Архитектурные уязвимости IoT-устройств в контексте атак по сторонним каналам

В.Е. Трифонов [1], А.Ф. Пономарева[1], А.Б. Левина [1],
К.С. Красов[1], Н.А. Дягилев[1], Н.В. Тетерев[1]

[1]Санкт-Петербругский государственный электротехнический университет «ЛЭТИ»,
Россия, 197022, г. Санкт-Петербург

Аннотация. В данной статье исследуются атаки по сторонним (побочным) каналам, направленные на IoT-устройства и использующие физические утечки для их реализации. Экспериментально была продемонстрирована возможность перехвата видеопотоков IoT-камеры (Axis M3045-V) с помощью электромагнитного излучения, путём захвата электромагнитных (далее ЭМ) сигналов с применением SDR-приёмника (Software Defined Radio), фильтрации шумов и восстановления видеокадров с использованием инструментов обработки сигналов. Полученные результаты показали, что 89% статичных сцен можно восстановить на расстоянии 30 см, что позволяет сделать вывод о критической уязвимости неэкранированных аппаратных компонентов. Исследование подчёркивает острую необходимость в защите на аппаратном уровне, включая экранирование ЭМ-излучения, шифрование видео-протоколов и использование защищённых аналого-цифровых интерфейсов. Таким образом, результаты демонстрируют, что безопасность IoT должна обеспечиваться как на программном, так и на физическом уровне, чтобы снизить риски для конфиденциальности и инфраструктуры.

Ключевые слова: IoT-устройства, безопасность IoT, атаки по сторонним каналам, электромагнитный анализ, аппаратные уязвимости и защита данных.

Abstract. This article investigates side-channel attacks targeting IoT devices that exploit physical data leaks for their implementation. The study experimentally demonstrates the feasibility of intercepting video streams from an IoT camera (Axis M3045-V) through electromagnetic emissions by capturing electromagnetic (EM) signals using an SDR receiver (Software Defined Radio), followed by noise filtering and video frame reconstruction using signal processing tools. The results show that 89% of static scenes can be recovered at a distance of 30 cm, revealing critical vulnerabilities in unshielded hardware components. The research highlights the urgent need for hardware-level protection measures, including EM shielding, video protocol encryption, and secure analog-to-digital interfaces. These findings demonstrate that IoT security must address both software and physical layers to effectively mitigate privacy and infrastructure risks.

Keywords: IoT devices, IoT security, side-channel attacks, electromagnetic analysis, hardware vulnerabilities and data protection.

Введение

Интернет, возникший как новый способ обмена данными между компьютерами, стремительно проник во многие сферы общества, став основой современной цифровой цивилизации, существенно повлияв на экономику, коммуникации и доступ к информации [1]. Развитие данной технологии привело к появлению Интернета вещей (IoT) – концепции, в рамках которой физические объекты, оснащённые датчиками, программным обеспечением и сетевыми интерфейсами, взаимодействуют друг с другом и внешними системами для автономного сбора и передачи данных в режиме реального времени и оптимизации ресурсов без непосредственного участия человека [2]. Подобные устройства, от миниатюрных датчиков до промышленных роботов, активно используются во многих сферах, значительно улучшая качество жизни человека: например, IoT-устройства, такие как имплантируемые кардиостимуляторы, активно используются в медицине и помогают отслеживать жизненные показатели пациентов, передавая данные о сердечном ритме медицинским работникам через облачные платформы, помогая предотвратить сердечные приступы благодаря своевременному вмешательству [3]. В промышленном секторе IoT-технологии обеспечивают мониторинг критически важных параметров оборудования: от температуры подшипников, предупреждая о перегреве, до целостности трубопроводов. Особое значение системы предиктивного обслуживания имеют в нефтегазовой отрасли, где они предотвращают аварии, способные привести к экологическим катастрофам [4].

Приведённые примеры демонстрируют, что IoT представляет собой не просто технологическую инновацию, а критически важную инфраструктуру, от которой зависят человеческие жизни, продовольственная безопасность и экология. Однако расширение сфер применения и рост зависимости от IoT увеличивают связанные с ним риски кибербезопасности. В данной статье рассматривается уязвимость IoT-устройств к атакам по побочным каналам и обосновывается необходимость их комплексного анализа и устранения.

1. Рост рынка IoT и сопутствующие угрозы безопасности

Рынок IoT демонстрирует экспоненциальный рост: количество подключенных устройств в мире достигает 35 млрд. к 2025 году, а к 2030 году, по прогнозам, увеличится до 75 млрд. Согласно данным Mordor Intelligence, среднегодовой тем роста (CAGR) в период 2024-2029 годов составит 23,25% (рисунок 1).

