуті постійні загрози (APT) – це добре організована атака на організацію, яка охоплює безліч кроків атаки до тих пір, поки мета атаки не буде досягнута [20]. У APT початкове вторгнення часто відбувається у формі атаки соціальної інженерії, коли співробітника обманом змушують надати облікові дані або встановити шкідливе ПЗ. Найбільш ефективним способом пом'якшення цих початкових вторгнень є: (1) навчання користувачів системи потенційним векторам атаки і (2) попередження користувачів бути обережними з небажаними повідомленнями і запитами, зробленими під помилковими приводами [12].

Висновки

У роботі запропоновано варіант технології захисту систем відеоспостереження на базі рішення Hikvision. Для виконання цих завдань система відеоспостереження на базі рішення Hikvision повинна комплексно працювати з системою виявлення та запобігання вторгнень. На пристроях системи відеоспостереження необхідно налаштовувати функції та політики доступу, шифрування, забезпечити обмеження фізичного доступу до пристроїв відеоспостереження на провести обов’язкове навчання користувачів системи щодо можливих векторів атак на систему.

Таким чином, правильна реалізація технології захисту систем відеоспостереження на базі рішення Hikvision має забезпечити ефективний захист конфіденційних даних та кібербезпеку системи відеоспостереження.

Перелік посилань

1. Cabasso, J. Analog vs. IP cameras. Aventura Technol. Newsl. 2009, 1, 1–8.
2. Statista. Security & Surveillance Technology Statistics & Facts. Technical Report. 2015. // [Електронний ресурс]. URL: https: //www.statista.com/topics/2646/security-and-surveillance-technology/
3. Mukkamala, S.; Sung, A.H. Detecting denial of service attacks using support vector machines. In Proceedings of the 12th IEEE Int. Conf. on Fuzzy Systems, St. Louis, MO, USA, 25–28 May 2003; pp. 1231–1236.
4. Peeping into 73,000 Unsecured Security Cameras Thanks to Default Passwords. // [Електронний ресурс]. Режим доступу: World Wide Web. – URL: https://www.csoonline.com/article/2844283/peeping-into-73-000-unsecured-security-cameras-thanksto-default-passwords.html
5. Akhtar, N.; Mian, A. Threat of adversarial attacks on deep learning in computer vision: A survey. IEEE Access 2018, 6, 14410–14430. // URL: https://ieeexplore.ieee.org/document/8294186
6. Liu, Z.; Peng, D.; Zheng, Y.; Liu, J. Communication protection in IP-based video surveillance systems. In Proceedings of the Seventh IEEE International Symposium on Multimedia, Irvine, CA, USA, 14 December 2005; p. 8.
7. Guri, M.; Elovici, Y. Bridgeware: The air-gap malware. Commun. ACM 2018, 61, 74–82. // [Електронний ресурс]. Режим доступу: World Wide Web. – URL: https://dl.acm.org/doi/10.1145/3177230
8. Liu, F.; Koenig, H. A survey of video encryption algorithms. Comput. Secur. 2010, 29, 3–15. // [Електронний ресурс]. URL: https://www.sciencedirect.com/science/article/pii/S0167404809000698?via%3Dihub
9. Mitmproxy—An Interactive HTTPS Proxy. // [Електронний ресурс]. Режим доступу: World Wide Web. – URL: https://mitmproxy.org/
10. Bala, R. A Brief Survey on Robust Video Watermarking Techniques. Int. J. Eng. Sci. 2015, 4, 41–45.
11. Garg, R.; Varna, A.L.; Wu, M. Seeing ENF: natural time stamp for digital video via optical sensing and signal processing. In Proceedings of the 19th ACM International Conference on Multimedia; Association for Computing Machinery: New York, NY, USA, 2011; pp. 23–32.
12. Колісник Д. Р., Місевич К. С., Коваленко С. В. Системна архітектура IoT-Fog-Cloud для систем аналізу великих даних і кібербезпеки: огляд туманних обчислень, впровадження аудиту інтернету речей // [Електронний ресурс]. – Науковий журнал «Сучасний захист інформації». – Київ, ДУТ. – с. 34-38

Надійшла: 16.07.2021 Рецензент: д.т.н., доцент Ахрамович В.М.