УДК 004.056:621.397.42

Анализ уязвимостей и методов защиты IoT-устройств на примере систем видеонаблюдения

И.И. Андреев
студент 3-го курса бакалавриата НИЯУ МИФИ, Москва
Email: mega.igory@bk.ru
А.А. Бикмухаметов
студент 3-го курса бакалавриата НИЯУ МИФИ, Москва
Email: amir_bikmukhametov@mail.ru
С.В. Тарасов
студент 3-го курса бакалавриата НИЯУ МИФИ, Москва
Email: sergej.tarasov.04@bk.ru
В.А. Рычков
старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва
Email: VARychkov@mephi.ru
В.И. Рычкова
старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва
Email:virychkova@mephi.ru

Аннотация: *В статье проводится комплексный анализ уязвимостей систем видеонаблюдения как одного из наиболее распространенных и уязвимых сегментов IoT. Исследуются технические аспекты различных векторов атак, приводятся конкретные примеры критических уязвимостей, а также предлагаются методы защиты на разных уровнях архитектуры IoT.*

Ключевые слова: *Internet of Things, IoT, IoVT, cybersecurity, video surveillance, vulnerabilities, protection methods, botnet, DDoS attacks, authentication, network segmentation*

Analysis of vulnerabilities and methods of protection of IoT devices on the example of video surveillance systems

I.I. Andreev
3rd year Bachelor's degree student at NRNU MEPhI, Moscow
Email: mega.igory@bk.ru
A.A. Bikmukhametov
3rd year Bachelor's degree student at NRNU MEPhI, Moscow

Email: amir_bikmukhametov@mail.ru
S.V. Tarasov
3rd year Bachelor's degree student at NRNU MEPhI, Moscow
Email: sergej.tarasov.04@bk.ru
V.A. Rychkov
Senior Lecturer of the department of financial monitoring
NRNU MEPhI, Moscow
Email: VARychkov@mephi.ru
V.I. Rychkova
Senior Lecturer of the department of financial monitoring
NRNU MEPhI, Moscow
Email: virychkova@mephi.ru

Abstract: *The article provides a comprehensive vulnerability analysis of video surveillance systems as one of the most widespread and vulnerable segments of IoT. Technical aspects of various attack vectors are investigated, specific examples of critical vulnerabilities are given, and defense methods at different levels of IoT architecture are proposed.*

Keywords: *Internet of Things, IoT, IoVT, cybersecurity, video surveillance, vulnerabilities, protection methods, botnet, DDoS attacks, authentication, network segmentation*

Введение

К 2025 ожидается рост количества Интернет вещей (IoT), а именно - 20,1 млрд. устройств [1]. Даже сейчас Интернет вещей активно развивается и внедряется во все сферы жизни - от промышленности до сельского хозяйства. Но по мере увеличения разнообразия и количества устройств увеличивается и количество возможных кибератак. По данным jumpcloud, уже сегодня более 50% устройств IoT имеют критические уязвимости, которыми могут воспользоваться хакеры [2]. В данной статье рассматриваются основные уязвимости IoVT-систем, проводится анализ потенциальных угроз и предлагаются методы комплексной защиты различных элементов IoVT-системы в различных кейсах.

Основные понятия в сфере Интернета вещей

Прежде чем углубляться в тему, разберем основные термины, которые будут использоваться далее:

IoT (Internet of Things, Интернет вещей) представляет собой физические устройства, оснащенные технологиями для взаимодействия между собой и внешней сетью для сбора, обмена и анализа данных. Примеры: умные часы, термостаты [3].

IIoT (Industrial Internet of Things, Промышленный Интернет вещей) - подмножество IoT, которые ориентируются на промышленные приложения. Они используют такие технологии, как межмашинный обмен

(M2M), большие данные и машинное обучение, что повышает их эффективность и надежность. Примеры: робототехника, автоматизированные производственные линии [3].

OT (Operational Technology, Операционные технологии) относится к объединению в сеть операционных процессов и промышленных систем управления (ICS), включая человеко-машинные интерфейсы [4]. В отличие от информационных технологий (IT), сфокусированных на обработке данных, OT отвечает за управление физическими процессами, оборудованием и инфраструктурой [3].

ICS (Industrial Control Systems, Промышленные системы управления) – это системы, используемые для управления промышленными процессами. Они включают SCADA (системы диспетчерского управления и сбора данных), DCS (распределенные системы управления) и другие автоматизированные решения для контроля производства [3].

IoVT (Internet of Video Things) — это подмножество IoT, объединяющее устройства, которые собирают, обрабатывают и передают видеоданные в реальном времени. Такие системы широко применяются в умных городах, видеонаблюдении, промышленной автоматизации и даже в потребительских решениях (например, умные камеры, дроны, системы распознавания лиц).

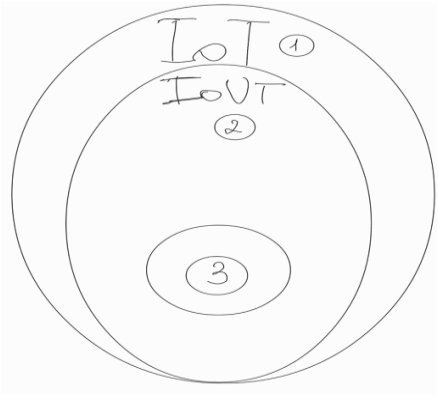

Рисунок 1 – Разделение IoT, где 1 – IoT, 2 – IoVT, 3 – Видеонаблюдение

Актуальность IoT.