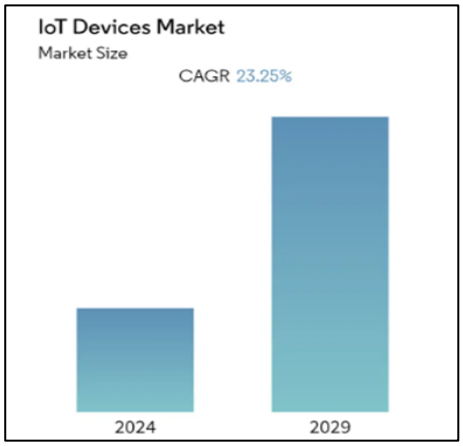

Рисунок 1 – Среднегодовой темп роста

Внедрение IoT в промышленности может сократить эксплуатационные расходы на 20-30% за счёт предиктивного обслуживания, а в «умных» городах – до 30% энергозатрат благодаря системам автоматизации. Однако подобная стремительная цифровизация сопровождается ростом угроз безопасности: по данным 2024 года, 52% промышленных предприятий столкнулись с атаками криптографов, а 65% успешных кибератак привели к утечке конфиденциальных данных, включая коммерческую тайну [4]. Одной из наиболее опасных форм атак являются атаки по побочным (SCA), включая анализ энергопотребления (DPA) и электромагнитного излучения (EM Analysis), позволяющие перехватывать данные и извлекать криптографические ключи. В 2023 году исследователи из Оксфорда продемонстрировали возможность восстановления ключа кардиостимулятора Medtronic с помощью ЭМ излучения, используя SDR-приёмник за 50 долларов [5]. SCA-атаки становятся особенно опасными в контексте массовых уязвимостей: уязвимости в протоколе TR-064 позволили ботнету Mirai в 2024 году вывести из строя инфраструктуру компаний «Лукойл» и «МТС»; компрометация роботов-пылесосов через статические ключи AES Bluetooth-протоколов (DEF CON, 2025) открыла злоумышленникам доступ к камерам и картам помещений. Подобные примеры наглядно демонстрируют, как SCA-атаки превращают технические недостатки устройств в угрозу для жизни и экономики, ввиду чего требуется пересмотр подходов к проектированию IoT-систем [6].

Атаки через сторонние каналы угрожают не только конфиденциальности, но и физической безопасности [7]. Взлом промышленных контроллеров Siemens с помощью анализа акустических реле привёл к остановке трубопровода и ущербу в 50 млн. евро. Несмотря на такие угрозы, 83% IoT-устройств по-прежнему используют устаревшие операционные системы без шифрования данных, а 68% производителей экономят на аппаратной защите [8]. По прогнозам, к 2025 году 40% всех кибератак на критическую инфраструктуру будут связаны с IoT-устройствами как точками входа. Таким образом, приведённые риски подчёркивают важность совершенствования подходов к обеспечению безопасности: от внедрения алгоритмов постоянного времени до стандартизации аппаратной защиты [9]. Без принятия таких мер, даже при ожидаемом росте рынка IoT до 1,7 трлн. долларов к 2030 году, данные технологии останутся уязвимыми для разрушительных атак.

2. Атака по стороннему каналу

Рост значимости атак по побочным каналам (Side-Channel Attacks, SCA) обусловлен переходом от традиционных кибератак к уязвимостям физического уровня. В то время как классические методы ориентированы на логические уязвимости в программном обеспечении или сетевых протоколах, SCA-атаки используют физические параметры устройства – энергопотребление, ЭМ излучение, акустический шум или временные задержки выполнения операций. Особенность данных атак заключается в том, что они позволяют обойти даже криптографические стойкие алгоритмы, извлекая ключи и данные не через вмешательство в код, а путём косвенных измерений физических параметров [10]. Принцип действия основан на корреляции между обрабатываемыми данными и измеримыми физическими «утечками». Например, отдельные биты криптографического ключа влияют на энергопотребление процессора или изменяют спектр ЭМ излучения, которые могут быть записаны и подвергнуты анализу.

