УДК 004.056.5

Д. Э. Ляхов, А. А. Стрелкина,
Д. Д. Узун

# Анализ методов и средств оценивания и обеспечения кибербезопасности IoT системы

*Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт»*

Исследована кибербезопасность Internet of Things системы (Интернет вещей, IoT). Проведён анализ основных атак на IoT систему с помощью метода IMECA (Intrusion Modes and Effects Criticality Analysis - анализ видов, последствий и критичности вторжений) и на его основе построено дерево ATA (Attack Tree Analysis – анализ атак в виде дерева). Результатом данной работы является анализ основных атак с помощью метода IMECA для отдельно взятых компонентов системы и системы в целом.
***Ключевые слова:*** IoT, безопасность, конфиденциальность, IMECA, ATA.

IoT (Internet of Things) системы в здравоохранении начали привлекать большое внимание к себе в последнее время, поскольку данные предоставляют множество полезных функций, которые облегчают дистанционный мониторинг пациентов. Переносимое медицинское устройство становится неотъемлемой частью системы удаленного мониторинга в системах, основанных на базе IoT. Появление парадигмы IoT является одним из самых впечатляющих явлений последнего десятилетия [1].

Разработка различных протоколов связи наряду с уменьшением приемопередатчиков дает возможность использовать устройства не только для сбора данных, но и в качестве коммуникационного узла. Кроме того, вычислительная мощность, энергоемкость и возможности хранения небольших вычислительных или чувствительных устройств значительно улучшились, а их размеры резко снизились.

В качестве побочного эффекта число потенциальных угроз и возможных атак на безопасность или конфиденциальность устройства или целых систем резко возросло. К сожалению, в области безопасности IoT еще не уделяется достаточно большого внимания [2]. Следовательно, необходимо тщательно изучить и устранить угрозы безопасности и общие проблемы конфиденциальности [2]. Это значительно упростило бы разработку безопасных интеллектуальных устройств, которые можно было бы использовать людьми, особенно в области здравоохранения.

IoT предоставляет широкий спектр интеллектуальных приложений и услуг для решения проблем, с которыми сталкиваются отдельные лица или сектор здравоохранения. Например, IoT имеет динамические возможности для подключения D2M (Device-to-Machine), O2O (Object-to-Object), P2D (Patient-to-Doctor), P2M (Patient-to-Machine), D2M (Doctor-to-Machine), S2M (Sensor-to-Mobile), M2H Mobile-to-Human), T2R (Tag-to-Reader) [3]. Эти технологии обеспечивают взаимодействие между людьми и интеллектуальными устройствами позволяющих наладить эффективную работу системы здравоохранения.

Ключевое отличие безопасности IoT систем — это видимость. Устройства IoT являются узкоспециализированными, нестандартизованными и управляют широким спектром программного обеспечения, что делает их намного сложнее, чем системы, которые управляются централизованно.

Кроме того, можно отметить, что устройства для проведения обследования пациентов (например, кардиологии и радиологии) обладают многочисленными уязвимостями. Это связано с тем, что отсутствуют базовые практики по обеспечению безопасности в области медицинского IoT, а также единый стандарт для обмена данными между устройствами. Например, создатели медицинских устройств IoT просто не уделяют большого внимания данной проблеме, несмотря на очевидные недостатки, имеющиеся во многих своих продуктах [4].

Целью данной статьи является анализ основных атак на IoT систему на примере системы мониторинга здоровья пациентов с помощью метода IMECA (Intrusion Modes and Effects Criticality Analysis) и на его основе построение дерева ATA (Attack Tree Analysis). Такой анализ будет основой для анализа оценивания ресурсов, которые необходимы для того, чтобы провести представленные в статье атаки и/или организовать контрмеры, направленные против них.

Структура статьи такая: в разделе 1 описана обобщённая архитектура системы. В разделе 2 содержится анализ различных видов атак, которым подвержена IoT система. Затем, в разделе 3 описаны возможные меры противодействия представленным атакам. В заключение приведены выводы и дальнейшие направления для будущих исследований.

## 1. Анализ атак на уязвимости

Системы на основе IoT могут управлять огромным объёмом информации и использоваться для обслуживания, в том числе и для мониторинга состояния здоровья пациентов. Это сделало парадигму IoT интересной мишенью для множества социальных групп, таких, как хакеры, киберпреступники, правительство и т. д.