Влияние Интернета вещей на нашу жизнь трудно переоценить:

- 62% производителей внедряют технологии IoT в процесс производства или сборки;
- Технологии сотовой связи IoT в настоящее время составляют около 21% глобальных соединений IoT;
- В 2022 году рынок Интернета медицинских вещей оценивался в 158 миллиардов долларов

- По прогнозам, к концу 2025 года выручка автомобильной отрасли Интернета вещей составит около 23,6 млрд долларов.
- 21% взрослого населения США носят умные часы
- Рынок IoT оценивается в $714,48 млрд в 2022 году, а к 2023 предполагался более триллиона долларов [1].

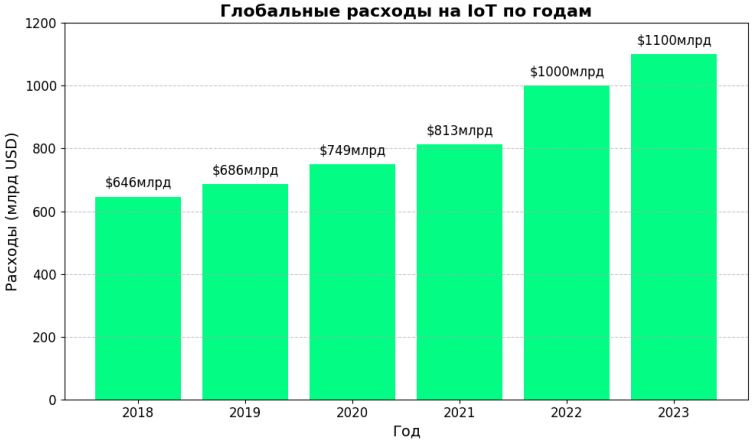

График 1 – Расходы на IoT по всему миру

Но несмотря на такие внушительные цифры, количество кибератак на такие устройства тоже вырастет с каждым годом. Лишь за 2022 было зарегистрировано более 100 млн случаев кибератак по всему миру.

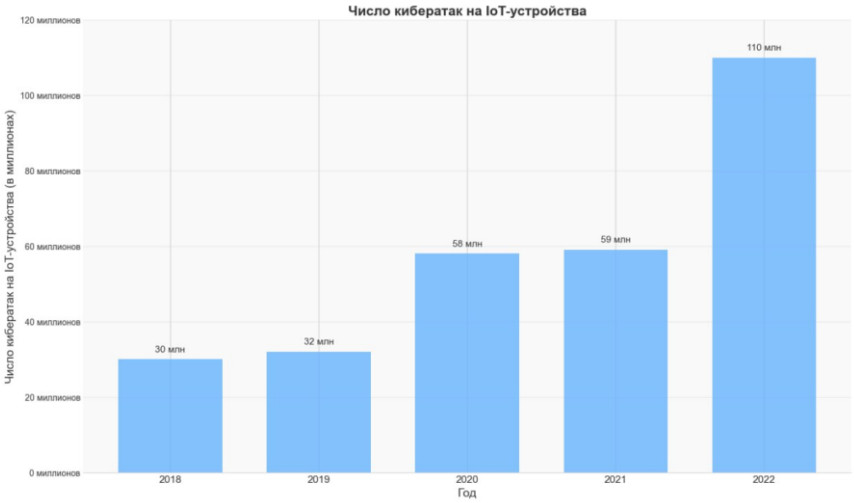

График 2 – Количество кибератак на Интернет вещи

Так же статистика говорит следующее:

- Более 50% устройств IoT имеют критические уязвимости, которыми хакеры могут воспользоваться прямо сейчас.
- Сбой в системе безопасности Интернета вещей в среднем обходятся в $330000, а также к простою на 6,5 часов на один инцидент.
- Каждое пятое устройство использует пароль по умолчанию, что делает их легкими для взлома.
- На IoT-ботнеты приходится около 35% DDoS-атак

Помимо этого, такие отрасли, как здравоохранение, умные города, промышленность особенно сильно подвергаются атаке хакеров [2].

Актуальность IoVT

Поскольку различных типов Интернет вещей слишком велико, а различных атак на них еще больше, то мы не сможем рассмотреть все атаки на IoT. Поэтому, вместо этого, рассмотрим одно конкретное устройство.

По данным ИБ-компании SAM Seamless Network, почти половина всех атак на IoT-устройства (47%) приходится на домашние камеры и системы видеонаблюдения, что делает их самыми популярными устройствами для взлома [5].