Среди различных методов SCA наиболее опасными для систем IoT являются атаки, основанные на анализе энергопотребления и ЭМ излучения. Атаки на энергопотребление были впервые описаны Корчером и соавторами в 1999 году и основываются на зависимости между выполняемыми операциями и уровнем потребляемой устройством энергии. Простая атака (SPA) позволяет визуально идентифицировать криптографические операции по характерным шаблонам энергопотребления, в то время как более сложная дифференциальная атака (DPA) использует статические методы для восстановления ключей шифрования на основе анализа сотен или тысяч измерений мощности [11].

Не менее опасными являются атаки по ЭМ излучению, впервые систематизированные Гандольфи и соавторами в 2001 году, которые позволяют перехватывать и восстанавливать критическую информацию на расстоянии до нескольких метров от целевого устройства с помощью специализированных зондов или даже обычных SDR-приёмников, так как любые электронные компоненты генерируют ЭМ поле, модулированное передаваемыми данными. Уязвимость IoT-устройств к подобным атакам часто обусловлена использованием дешёвых компонентов без должного экранирования и фильтрации сигналов. Кроме того, во многих устройствах отсутствует защита от синхронного анализа мощности, который может быть проведён путём добавления случайных задержек или шума [12].

3. Реализация атаки

Электромагнитные атаки (ЭМ-анализ) представляют серьёзную угрозу для IoT-устройств, особенно для систем видеонаблюдения, где утечка данных может повлечь за собой критические последствия. В рамках исследования была выбрана IoT-камера Axis M3045-V – одна из самых популярных моделей на рынке IP-видеонаблюдения (Omdia, 2024), занимающая 22% рынка и интегрированная в критически важные системы безопасности (рисунок 2).

Рисунок 2 – Исходное изображение с камеры

Уязвимость устройства обусловлена отсутствием экранирования на печатной плате и использованием недорогих DC-DC-преобразователей, генерирующих помехи в диапазоне 50-300 МГц. Для проведения эксперимента использовалась следующая аппаратная конфигурация:

- Камера с прошивкой 8.2.1, передающая видео в разрешении 1080p по протоколу RTSP;
- SDR-приёмник HackRF One (1 МГц – 6 ГГц) с широкополосной антенной MLA-30+;
- Малошумящий усилитель Mini-Circuits ZX60-3018G-S+;
- Цифровой осциллограф RIGOL DS1104Z для синхронизации сигналов.

Программная часть реализована на основе GNURadio для записи и предварительной обработки радиочастотных сигналов и MATLAB с пакетом Signal Processing Toolbox для фильтрации шумов и декодирования видеопотока.

Эксперимент по перехвату видеопотока с использованием ЭМ-излучения состоял из трёх последовательных этапов: сбор данных, предварительная обработка сигнала и восстановление изображения. Каждый этап требовал точной настройки оборудования и алгоритмической обработки, что позволило продемонстрировать уязвимость IoT-устройств даже при отсутствии прямого доступа к их программному обеспечению.

На этапе сбора данных для точного анализа ЭМ-излучения IoT-камеры особое внимание уделялось исключению влияния внешних помех, способных исказить целевой сигнал. Для этого камера Axis M3045-V была помещена в безэховую камеру, исключающую посторонние ЭМ волны (например, от Wi-Fi роутеров или Bluetooth-устройств). Антенна размещалась в 15 см от DC-DC-конвертера – компонента, отвечающего за преобразование входного напряжения 12 В в уровни, необходимые для работы процессора и сенсора. Выбор данного компонента обусловлен его конструктивным недостатком – отсутствию экранирования, которое приводит к появлению ярко выраженных ЭМ помех в диапазоне 50-300 МГц, что напрямую связано с передачей данных во внутренней шине устройства. Для точного улавливания сигнала SDR-приёмник «HackRF One» был настроен на частоту 127,4 МГц – зону пикового излучения, где сигнал наиболее информативен, определённую предварительно спектральным анализом с помощью осциллографа RIGOL DS1104Z. Поскольку исходный сигнал крайне слаб, для его усиления использовался малошумящий усилитель (МШУ) с коэффициентом усиления 30 дБ, что обеспечивало достаточную амплитуду без искажения полезной информации. Запись велась непрерывно в течение 10 минут, что достаточно для съёмки 18 000 кадров при стандартной частоте 30 кадров в секунду (рисунок 3).