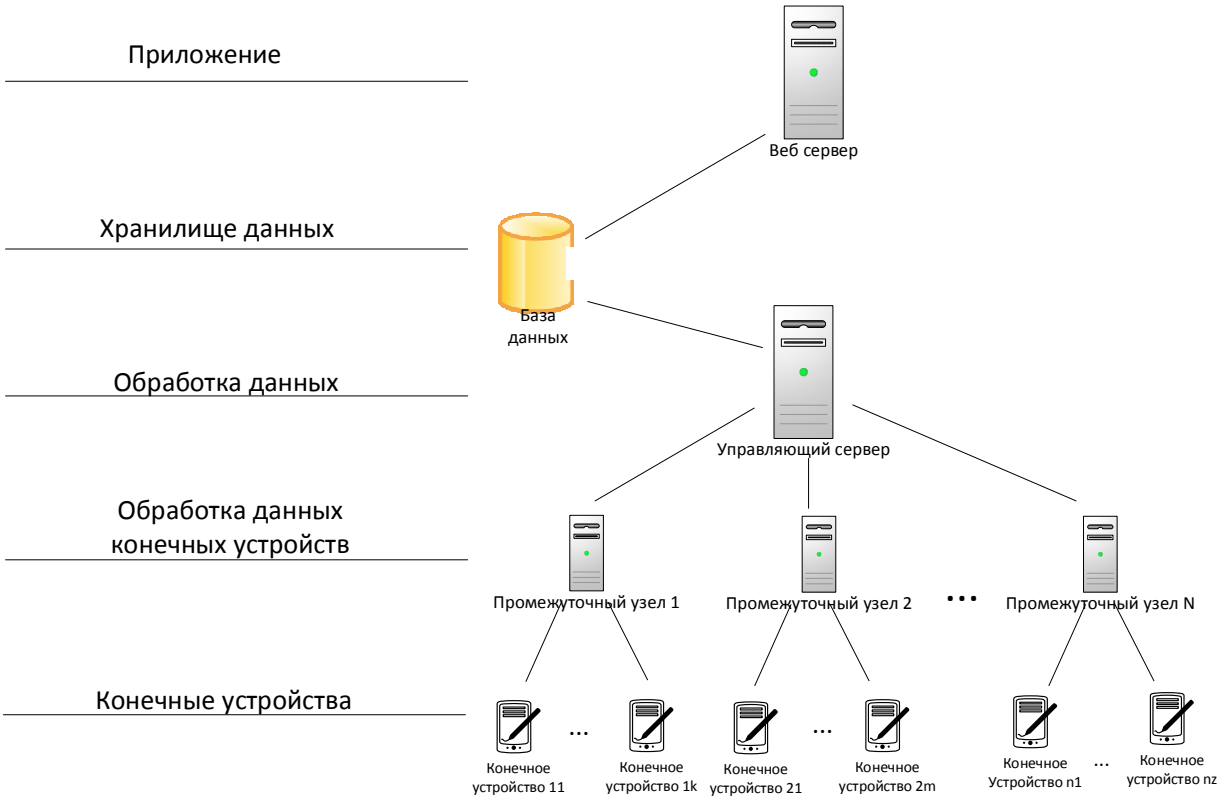


Рисунок 1 - Обобщённая структура IoT системы

Потенциальные злоумышленники могут быть заинтересованы в краже конфиденциальной информации, например, текущее состояние пациента, история здоровья, номера кредитных карт, данных о местоположении, паролей финансовых учётных записей и информации, связанной со здоровьем. Более того, они могут попытаться подменить компоненты IoT, например, конечные узлы, для запуска атак.

Особенностью IoT системы для системы мониторинга состояния здоровья пациентов является то, что эта система генерирует очень большое количество информации и является более критически важной по сравнению с другими IoT системами [3].

На рис. 2 была показана классификация атак на IoT систему.

*Физические атаки*. Атаки данного вида наносят вред аппаратным компонентам, и такие атаки относительно сложнее выполнить, поскольку для этого требуется достаточно дорогие ресурсы.

*Атаки по сторонним каналам*. Эти атаки основаны на «информации о сторонних каналах», которую можно извлечь из устройства шифрования, не являющегося криптозащищённым. Устройства шифрования выдают информацию о времени, которая легко поддаётся измерению, о различных видах излучения, статистику потребления энергии и многое другое, и таким образом уязвимы для так называемых тайминг атак [4].