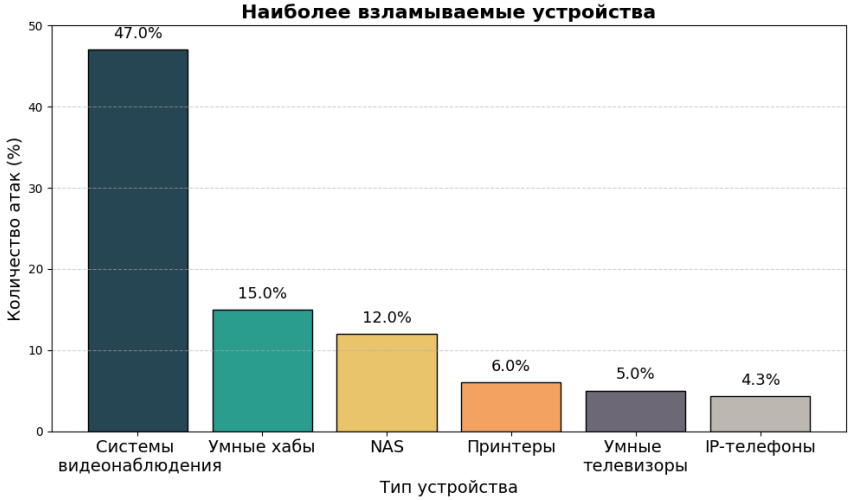

График 3 – Распределения по количествам атак на разные Интернет вещи

Во-вторых, их количество с каждым годом продолжает расти, потому что они автоматизируют такие процессы, как повышение эффективности за наблюдением места преступления, распознавание лиц и многое другое [6]. В-третьих, около 43% владельцев беспокоятся, что их могут взломать [7]. Это говорит о высокой потребности в безопасности. В-четвертых, многие камеры подключены к Интернету, что означает, что через них можно

украсть ваши персональные данные, не говоря о том, что некоторые из них вообще имеют открытые базы данных MySQL.

Самой популярной и простой атакой, направленной на взлом камер, является DDoS-атака. Причем среди всех многовекторных DDoS-атак, самой частой (31%) как раз является атака на сферу телекома [8].

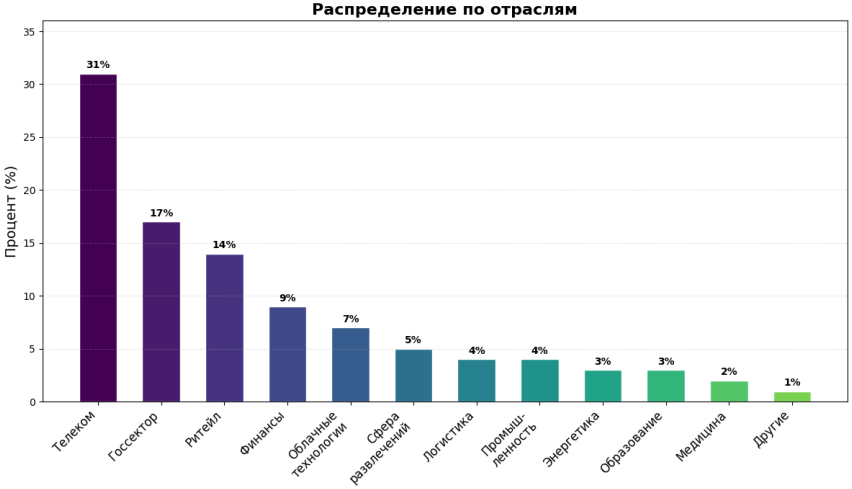

График 4 – Распределения по количествам атак на разные Интернет вещи

Это следствие того, что камеры могут быть внедрены в различные отрасли - начиная от банков и заканчивая логистикой. Зачастую камеры имеет внутреннюю сеть, которая связывает все устройства в едино. Поэтому хакеры после взлома одного устройства сразу переходят ко второму, потом к третьему и т.д. После того, как они получили доступ к сотням камер, можно целенаправленно взломать или вывести из строя какое-либо устройство или программу. Такой подход называется ботнет.

Ботнеты – это сети, состоящие из компьютеров, захваченных киберпреступниками, которые те используют для различных махинаций и кибератак [9].

Виды ботнетов [9][10].

Для управления ботнетом надо отдавать команды, и при этом делать это анонимно. Для этого используют 2 модели управления: напрямую или опосредственно.

Централизованная клиент-серверная модель - ботмастер управляет ботнетом через единый сервер, иногда используют несколько дополнительных серверов, которые называют прокси. В таком случае все команды исходят от ботмастера и передаются в соответствии с иерархией. Такой метод очень просто в использовании, но также очень прост в обнаружении.

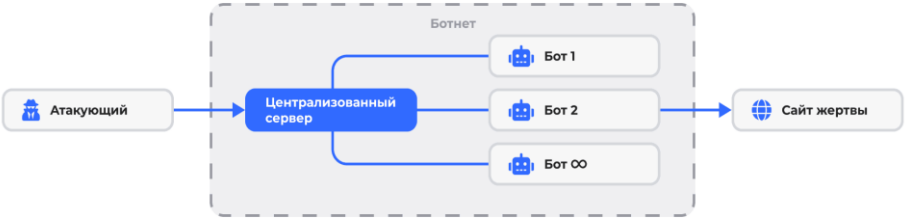

Рисунок 2 – Модель “Клиент-сервер”

Децентрализованная пиринговая модель (P2P) сложнее, но и обнаружить ее гораздо тяжелее. Каждое устройство может выполнять роль клиента и сервера, что обеспечивает передачу команд и данных по всей сети. Т.е. пока ботмастер может связаться хотя-бы с одним устройством, команды будут передаваться. Отсутствие центрального сервера снижает уязвимость сети и затрудняет контроль со стороны специалистов по безопасности

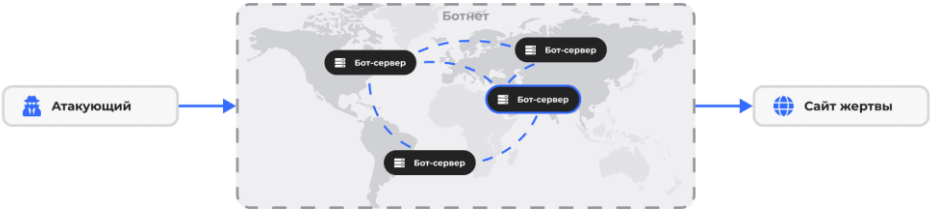

Рисунок 3 – P2P модель

В основном ботнеты используются для DDoS-атак, но также могут быть использованы для фишинга, брутфорс-атак, скликивания или майнинга криптовалюты. [11]. Нас же интересует первый вариант.