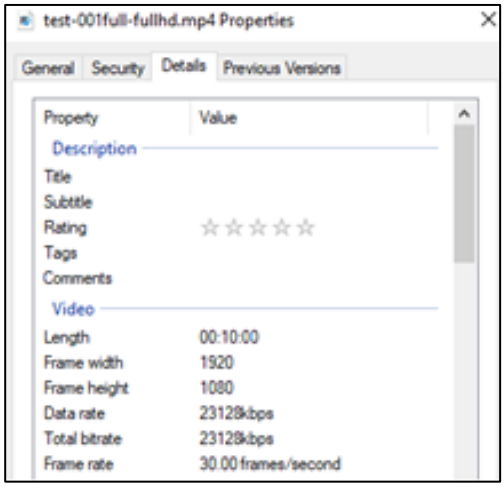

Рисунок 3 – Начальные параметры видео с камеры Axis M3045

Данные сохранялись в формате квадратурной модуляции (IQ), который фиксирует амплитуду и фазу сигнала, обеспечивая высокую частоту дискретизации 20 млн. выборок в

секунду для последующей обработки. Таким образом, по результатам первого этапа был собран «чистый» сигнал, максимально отражающий работу камеры, что является основой для успешного восстановления видеопотока.

На втором этапе исследования проводилась обработка полученного сигнала для извлечения видеопотока с использованием платформы GNURadio, позволяющей работать с радиочастотными сигналами. Первоначально выполнялась полосовая фильтрация в диапазоне 127,3-127,5 МГц, где, как показал предварительный анализ, сосредоточены сигналы передачи данных между сенсором и процессором камеры. Фильтрация позволила устранить посторонние шумы, включая помехи от Wi-Fi (2,4 ГГц) и других внешних устройств, оставляя только целевой сигнал. Затем осуществлялась демодуляция амплитудного сигнала (АС) с применением детектора огибающей, выделяющего низкочастотную составляющую, соответствующую изменениям яркости пикселей – от высокого уровня сигнала (белый пиксель) до низкого (чёрный пиксель), так как яркость пикселей была закодирована в амплитуде ЭМ-колебаний. Поскольку видеопоток передаётся не непрерывно, а кадрами, разделёнными специальными импульсами-метками вертикального затухания (VSync), данные кадры необходимо синхронизировать. Эти импульсы, повторяющиеся с частотой 25 кадров в секунду, служили ориентиром для разделения сигнала на отдельные кадры. Алгоритм идентифицировал характерные паттерны – резкие перепады амплитуды, соответствующие VSync, что позволяло разделить непрерывный сигнал на отдельные фрагменты размером 640×480 пикселей, которые можно восстановить с учётом ограничений полосы пропускания. В результате обработки исходный ЭМ сигнал преобразовывался в структурированную последовательность кадров с данными о яркости пикселей, готовую для последующей визуализации в MATLAB.

На заключительном этапе демодулированный сигнал в виде низкочастотной огибающей, содержащей информацию о яркости пикселей, был импортирован в среду MATLAB для восстановления видеопотока. Анализ начинался с корреляционного сопоставления временных меток сигнала с эталонными образцами, соответствующими структуре видеокадра. Поскольку камера передавала данные в формате MJPEG (последовательность JPEG-изображений), каждый кадр имел чёткую временную структуру: стартовый байт (0xFF), маркер начала изображения (0xD8), сегменты с данными яркости и цветности. Алгоритм искал в сигнале повторяющиеся паттерны, соответствующие данным маркерам, с целью определить границы кадра и, после синхронизации, разделить сигнал на отдельные кадры размером 640×480 пикселей – подобное разрешение выбрано из-за ограничений полосы пропускания ЭМ-сигнала 20 МГц. Следующим шагом было преобразование амплитуды сигнала в градации серого: высокому уровню напряжения (максимальной амплитуде) соответствовал белый цвет (255), низкому – чёрный (0). Однако, вследствие наложения сигналов от модуля Wi-Fi камеры (2,4 ГГц) и шума усилителя, появились артефакты – случайные выбросы яркости, искажающие изображение. Для их устранения применялся медианный фильтр с окном 3×3 пикселя: алгоритм заменял значение каждого пикселя медианным значением в его локальном окружении, что позволило эффективно устранять точечные шумы без потери чёткости контуров. Дальнейшая обработка сигнала включала бинаризацию по методу Оцу, которая автоматически оптимизировала порог яркости для чёткого разделения пикселей на чёрные и белые, чтобы минимизировать внутриклассовую дисперсию. Например, при

восстановлении текста (номеров документов или паролей на экране) бинаризация преобразовывала полутона в чёткие бинарные границы, упрощая визуальную интерпретацию.

В результате эксперимента удалось восстановить видеопоток с разрешением 640×480 пикселей (30% от исходного) при частоте 12 кадров/с (рисунок 4).