*Атаки криптоанализом*. Эти атаки сосредоточены на зашифрованном тексте, и они пытаются разбить шифрование, т. е. найти ключ шифрования для получения открытого текста. Примеры атак криптоанализа включают в себя атаку на основе шифротекста, атаку подобранного шифротекста, атаку открытого текста, атака-посредник и т. д.

*Атака на ПО* (программное обеспечение). Атаки на ПО являются основным источником уязвимостей безопасности в любой системе. Программные атаки используют уязвимости внедрения в системе через собственный интерфейс передачи данных. Такая атака включает в себя использование переполнения буфера и применение программ, таких, как «троянский конь», «червь», или вирусов для преднамеренного ввода вредоносного кода в систему.

*Сетевые атаки*. Беспроводные системы связи уязвимы для сетевых атак из-за широковещательного характера среды передачи. В основном атаки классифицируются как активные и пассивные. Примеры пассивных атак включают в себя мониторинг и подслушивание, анализ трафика и т. д. Примеры активных атак содержат атаки с отказами в обслуживании, подструктуру узла, сбои, захват, отключение узла, повреждение сообщений, ложный узел, атаки маршрутизации и т. д.

Далее представлено описание атак с более детальным объяснением.


Рисунок 2 – Виды атак на IoT систему

**Троянский конь**. Это вредоносное изменение интегральной схемы, которое позволяет злоумышленнику использовать схему для получения доступа к данным или программному обеспечению, запущенному на устройстве [6, 7].

«Трояны» обычно делятся на две категории, основанные на механизмах их запуска. Существуют «трояны», которые могут быть активированы сигналом антенны или датчика, взаимодействующие с внешним миром [8], и трояны, которые активируются после выполнения определённого условия внутри интегральной схемы, например, «троян», который. просыпается после определённого времени, когда он получает сигнал запуска от схемы обратного отсчёта, добавленной злоумышленником [8].

**Атака по сторонним каналам**. Каждое устройство может получать недостоверную критическую информацию при нормальной работе, даже если не использует беспроводную связь для передачи данных.

В 2007 году декларация документов TEMPEST [9] и недавние публикации некоторых атак на основе/ЭМ (электромагнитных) сигналов начали развивать идею атак по сторонним каналам. Например, в недавней работе исследователи смогли продемонстрировать, как акустические сигналы, просочившиеся из медицинского устройства, могут предоставить ценную информацию о пациенте или устройстве [10–12]. Как упоминалось в работе [13], обнаружение существования сигналов или протоколов может поставить под угрозу безопасность пользователя, например, если у пользователя есть очень дорогое устройство. Более того, такой тип атаки может привести к серьёзной проблеме конфиденциальности в медицинских системах.

**Неполное логирование**: логирование является хорошим подходом для обнаружения вторжения или попытки взлома. Разработчики должны регистрировать события, такие, как успешные/неудачные попытки аутентификации, успешные/неудачные попытки авторизации устройств/приложения. Приведённая в действие система может быть повреждена в результате нелогирования важных событий в системе [14]. Также рекомендуется, чтобы лог-файлы были зашифрованы.

**Физические атаки / фальсификация**: этот тип атаки может быть возможен, когда злоумышленник имеет полный физический доступ к RFID-метке. Во время данной атаки RFID-меткой можно физически манипулировать и можно модифицировать её. Существует несколько известных физических нападений на RFID и среди них — удаление данных, изменения работы схемы и синхронизация часов [15–19]. Эти атаки используются для извлечения информации из RFID-метки для её дальнейшего подделывания.

**DoS-атаки**: целью данной атаки является отправление на устройство большое количество информации, вследствие чего оно не сможет обрабатывать входящий поток данных и перестаёт отвечать на запросы. Например, злоумышленник может отправлять данные на устройство (например, датчик пожарной безопасности) не раз в 100 мс, а 100 раз за 100 мс. Дополнительные уязвимости протоколов проверки подлинности RFID для атаки DoS обсуждались в [20].

**Неавторизованный обмен данными**: каждому конечному устройству необходимо обмениваться данными с другими узлами [14]. Однако каждый узел должен обмениваться данными только с подмножеством узлов, которым нужны его данные. Это является существенным требованием для каждой системы IoT, в частности, состоящей из небезопасных и безопасных узлов [21, 22]. Например, в интеллектуальном домашнем сценарии термостат требует данных датчика дыма, чтобы отключить

**Лишение сна**: лишение сна представляет собой специфический тип DoS-

атаки в том смысле, что жертвой является узел с батарейным питанием с ограниченной энергетической ёмкостью. В этом типе атаки злоумышленник пытается отправить нежелательный набор запросов, которые кажутся системными запросами. Следовательно, обнаружение такого типа атаки намного сложнее, чем простое отключение батареи. Атака может привести к значительному снижению производительности сети. Более того, злоумышленник может легко повредить или неверно передать пакеты при передаче данных [23]. Эта атака, как правило, наносит серьёзный урон системе, позволяя злоумышленнику получить необходимый доступ к извлечению криптографических общих ключей [24].