DDoS-атака.

DDoS-атака - тип кибератаки, при которой злоумышленники отправляют поддельные запросы на сервер или сеть с целью перегрузить их и сделать недоступными для обычных пользователей [12].

Самой популярной и известной атакой была Mirai. Этот ботнет как раз таки искал уязвимости в бытовых устройствах, из-за того, что во многих из них логин и пароль были однотипны или вообще одинаковы. И если Вы подумаете, что такого не может быть, то чуть ниже представлен топ-10 наиболее популярных комбинаций имен пользователей и паролей службы Telnet, которые киберпреступники использовали в 2019 году при осуществлении атак на IoT-устройства. Все эти комбинации были включены в Mirai.

Рисунок 4 – наиболее популярных комбинаций имен пользователей и паролей

Позже от Mirai пойдут такие боты, как Mantis и Eleven11bot[13][14] . Кстати, последний использовал в основном камеры видеонаблюдения и сетевые видеорегистраторы, а атаковал телекоммуникационные компании и игровые платформы. Да и было это относительно недавно - 3 месяца назад.

Угрозы систем IP-видеонаблюдения

Системы видеонаблюдений представляют собой самую уязвимую категорию IoT, а именно - 47%. Широкое распространение этих устройств во всех промышленных сферах, постоянное подключение к сети, доступ к конфиденциальным данным делает эти устройства очень привлекательными для хакеров. В этом разделе будет проведен анализ различных атак, с приведенными примерами и предложены рекомендации против их действия.

1. Удаленное выполнение кода (RCE - Remote Code Execution)

Внедрение кода — это использование уязвимости, возникающей из-за некорректной обработки входящих данных, в результате чего эти данные могут быть интерпретированы сервером как код. Злоумышленник может использовать этот метод для получения конфиденциальной информации или установки вредоносного ПО. Приведем несколько типов уязвимостей выполнения произвольного кода:

- SQL-инъекция. Если камера хранит информацию о пользователях и паролях в базе данных, то программа может быть уязвима к SQL-инъекциям.
- Переполнение стекового буфера. В процессе работы ПО, при попытке записи данных в стековый буфер, превышающих его заранее определенный размер, происходит выход за пределы выделенной области

памяти. Это приводит к перезаписи смежных участков памяти, в которых могут располагаться важные данные или исполняемый код. Злоумышленник может внедрить и выполнить произвольный код.

Практический пример уязвимости: Инъекция команд через параметр HTTP-запроса в IP-камерах AVTECH AVM1203 (CVE-2024-7029) [15]

Приведем пример уязвимости, имеющей серьезные последствия эксплуатации и высокий уровень критичности. Это одна из классических уязвимостей - Инъекция команд через параметр HTTP-запроса. Степень серьезности этой проблемы усугубляется тем, что само устройство больше не будет получать обновлений ПО, следовательно, все уже выпущенные устройства, достоверно уязвимые, являются угрозой безопасности для системы, в которой они установлены. Первые доказательства существования этой уязвимости появились в 2019 году, после чего камера была снята с производства, из-за чего и не планируется обновлений ПО. Тем не менее, данные камеры до сих пор установлены на коммерческих объектах, в финансовых организациях, заметно снижая их безопасность. Так же, эту камеру до сих пор можно приобрести в некоторых магазинах оборудования для систем безопасности.

Уязвимый хост: веб-сервер IP-камеры AVTECH AVM1203, эндпоинт /cgi-bin/supervisor/Factory.cgi

CWE-77: Командные инъекции

Критичность: Высокая (CVSS Score – 8.7)

CVSS v4.0 Vector: V:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N.

Описание:

В IP-камерах AVTECH AVM1203 обнаружена критическая уязвимость к инъекции команд через параметр яркости (brightness) HTTP-запроса. Эта уязвимость позволяет злоумышленнику, даже без аутентификации, выполнять произвольные команды непосредственно на устройстве.

Риск:

В результате эксплуатации данной уязвимости злоумышленник получает возможность полного контроля над устройством. Это открывает возможности для включения камеры в ботнет-сеть, несанкционированного доступа к видеопотоку и использования устройства как точки входа в защищенную сеть организации. Так как любые IoT-устройства, в том числе IP-камеры, имеют вычислительные мощности, интересующие злоумышленников с точки зрения использования их как часть ботнет-сети, частым последствием атаки, которая не является направленной на конкретного человека или конкретную компанию, является заражение устройства, использование или продажа его как бота.

Технические детали:

Уязвимость вызвана отсутствием должной санитизации входных данных в реализации функции управления яркостью и использованием

устаревшего ядра Linux 2.6.32, библиотеки которого имеют известные уязвимости (это упрощает эскалацию привелегий). При обработке HTTP-запроса с параметром brightness система не выполняет проверку и фильтрацию вводимых данных, позволяя внедрить команды операционной системы, которые затем выполняются с привилегиями веб-сервера камеры.