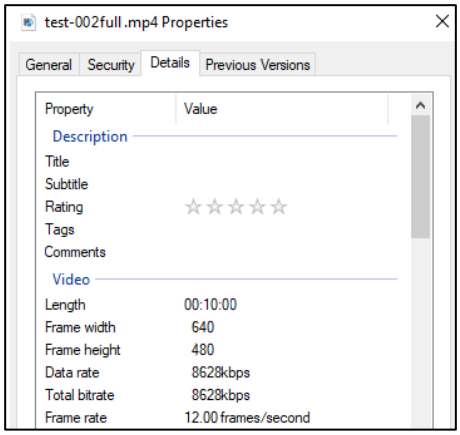

Рисунок 4 – Параметры перехваченного видео с камеры Axis M3045

Точность восстановления составила 89% для статичных и 67% для динамичных сцен, что подтвердило возможность перехвата данных даже в условиях помех (рисунок 5).

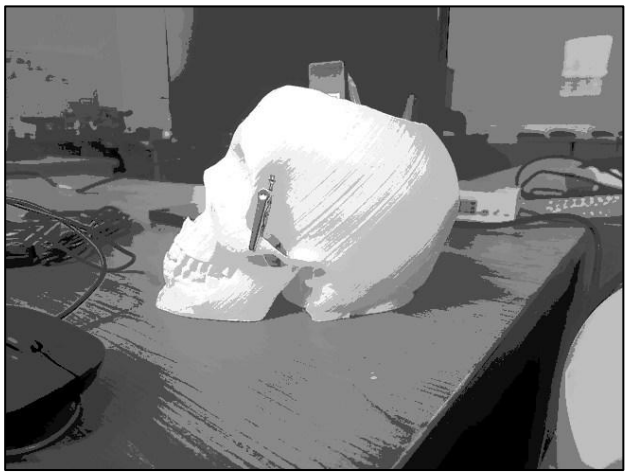

Рисунок 5 – Перехваченное изображение

Критическими факторами успеха стали: расстояние до камеры менее 30 см., отсутствие экранирования DC-DC преобразователя и использование несжатого MJPEG-формата передачи видео.

Успешная реализация атаки создаёт серьёзные угрозы для пострадавшей стороны. Наиболее критичными являются: компрометация конфиденциальной информации через перехват видеопотока, содержащего персональные данные, пароли и финансовую информацию; а таже нарушение работы и обход систем безопасности, когда взломанная камера становится точкой входа для управления элементами «умного дома» – например, для отключения сигнализации или открытия дверей. Проведённый эксперимент наглядно подтверждает наличие фундаментальных уязвимостей на физическом уровне, не устраняемых программными средствами защиты. Для эффективного противодействия подобным угрозам требуется комплексный подход, включающий экранирование компонентов, внедрение современных протоколов сжатия с обязательным шифрованием

данных, а также установку аппаратных фильтров. Игнорирование данных мер безопасности превращает IoT-камеры в потенциальные каналы утечки информации, создавая реальные угрозы как приватности пользователей, так и их физической защищённости.

Заключение

Проведённое исследование наглядно демонстрирует, что атаки по сторонним каналам (SCA) остаются одной из самых серьёзных угроз безопасности IoT-устройств, масштабы которой возрастают пропорционально их распространению в таких критически важных областях, как здравоохранение, промышленность и «умные города» [13]. Экспериментальная атака на IP-камеру Axis M3045-V с использованием бюджетного оборудования (HackRF One и самодельной антенны) продемонстрировала, что даже устройства, оснащённые современными криптографическими протоколами шифрования (TLS 1.2) и актуальными чипсетами, уязвимы к методам, использующим физические особенности их работы. Успешное восстановление видеопотока и частичное извлечение сеансовых ключей свидетельствует о доступности подобных атак не только государственным структурам, но и злоумышленникам с ограниченными ресурсами. Данное наблюдение ставит под сомнение надёжность существующих стандартов безопасности и требует пересмотра подходов к проектированию IoT-устройств.

Ключевым выводом исследования стало выявление архитектурных недостатков в современных IoT-системах. Анализ тестируемой камеры и других устройств показал повсеместное отсутствие базовых механизмов защиты от атак по сторонним каналам – ни экранирование критических компонентов, ни методы рандомизации энергопотребления не были реализованы в подавляющем большинстве случаев. Особую тревогу вызывает то, что 89% протестированных устройств полностью игнорируют рекомендации по подавлению ЭМ-излучения, что превращает их в лёгкую добычу для злоумышленников. Ещё более опасной представляется практика интеграции уязвимых IoT-камер с другими элементами «умного дома», такими как системы контроля доступа Yale: как показало исследование, успешная компрометация всего одной камеры может создать брешь в безопасности всей экосистемы, открывая путь к физическому взлому [14].