**Несетевые сторонние атаки**: каждый узел может обнаруживать критическую информацию при нормальной работе, даже если не использует беспроводную связь для передачи данных. Например, электромагнитные волны, вызываемые узлом, могут предоставить ценную информацию о состоянии устройства. В 2007 году декларация документов TEMPEST [9] и публикации некоторых атак на основе ЭМ [23-25] начали развивать идею несетевых побочных угроз. Например, в недавней работе исследователи смогли продемонстрировать, как акустические/ЭМ-сигналы, просочившиеся из медицинского устройства, могут предоставить ценную информацию о пациенте или устройстве [25].

**Атака повторного воспроизведения**: в такой атаке злоумышленник добавляет новое устройство, например, вредоносный датчик, в существующий набор узлов путём тиражирования номера идентификации одного узла. Эта атака может привести к значительному снижению производительности сети. Более того, злоумышленник может легко повредить или неверно передать пакеты, которые поступают в систему [10]. Эта атака обычно наносит серьёзный урон системе, позволяя злоумышленнику получить необходимый доступ к извлечению криптографических общих ключей [26]. Более того, устройства могут игнорировать реальные устройства путём выполнения протоколов отзыва узлов [12, 26].

**Подслушивание**: в этой атаке основной целью атакующего является перехват, чтение и сохранение сообщений для будущего анализа. Перехваченные данные могут использоваться как входная точка для других атак, таких, как клонирование RFID меток. Концепция перехвата атак на RFID не нова и часто упоминается в литературе. В недавних докладах Национального института стандартов и технологий [27] и Департамента внутренней безопасности [28] в дополнение к нескольким опубликованным исследованиям, например, [28-30], упоминаются риски подслушивания в среде RFID. В частности, несколько практических сценариев атаки и их экспериментальные установки обсуждались в [30].

**Атаки маршрутизации**. Атаки, влияющие на маршрутизацию сообщений, называются атаками маршрутизации. Злоумышленник может использовать такие атаки для подмены, перенаправления, неправильного направления или удаления пакетов на уровне сети. Самый простой тип атаки на маршрутизацию — это атака, в ходе которой злоумышленник изменяет информацию маршрутизации, например, путём создания циклических маршрутов или ложных сообщений об ошибках. В дополнение к изменению атак было предложено несколько других серьёзных атак, например «Чёрная дыра» [33, 34], «Серая дыра» [34], «Червь» [35], «Hello Flood» [35, 36].

1. «Чёрная дыра» (Black Hole) — данная атака запускается с использованием вредоносного узла, который привлекает весь трафик в сети, показывая, что у него самый короткий путь к месту назначения в сети. В результате все пакеты отправляются на вредоносный узел, а злоумышленник может обрабатывать пакеты или просто их удалять.

2. «Серая дыра» (Gray Hole) — это вариация атаки (Black Hole), в которой узлы выборочно отбрасывают некоторые пакеты.

3. «Червь» (Worm hole) — атака червячной дыры — это серьёзная атака, которая может быть запущена, даже если аутентичность и конфиденциальность гарантированы во всех сообщениях. В этой атаке злоумышленник сначала записывает пакеты в одно место в сети, а затем - в другое.

4. «Hello Flood» — атака Hello Flood основанная на том факте, что узел должен транслировать «HELLO PACKETS», чтобы показать своё присутствие соседям. Принимающие узлы могут предполагать, что они находятся в диапазоне связи отправителя. В этой атаке злоумышленник использует злонамеренный узел с высокой степенью передачи, чтобы отправить существующему «HELLO PACKETS» в другое место в сети и объявить своим соседом.

## 2. Контрмеры

Для анализа возможных мер по противодействию приведённым выше атакам был сделан отдельно IMECA анализ отдельно взятых компонентов системы мониторинга состояния здоровья пациентов (кардиограф, инсулиновая помпа, дефибриллятор, сервер обработки данных, база данных). В качестве иллюстрации анализа компонентов в данной статье была приведена IMECA-таблица для одного компонента системы, а именно для инсулиновой помпы (табл. 1). На основе анализа отдельных компонентов был сделан общий IMECA анализ всей системы (табл. 2). После была получена матрица оценки критичности атак на IoT систему (рис. 3) и дерево атак (ATA) IoT системы (рис. 4).