Шаги для воспроизведения:

Отправка вредоносного HTTP-запроса, аргумент brightness параметра action несет вредоносную нагрузку. Например, с помощью команды wget загружаем и исполняем вредоносный скрипт на ОС устройства.

POST /cgi-bin/supervisor/Factory.cgi HTTP/1.1

action=white_led&brightness=$(wget http://malware.cc/bot.sh -O /tmp/bot; chmod +x /tmp/bot; /tmp/bot)

Рекомендации:

Методов полного исключения данной уязвимости при использовании этих камер на данный момент не предвидится, то есть они подлежат замене. Неофициальные патчи данной уязвимости как хорошее решение с точки зрения безопасности не рассматриваются.

Методы митигации последствий эксплуатации данной уязвимости:

- Сегментация сети, изоляция камеры от потенциально вредоносного трафика.
- Минимизация количества используемых сервисов на камерах для уменьшения поверхности атаки.
- Использование межсетевых экранов для фильтрации трафика к уязвимым устройствам.
- Регулярный мониторинг сетевой активности камер на предмет попыток взлома.

CISA (агентство Министерства внутренней безопасности США) в (ICSA-24-214-07) подтверждает высокую (CVSS Score 8.7) угрозу данной уязвимости [16].

2. Манипулирование и наблюдение за сетевым трафиком.

Злоумышленник может осуществлять манипуляции, перенаправление или наблюдение за сетевым трафиком. Например, для атаки "человек посередине" (MitM, Man-In-The-Middle attack) злоумышленник может перенаправить трафик через себя с помощью отравления ARP (ARP spoofing) и подмены DHCP/DNS. Далее, для внедрения может быть использован инструмент VideoJak, который эксплуатирует незашифрованные видеопотоки по протоколам RTSP или RTP, которые часто встречающихся в системах видеонаблюдения.

Даже при использовании шифрования возможно извлечение информации о видеоконтенте на основе анализа паттернов трафика, обусловленных алгоритмами сжатия видео и буферизацией, а также получение топологической информации сети из трафика UPnP и

обнаружение учетных данных в открытом виде в HTTP-трафике, что подчеркивает уязвимость IP-видеонаблюдения к подобным атакам.

3. Утечка информации.

Камеры могут быть использованы для передачи информации злоумышленнику. Например, вредоносная программа, содержащаяся в изолированной сети, может мигать светодиодом в поле зрения камеры, подключенной к Интернету. Изменяя режим мигания, злоумышленник может перенести часть украденной информации в удаленное место. Это было продемонстрировано на жестких дисках, мониторах и сетевом оборудовании [17].

Практические примеры уязвимости:

Хранение паролей в файлах конфигурации IP-камер и цифровых видеорекордеров (DVR) Dahua

CVE-2017-7925[18] ;

Критичность: Критическая

Уязвимый хост: веб-сервер сетевых IP-камер и цифровых видеорекордеров Dahua Technology Co., Ltd (Dahua), эндпоинт /current_config/passwd

CWE-260 - Пароли в файлах конфигурации.
(доп. CWE-522 - Недостаточная защита учетных данных.)
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS Score = 9.8

Описание:

Уязвимость микропрограммного обеспечения затрагивает 15 серий устройств (12 IP-камер и 3 цифровых видеорекордеров) - хранение паролей в конфигурационных файлах, что позволяет злоумышленнику получать конфигурационные файлы, снимки с камер и учетные данные администратора без аутентификации [19][20].

Риск:

На момент 2017 года было обнаружено 1140446 уязвимых устройств по всему миру, уязвимость эксплуатировалась для создания ботнет-сетей.

Технические детали:

Уязвимость позволяет злоумышленнику получить доступ к конфигурационным файлам, хранящим конфиденциальные данные, в том числе хэши паролей, используя неаутентифицированный HTTP-запрос. Используются эндпоинты /current_config/passwd и /current_config/Account1

Шаги для воспроизведения:

Найти устройство, просканировав сеть, Dahua устройства можно идентифицировать, например, по уникальному хэшу иконки веб-интерфейса (т.е. выставив фильтр hash:2019488876) [21]

“curl http://IP_устройства/current_config/passwd”

Ответ содержит хэши паролей, имя пользователя, уровень привилегий.

Получая хэши паролей для разных пользователей, злоумышленник может провести их деобфускацию, т.к. MD5 считается криптографически неполноценным методом шифрования и страдает от множества уязвимостей.

Эта проблема отягощается тем, что на части устройств присутствует ограничение длины пароля не более, чем 6 символами, что позволяет без больших временных затрат провести оффлайн брутфорс-атаку.

Рекомендации:

Методы митигации последствий эксплуатации данной уязвимости: совпадают с методами митигации последствий эксплуатации cve-2024-7029, т.е. сегментация сети и использование межсетевых экранов, мониторинг активности и реагирование. В данном случае, уже реализованы патчи и обновления, которые исключают данную уязвимость, но многие уже не поддерживаются, что означает, что их использование небезопасно, обязательна физическая изоляция [22].

Так же, с устройствами Dahua связана уязвимость CVE-2017-7927 категорий CWE-798 - хранение конфиденциальных данных в коде, CWE-836 - использование хэшей паролей для аутентификации.

Серверы Dahua использовали хэши паролей для аутентификации вместо паролей, т.е. злоумышленнику, получившему пароль, не требовалось даже проводить деобфускацию. В результате он получал контроль над устройством.