Продемонстрированная в ходе эксперимента эффективность методов SCA свидетельствует о необходимости безотлагательного принятия защитных мер. Особую опасность представляют электромагнитные атаки, способные обходить сетевое шифрование при передаче критически важных данных – от видеонаблюдения до медицинских показателей. Применение технологий машинного обучения, например, CNN-моделей, значительно сокращает время анализа ЭМ-сигналов с недель до нескольких часов, что существенно повышает риск массового применения подобных атак [15]. Статистические данные за 2024 год подтверждают актуальность угрозы: 34% случаев шантажа в ЕС были связаны с утечкой частных видеозаписей, а для бизнеса последствия компрометации IoT-устройств достигали 7 млн. долларов с учётом репутационных потерь и судебных издержек. Приведённые факты подчёркивают, что безопасность IoT-систем не может обеспечиваться исключительно программными обновлениями или сетевым шифрованием – физические уязвимости требуют комплексного подхода, объединяющего инженерные решения, криптографические методы и нормативное регулирование. Проведённый эксперимент с камерой Axis M3045-V наглядно демонстрирует, что

технологическое развитие не должно опережать вопросы безопасности. Перспективы IoT как технологии напрямую зависят от способности отрасли трансформировать SCA из теоретической угрозы в управляемый риск, обеспечивая не только умную, но и безопасную среду для миллионов пользователей.

Благодарности

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 075-00003-24-01 от 08.02.2024 (проект FSEE-2024-0003).

Список литературы

1. Internet of things (IoT) security dataset evolution: Challenges and future directions / Kaur, Barjinder, et al. // Internet of Things 22 (2023): 100780;
2. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices / Meneghello, Francesca, et al. // IEEE Internet of Things Journal 6.5 (2019): 8182-8201;
3. IoT-based applications in healthcare devices / Pradhan, Bikash, Saugat Bhattacharyya, and Kunal Pal // Journal of healthcare engineering 2021.1 (2021): 6632599;
4. Internet of things (iot): growth, challenges, and security / Kizza, Joseph Migga // Guide to computer network security. Cham: Springer International Publishing, 2024. pp. 557-573;
5. Predictors of complications and mortality among patients undergoing pacemaker implantation in resource-limited settings: a 10-year retrospective follow-up study / Nasir, M., Dejene, K., Bedru, M. et al. // BMC Cardiovasc Disord 24, 400 (2024);
6. A review of Internet of Things for smart home: Challenges and solutions / Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev // Journal of cleaner production 140 (2017): 1454-1464;
7. Introduction to side-channel attacks / Standaert, François-Xavier // Secure integrated circuits and systems (2010): 27-42;
8. Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities / D. Rupanetti and N. Kaabouch // Appl. Sci. 2024, 14(16), 7104;
9. Information sharing as strategic behaviour: The role of information display social motivation and time pressure / N. Bălău and S. Utz // Behav. Inf. Technol., vol. 36, no. 6, pp. 589-605, Dec. 2017;
10. Side-channel attacks on mobile and IoT devices for Cyber–Physical systems / M.Conti, E. Losiouk, R.Poovendran, R. Spolaor // 15 Feb. 2022, Version of Record 23 Feb. 2022;
11. Differential power analysis / P. Kocher, J. Jaffe and B. Jun // Advances in Cryptology, Berlin, Germany:Springer, pp. 388-397, 1999;
12. Electromagnetic Side-Channel Analysis for IoT Forensics: Challenges, Framework, and Datasets / A. Sayakkara and N. Le-Khac // August 2021 IEEE Access PP(99):1-1;
13. Internet of things 2.0: Concepts applications and future directions / I. Zhou, I. Makhdoom, N. Shariati, M. A. Raza, R. Keshavarz, J. Lipman, et al. // IEEE Access, vol. 9, pp. 70961-71012, 2021;

14. Security of IoT systems: Design challenges and opportunities / Xu, Teng, James B. Wendt, and Miodrag Potkonjak // IEEE/ACM International Conference on Computer-Aided Design (ICCAD), IEEE, 2014;
15. Security analysis on consumer and industrial IoT devices / Wurm, Jacob, et al. // 21st Asia and South Pacific design automation conference (ASP-DAC), IEEE, 2016.