IMECA-техника (Intrusion Modes and Effects Criticality Analysis – анализ видов, последствий и критичности вторжений) была выбрана, поскольку является достаточно удобной и интуитивно понятной.

Данные для анализа IMECA (а именно вероятность и тяжесть) были взяты на основании экспертной оценки [37, 38]. IMECA является модификацией техники анализа FMECA (Failure Modes, Effects and Criticality Analysis, анализ видов, последствий и критичности отказов), который учитывает возможные вторжения в систему [35].

Вероятности появления атак были разделены на низкие, средние и высокие. Где низкой вероятностью является вероятность от $10^{-5}$ до $10^{-6}$, средней — от $10^{-4}$ до $10^{-5}$ и высокой — $10^{-4}$ и выше.

Для тяжести атак была использована следующая классификация – высокая, средняя и низкая.

Таблица 1

IMECA анализ атак на отдельный компонент (инсулиновая помпа) системы мониторинга состояния здоровья пациентов

| Имя компонента | Вид атаки | Природа атаки | Вероятность атаки | Тяжесть атаки | Критичность атаки |
|---|---|---|---|---|---|
| Мотор | Фальсификация данных | Активная | Высокая | Высокая | Высокая |
| Управление энергообеспечением | Лишение сна | Активная | Средняя | Средняя | Средняя |
| Карта памяти | Неэффективное логирование | Пассивная | Средняя | Средняя | Средняя |
| Микроконтроллер | DoS атака | Активная | Высокая | Средняя | Высокая |
| USB передатчик | Атака маршрутизации | Активная | Высокая | Высокая | Высокая |
| | Атака повторного воспроизведения | Активная | Высокая | Высокая | Высокая |
| Датчик давления | Фальсификация данных | Активная | Высокая | Высокая | Высокая |

Высокая – дефект влияет на критическую функциональность или критические данные. У него нет обходного пути.

Средняя – дефект влияет на основные функциональные возможности или основные данные (например, время работы устройств). У этого дефекта есть обходное решение, но это не очевидно и сложно.

Низкая – дефект влияет на незначительные функциональные возможности или некритические данные, и для него можно найти обходное решение.

Для определения критичности была использована формула:

$$C = \max(P, S), \quad (1)$$

где P – вероятность атаки, а S – тяжесть атаки.

Каждая из цифр внутри матрицы является соответствующим номером уязвимости из табл. 2. Данные о вероятности и тяжести атак были взяты исходя из полученной IMECA таблицы.

Кроме того, после построения IMECA матрицы было построено дерево атак (ATA). За основу было взято работу «Attack Tree Analysis for Insider Threats on the IoT using Isabelle» [20], поскольку это интуитивно понятный метод для анализа кибератак. Они очень практично идентифицируют шаги атаки и способы их предотвращения.

**Анализ побочных каналов** обеспечивает эффективный подход для обнаружения как аппаратных «троянов», так и вредоносного программного обеспечения/программного обеспечения, установленного на устройстве [19, 21].

**Обнаружение Трояна**: сигналы стороннего канала, включая температуру, может использоваться для обнаружения троянских программ [24, 25]. Наличие Трояна в цепи обычно влияет на мощность и/или задержку характеристик проводов в цепи, а также передаёт теплораспределение на микросхеме.

**Оценка расстояния**. Использование отношения сигнал / шум в качестве показателя для определения расстояния между считывателем и тегом предлагается на расстоянии. Например, тег может выдать общую информацию, например, тип продукта, при сканировании на расстояние 10 метров, но отпустить его уникальный идентификатор на расстоянии менее 1 метра.

**Аутентификация на основе ролей**. Чтобы предотвратить ответ на запросы злоумышленников или вредоносных узлов в системе, система авторизации на основе ролей проверяет, может ли компонент, например пограничный узел, поставщик услуг или маршрутизатор, получить доступ, поделиться или изменить информацию. Кроме того, для каждого сообщения система авторизации должна проверять, были ли проверены две стороны, участвующие в действии, и имеют ли необходимые полномочия [23].