Уязвимость Hikvision CVE-2017-7921

Критическая уязвимость неправильной аутентификации в IP-камерах Hikvision серий DS-2CD2xx2F-I, DS-2CD2xx0F-I и других. Позволяет злоумышленнику получать конфигурационные файлы, снимки с камер и учетные данные администратора без аутентификации. CVSS оценка: 10.0 (критическая).

Это уязвимость категории CWE-287 - неправильная аутентификация. Эксплуатация уязвимости позволяла злоумышленнику повышать привилегии, получать доступ к видеопотокам, использовать устройство в ботнет-сетях, по сути, полноценное управление устройством. На момент 2017 года, более миллиона камер были уязвимы, при этом все устройства получили в будущем необходимые обновления ПО, но случаи эксплуатации уязвимости были и после этого, т.к. не все оборудованные камерами системами вовремя устанавливают обновления, некоторые камеры имели стороннее, неофициально измененное ПО [23][24][25].

4. Атаки, вызывающие перегрузку и нарушения функционирования (Flooding and Disrupting).

Злоумышленник может целенаправленно выводить из строя сервисы и делать недоступными данные посредством организации атак, направленных на перегрузку сетевой инфраструктуры. Классические примеры атак:

● DoS-атака (Denial of Service - отказ в обслуживании), заключающаяся в массированной отправке пакетов на камеру. Перегрузка ресурсов приводит к блокировке новых или уже существующих сессий связи. Инструменты типа hping3 позволяют реализовывать SYN-флуд, выводя из строя веб-серверы, или UDP-флуд, приводящий к перегрузке сетевого интерфейса.

● Атаки на VPN-туннели. В случае использования VPN-туннелей, злоумышленник способен нарушить работу системы видеонаблюдения путем перегрузки VPN-шлюза, доступного из сети Интернет, что приводит к разрыву соединения со всеми подключенными камерами. Подобные атаки могут быть осуществлены, например, посредством отправки большого количества запросов на установление защищенного соединения по протоколу ISAKMP (Internet Security Association and Key Management Protocol - Ассоциация интернет-безопасности и протокол управления ключами).

● Атаки с использованием усиления SSDP (Simple Service Discovery Protocol). В этой атаке агент заставляет камеры отправлять большое количество метаданных UpnP по IP-адреса видеорегистратора.

● Уязвимость IP-камер из-за ограниченных ресурсов. IP-камеры особенно уязвимы к подобным атакам ввиду ограниченных вычислительных ресурсов. В частности, некоторые модели поддерживают лишь до 80 одновременных HTTP-соединений, что относительно легко исчерпать. Атака с регенерацией SSL заключается в многократном инициировании процедуры пересогласования ключей, перегружая центральный процессор устройства.

5. Сканирования и разведка.

В рамках подготовки к атаке, субъект угрозы может инициировать сетевое сканирование с целью получения информации о топологии сети: идентифицировать доступные ресурсы, обнаружить открытые сетевые порты и определить активные сервисы, которые могут быть потенциально использованы для эксплуатации уязвимостей. Для проведения сетевого сканирования могут быть использованы такие инструменты, NMAP, позволяющие построить карту сети и выявить информацию о подключенных хостах. Помимо сканирования сетевой инфраструктуры, злоумышленник может также собирать сведения о веб-сервисах, запрашивая информацию о версиях программного обеспечения. С целью обнаружения потенциальных уязвимостей, к открытым веб-интерфейсам могут быть применены методы фаззинга (техника тестирования программного обеспечения). Ввиду высокой вероятности обнаружения, фаззинг обычно осуществляется вне целевой инфраструктуры.

6. Атаки методом полного перебора (Brute-Force attack).

Данная атака представляет собой попытку угадать правильный ввод данных, используя множество возможных вариантов. Атаки методом

перебора могут использоваться для выявления учетных данных пользователя, таких как имена пользователей и пароли. Эти атаки можно предотвратить, ограничив допустимое количество неудачных входов в систему за определенное время. Однако в некоторых случаях производители камер не реализуют эту функцию безопасности. Чтобы быстро найти решение, можно использовать словарь распространенных паролей в качестве базы для подбора.

В качестве примера можно привести атаку, использовавшую вредоносную программу Mirai, которая распространялась на другие устройства путем подключения по Telnet, используя словарь из 62 общих учетных данных, используемых камерами, видеорегистраторами и IOT-устройствами [26].

Аналогичные подходы были реализованы вредоносным программным обеспечением Remaiten и Aidra, которое компрометировало камеры и другие устройства IoT. Например, камеры FOSCAM оказались уязвимыми к атакам методом полного перебора из-за отсутствия соответствующей защиты, при этом длина допустимого пароля была ограничена 12 символами [27].

7. Социальная инженерия.

Данный вид атаки представляет собой комплекс методов психологического воздействия, направленных на манипулирование человеком с целью побуждения его к совершению действий, отвечающих интересам злоумышленника.

К числу распространенных атак, основанных на принципах социальной инженерии, относятся фишинг (fishing) и приманки (baiting). Фишинг предполагает отправку сообщений (электронная почта, SMS и т.п.), замаскированных под сообщения от надежного источника, с целью подтолкнуть получателя к установке вредоносного ПО или раскрытию учетных данных. В случае приманки злоумышленник распространяет мультимедийные устройства (например, USB-накопители или карты microSD), содержащие вредоносный код. Не подозревающая жертва, подключая такое устройство к своему компьютеру, подвергает его заражению. Для реализации подобных атак могут использоваться как свободно распространяемые инструменты, так и специализированные комплексы, входящие в состав дистрибутива Kali Linux.