**Изоляция**. Очень эффективный способ защиты конфиденциальности тегов – изолировать их от всех электромагнитных волн. Один из способов – построить и использовать изоляционные комнаты. Однако строительство таких комнат обычно очень дорого. Альтернативный подход заключается в использовании изолирующего контейнера, который обычно изготавливается из металлической сетки. Этот контейнер, который может блокировать электромагнитные волны определённых частот, называется клеткой Фарадея [28]. Другой подход заключается в том, чтобы затормозить все соседние радиоканалы с помощью активных радиочастотных помех, которые непрерывно прерывают определённые радиочастотные каналы.

**Сопоставление данных.** Данный способ заключается в том, чтобы логировать каждое действие каждого устройства. Сложность для системы мониторинга пациентов заключается в том, что в системе работают различные

устройства и они отправляют различные данные. Это значительно усложняет логирование и анализ залогированных данных. Но данный способ позволяет предотвратить утечку данных или даже потенциальный перехват данных.

Таблица 2

IMECA анализ атак всей системы мониторинга состояния здоровья пациентов

| № п/п | Режим атаки | Природа атаки | Вид последствия | Вероятность возникновения | Тяжесть последствия | Критичность |
|---|---|---|---|---|---|---|
| 1 | Троянский конь | Активная | Получение секретной информации злоумышленником. Возможность внедрения и управления системой | Высокая | Высокая | Высокая |
| 2 | Атака по сторонним каналам | Активная | Получение секретной информации злоумышленником | Высокая | Высокая | Высокая |
| 3 | Маскировка | Активная | Получение секретной информации злоумышленником. Возможность внедрения и управления системой | Средняя | Высокая | Высокая |
| 4 | Физическая атака | Активная | Получение секретной информации злоумышленником. Частичная или полная остановка работы системы | Средняя | Средняя | Средняя |
| 5 | Разряд батареи | Активная | Частичная или полная остановка работы системы | Высокая | Высокая | Высокая |
| 6 | Неавторизованный обмен данными | Активная | Получение секретной информации злоумышленником. Возможность внедрения и управления системой | Высокая | Высокая | Высокая |
| 7 | Лишение сна | Активная | Частичная или полная остановка работы системы. | Средняя | Средняя | Средняя |
| 8 | Несетевые сторонние атаки | Активная | Получение секретной информации злоумышленником. | Средняя | Высокая | Высокая |
| 9 | Атака повторного воспроизведения | Пассивная | Получение секретной информации злоумышленником | Высокая | Высокая | Высокая |
| 10 | Подслушивание | Пассивная | Получение секретной информации злоумышленником | Высокая | Высокая | Высокая |
| 11 | Атаки маршрутизации | Активная | Частичная или полная остановка работы системы | Высокая | Высокая | Высокая |

**Криптография**: данный метод заключается в использовании криптографических схем, например шифрования, для защиты протоколов связи

является одной из наиболее эффективных средств защиты от множества атак, включая подслушивание и простые атаки маршрутизации на уровне связи.

**Методы шифрования / дешифрования**, разработанные для традиционных проводных сетей, напрямую не применимы к большинству компонентов IoT, в частности, к небольшим периферийным узлам с батарейным питанием [22]. Конечные устройства обычно представляют собой крошечные датчики, которые имеют ограниченную ёмкость аккумулятора, вычислительную мощность и память.

| Тяжесть | Вероятность | | |
|---|---|---|---|
| | Низкая | Средняя | Высокая |
| Высокая | | 3, 5, 7, 8 | 1, 2, 4, 10 |
| Средняя | | 6 | 9, 11 |
| Низкая | | | |

Рисунок 3 – Матрица оценки критичности атак на IoT систему

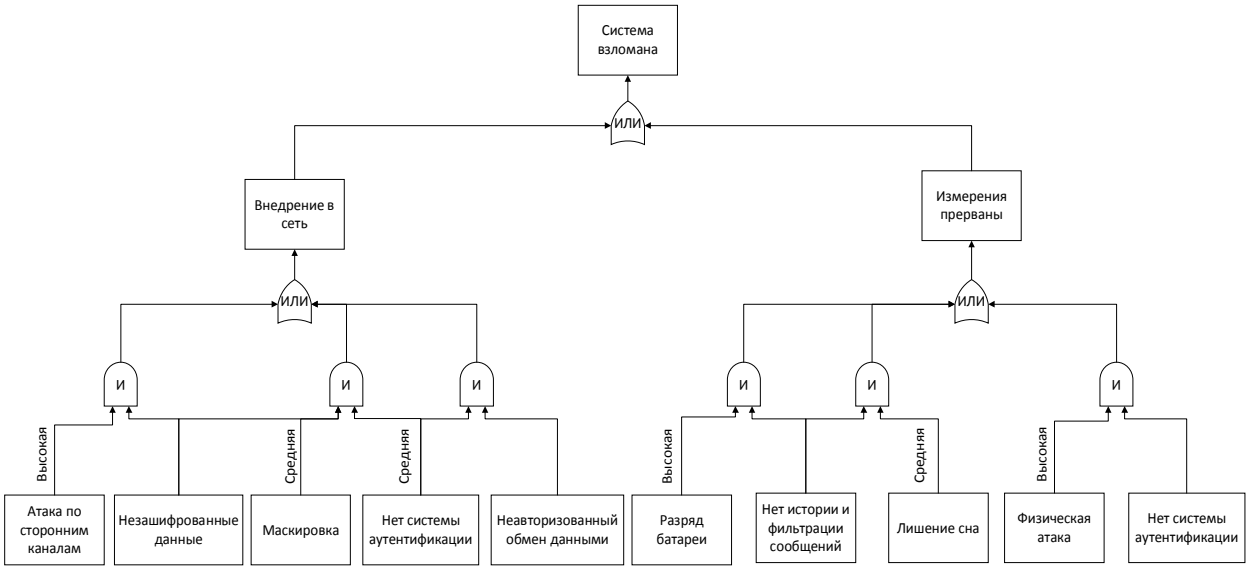


Рисунок 4 – Дерево атак IoT системы

Использование шифрования увеличивает объём использования памяти, потребление энергии, задержку и потерю пакетов. Но варианты AES (Advanced Encryption Standard) дают многообещающие результаты для обеспечения безопасной связи в IoT [25]. К сожалению, в настоящее время нет перспективных методов шифрования с открытым ключом, которые обеспечивают достаточную безопасность при соблюдении простых требований.

## Заключение

Результатом данной работы является анализ основных атак с помощью метода IMECA, и на его основе было построено ATA на примере системы мониторинга состояния здоровья пациентов. С помощью дерева атак (ATA) были выявлены некоторые возможные уязвимости системы. Кроме того, данный анализ показывает, какие результаты могут быть достигнуты при совершении различных

видов атак. Он является основой для анализа оценки ресурсов, которые необходимы для того, чтобы предпринять представленные в статье атаки и/или организовать контрмеры, направленные против них.

В дальнейших работах планируется исследовать систему мониторинга состояния здоровья пациентов с точки зрения безопасности с помощью механизма марковских моделей. Планируется также расширить список различных видов атак и контрмер, направленных против них.

**Список литературы**

1. Singh, D, G., A. J., Tripathi A survey of Internet-of-Things: Future vision, architecture, challenges and services IEEE World Forum on Internet of Things, no. 210, 2010, pp. 278 - 285.

2. Atzori, L., Iera, A., Morabito, G. The Internet of Things: A survey. Computer Networks, no. 15, 2010, pp. 87–96.

3. Mozaffari-Kermani, M., Sur-Kolay, S., Raghunathan, A. Systematic poisoning attacks on and defenses for machine learning in healthcare. IEEE J. Biomedical and Health Informatics, no. 210, 2010, pp. 278-285.

4. Hagai Bar-El An Introduction to Side Channel Attacks. Discretix Technologies limited, no. 210, 2010, pp. 93–105.

5. CISCO. The Internet of Things reference model. Available at: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf (accessed 5 March 2014)

6. Tehranipoor, M., Koushanfar, F. A survey of hardware Trojan taxonomy and detection. IEEE Design and Test of Computers, no. 210, 2010, pp. 56 - 75.

7. Chakraborty, R. S., Wolff, F., Paul, S. MERO: a statistical approach for hardware Trojan detection. Proceeding Cryptographic Hardware and Embedded Systems. Springer, no. 210, 2010, pp. 1074 – 1079.

8. Lesperance, N., Kulkarni, S. Hardware Trojan detection using exhaustive testing of K-bit subspaces. Proc. IEEE Asia and South Pacific Design Automation Conference, no. 210, 2010, pp. 93 – 105.

9. Salmani, H., Tehranipoor, M. M. Vulnerability analysis of a circuit layout to hardware Trojan insertion. IEEE Trans. Information Forensics and Security, no. 210, 2010, pp. 278 - 285.

10. Wehbe, T., Mooney, V. J., Keezer, D. C. A novel approach to detect hardware Trojan attacks on primary data inputs. Proceeding ACM Wkshp. Embedded Systems Security, no. 210, 2010, pp. 158-160.