8. Физический доступ.

Это категория атак, при которых злоумышленник осуществляет действия, требующие непосредственного физического контакта с системами видеонаблюдения, что позволяет ему осуществлять манипуляции, которые не осуществимы при дистанционном воздействии.

Примерами таких действий являются установка прослушивающих устройств, внедрение бэкдоров в аппаратное обеспечение, получение несанкционированного доступа к терминалу в серверной комнате,

модификация прошивки камер, физическое препятствие обзору камеры видеонаблюдения или преднамеренное повреждение кабельной инфраструктуры.

9. Состязательное машинное обучение.

Видеонаблюдение требует как ручной, так и автоматизированной обработки видеоконтента с целью выявления значимых событий, таких как несанкционированные вторжения или установление местонахождения подозреваемых. В связи с этим, для минимизации человеческих усилий применяются методы видеоаналитики. В случае масштабных систем, примером которых является государственная система видеонаблюдения в Китае, автоматизированные методы становятся необходимостью. К таким технологиям относятся распознавание лиц, обнаружение событий и отслеживание объектов. Однако, поскольку большинство из этих технологий основаны на машинном обучении, они подвержены враждебным атакам. Враждебная атака представляет собой злонамеренное использование модели машинного обучения, реализуемое посредством отравления модели на этапе обучения с целью принуждения модели к действиям, соответствующим намерениям злоумышленника, формирования входных данных, приводящих к непредсказуемому выходному результату, или получения информации об обучающих данных или самой модели путем анализа взаимосвязи между входом и выходом. Враждебные атаки на указанные технологии могут позволить злоумышленнику избежать обнаружения, фальсифицировать распознавание объекта или даже вызвать DoS-атаку (отказ в обслуживании) за счет повышения частоты ложных срабатываний.

В качестве примера враждебных атак на системы видеонаблюдения можно привести следующие сценарии:

- Злоумышленник может разработать цветные оправы очков, ношение которых приводит к изменению идентификации человека в перспективе глубокой нейронной сети, осуществляющей мониторинг изображений. Данная атака может быть использована не только для уклонения от обнаружения, но и для выдачи себя за другое лицо [28].
- Другим примером атаки на эти системы является DoS-атака, в которой злоумышленник перегружает систему ложными срабатываниями для потребления значительных вычислительных ресурсов, например, путем ношения одежды с изображениями, имитирующими номерные знаки, что приводит к перегрузке камер дорожного наблюдения [29] .
- Злоумышленник может попытаться перегрузить систему миллионами ложных тревог, скрывая важные предупреждения и уведомления от поля зрения группы реагирования. Это может быть достигнуто путем создания враждебных изображений, содержащих тысячи паттернов, вызывающих срабатывание детектора объектов. Например,

одиночное изображение, содержащее множество незаметных паттернов оружия или лиц.

- Системы видеонаблюдения, основанные на искусственном интеллекте и предназначенные для измерения интенсивности дорожного движения, могут быть обмануты и сообщать о дорожных заторах или их отсутствии. Это дает злоумышленнику возможность влиять на дорожное движение в соответствии со своими потребностями, создавать хаос или блокировать маршруты экстренной помощи в качестве акта терроризма.

Заключение

Современный мир стремительно движется к интеграции умных устройств в повседневную жизнь, что делает проблему безопасности таких устройств одной из ключевых в сфере кибербезопасности. В данной статье были рассмотрены основные угрозы, связанные с уязвимостью IoVT-устройств, а также методы противодействия им. Выявленные уязвимости и методы атак – от базовых (использование стандартных паролей и эксплуатация известных уязвимостей) до сложных (атаки на системы машинного обучения) – подтверждают необходимость комплексного подхода к обеспечению безопасности.

Основные угрозы IoVT демонстрируют, насколько важен вопрос защиты этих устройств. Их массовое распространение, особенно в чувствительных областях (медицина, промышленность, умный дом), превращает каждую уязвимость в потенциальную точку для масштабных кибератак. В условиях растущего числа подключенных устройств и усложняющихся атак особенно важно стремиться к созданию замкнутых защищенных сред и внедрению передовых методов гарантированной аутентификации и защиты, которые будут способствовать устойчивому развитию технологий Интернета вещей.

Список используемых источников:

1. Internet of Things Statistics [Электронный ресурс] // Demand Sage. – URL: https://www.demandsage.com/internet-of-things-statistics/ (дата обращения: 18.05.2025).
2. IoT Security Risks, Stats, and Trends to Know in 2025 [Электронный ресурс] // JumpCloud. – URL: https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025 (дата обращения: 18.05.2025).
3. Обзоры технологий [Электронный ресурс] // CTA. – URL: https://www.cta.ru/articles/cta/obzory/tekhnologii/124338/ (дата обращения: 18.05.2025).
4. Архитектура IIoT: уровни и инструменты [Электронный ресурс] // Big Data School. – URL: https://bigdataschool.ru/blog/iiot-architecture-levels-and-tools.html (дата обращения: 18.05.2025).
5. Новости кибербезопасности [Электронный ресурс] // NAG. – URL: https://nag.ru/news/35312 (дата обращения: 18.05.2025).

6. Cameras, Video Analytics & Legislation: Top Video Privacy Trends 2022 [Электронный ресурс] // Pimloc. – URL: https://www.pimloc.com/blog-1/cameras-video-analytics-legislation-top-video-privacy-trends-2022 (дата обращения: 18.05.2025).

7. A Worrying Watch: Over 43% of Security Camera Owners Worried About Being Hacked [Электронный ресурс] // Faction Networks. – URL: https://www.factionnetworks.com/security-and-privacy-news/cameras/a-worrying-watch-over-43-of-security-cameras-owners-worried-about-being-hacked/ (дата обращения: 18.05.2025).

8. DDoS в 2024: Годовой отчет [Электронный ресурс] // StormWall. – URL: https://stormwall.pro/resources/blog/ddos-2024-godovoj-otchet (дата обращения: 18.05.2025).

9. Botnet Attacks [Электронный ресурс] // Kaspersky. – URL: https://www.kaspersky.ru/resource-center/threats/botnet-attacks (дата обращения: 18.05.2025).

10. Ботнеты и их влияние на кибербезопасность [Электронный ресурс] // DDoS-Guard. – URL: https://ddos-guard.ru/blog/botnet (дата обращения: 18.05.2025).

11. IoT-ботнеты: угрозы и защита [Электронный ресурс] // Botfaqtor. – URL: https://botfaqtor.ru/blog/iot-botnets/ (дата обращения: 18.05.2025).

12. DDoS-атаки: механизмы и противодействие [Электронный ресурс] // DDoS-Guard. – URL: https://ddos-guard.ru/blog/ddos-ataka (дата обращения: 18.05.2025).

13. Mantis Botnet: анализ угрозы [Электронный ресурс] // Cloudflare. – URL: https://blog.cloudflare.com/ru-ru/mantis-botnet/ (дата обращения: 18.05.2025).

14. 86,000 IoT Devices Compromised in Eleven11 Botnet [Электронный ресурс] // Cybersecurity Dive. – URL: https://www.cybersecuritydive.com/news/86000-iot-compromised-eleven11-botnet/741507/ (дата обращения: 18.05.2025).

15. CVE-2024-7029 [Электронный ресурс] // NIST NVD. – URL: https://nvd.nist.gov/vuln/detail/cve-2024-7029 (дата обращения: 18.05.2025).

16. ICS Advisory (ICSA-24-214-07) [Электронный ресурс] // CISA. – URL: https://www.cisa.gov/news-events/ics-advisories/icsa-24-214-07 (дата обращения: 18.05.2025).

17. IoT Security Challenges and Solutions [Электронный ресурс] // PMC (PubMed Central). – URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7506579/ (дата обращения: 18.05.2025).

18. CVE-2017-7925 [Электронный ресурс] // NIST NVD. – URL: https://nvd.nist.gov/vuln/detail/CVE-2017-7925 (дата обращения: 18.05.2025).

19. ICS Advisory (ICSA-17-124-02) [Электронный ресурс] // CISA. – URL: https://www.cisa.gov/news-events/ics-advisories/icsa-17-124-02 (дата обращения: 18.05.2025).

20. CVE-2017-7921 Exploit [Электронный ресурс] // GitHub. – URL: https://github.com/K3ysTr0K3R/CVE-2017-7921-EXPLOIT (дата обращения: 18.05.2025).

21. Hikvision Camera Vulnerability Discussion [Электронный ресурс] // GitHub (Nuclei Templates). – URL: https://github.com/projectdiscovery/nuclei-templates/issues/5639 (дата обращения: 18.05.2025).

22. Hikvision Camera Vulnerability Analysis [Электронный ресурс] // Antiy. – URL: https://www.antiy.cn/research/notice&report/research_report/20170717.html (дата обращения: 18.05.2025).

23. Vulnerability in Hikvision Cameras [Электронный ресурс] // Infosecurity Magazine. – URL: https://www.infosecurity-magazine.com/news/vulnerability-hikvision-cameras/ (дата обращения: 18.05.2025).

24. Privilege Escalation Vulnerability Notice [Электронный ресурс] // Hikvision. – URL: https://www.hikvision.com/us-en/support/document-center/special-notices/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/ (дата обращения: 18.05.2025).

25. Hikvision IP Camera Vulnerability (ID 100897) [Электронный ресурс] // VulDB. – URL: https://vuldb.com/?id.100897 (дата обращения: 18.05.2025).

26. Understanding the Mirai Botnet [Электронный ресурс] // USENIX. – URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis (дата обращения: 18.05.2025).

27. BYOD and Wireless IP Cameras Vulnerable to Hijacking [Электронный ресурс] // Network World. – URL: https://www.networkworld.com/article/672026/byod-widely-used-wireless-ip-cameras-open-to-hijacking-over-the-internet-researchers-say.html (дата обращения: 18.05.2025).

28. IoT Security Research [Электронный ресурс] // NSF PAR. – URL: https://par.nsf.gov/biblio/10488183 (дата обращения: 18.05.2025).

29. The Batch: AI & Cybersecurity [Электронный ресурс] // DeepLearning.AI. – URL: https://www.deeplearning.ai/the-batch/ (дата обращения: 18.05.2025).

30. IoT Security Challenges and Solutions [Электронный ресурс] // PMC (PubMed Central). – URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7506579/#sec4-sensors-20-04806 (дата обращения: 18.05.2025).