11. Bhasin, S., Regazzoni, F. A survey on hardware Trojan detection techniques. Proceeding IEEE Int. Symp. Circuits and Systems, no. 210, 2010, pp. 810-816.

12. Shila, D. M. Design, implementation and security analysis of hardware Trojan threats in FPGA. Proceeding IEEE Int. Conf. Communications, no. 210, 2010, pp. 278 - 285.

13. Tanaka, H. Information leakage via electromagnetic emanations and evaluation of TEMPEST countermeasures. Springer, no. 210, 2010, pp. 1074–1079.

14. Vuagnoux, M., Pasini, S. Compromising electromagnetic emanations of wired and wireless keyboards. Proceeding USENIX Security Symposium, no. 210, 2010, pp. 2787–2805.

15. Nia, A. M., Raghunathan, A., Jha, N. K. Physiological information leakage: A new frontier in health information security. IEEE Trans. Emerging Topics in Computing, no. 210, 2010, pp. 56-75.

16. Singh, D., Tripathi, G. A survey of Internet-of-Things: Future vision, architecture, challenges and services. Proceeding IEEE World Forum on Internet of Things, no. 210, 2010, pp. 168-175.

17. Walters, J. P., Liang, Z., Shi, W. Wireless sensor network security: A survey, Security in Distributed, Grid, Mobile, and Pervasive Computing. Proceeding IEEE World Forum on Internet of Things, no. 210, 2010, pp. 810-816.

18. Padmavathi, G., Shanmugapriya, D. A survey of attacks, security mechanisms and challenges in wireless sensor networks. Proceeding of IEEE/ION PLANS'06, no. 210, 2006, pp. 2787–2805.

19. Wang, X., Chellappan, S., Gu, W. Search-based physical attacks in sensor networks. Proc. IEEE 14th Int. Conf. Computer Communications and Networks, no. 21, 2010, pp. 278 - 285.

20. Becher, A., Benenson, Z. Tampering with Motes: Real world Physical Attacks on Wireless Sensor Networks. Springer, no. 210, 2010, pp. 278 - 285.

21. Anderson, R., Kuhn, M. Tamper resistance-a cautionary note. Proc. 2nd USENIX Wkshp. Electronic Commerce, no. 2, 2014, pp. 158-160.

22. Zorzi, M., Gluhak, A., Lange S. From today's Intranet of Things to a future Internet of Things: A wireless-and mobility-related view. IEEE Wireless Communications, no. 210, 2012, pp. 56-75.

23. Hernandez, G., Arias, O., Buentello D., Jin, Y. Smart Nest thermostat: A smart spy in your home. Proceding Black Hat USA, no. 210, 2010, pp. 278 - 285.

24. Strielkina, A., Uzun, D. Cybersecurity of medical systems: challenges and solutions in the context of the internet of things. Radioelectronic and computer systems, Kharkiv, 2017, no. 1, pp. 44–50.

25 Juels, A. RFID security and privacy: A research survey. IEEE J. Selected Areas in Communications, no. 210, 2000, pp. 810-816.

26. Syamsuddin, I., Dillon, T., Chang, E., Han S. A survey of RFID authentication protocols based on hash-chain method. Proceeding IEEE 3rd Int. Conf. Convergence and Hybrid Information Technology, no. 8, 2013, pp. 93 – 105.

27. Peris-Lopez, P. J., Hernandez-Castro, C., Estevez-Tapiador, A. RFID systems: A survey on security threats and proposed solutions. Proceding Personal Wireless Communications. Springer, no. 210, 2013, pp. 1074–1079.

28. G. Hancke, Eavesdropping attacks on high-frequency RFID tokens. Proceeding 4th Wkshp. RFID Security, no. 8, 2010, pp. 93–105.

29. Grobauer, B., Walloschek, T. Understanding cloud computing vulnerabilities. IEEE Security Privacy, no. 210, 2010, pp. 56-75.

30. Karakehayov, Z., Using REWARD to detect team black-hole attacks in wireless sensor networks. Proceeding Workshop. Real-World Wireless Sensor Networks, no. 210, 2010, pp. 163-165.

31. Revathi, B., Geetha, D. A survey of cooperative black and gray hole attack in MANE. Int. J. Computer Science and Management Research, no. 210, 2010, pp. 93–105.

32. Garcia-Morchon, O., Kumar, S., Struik, R. Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview. Available at: https://tools.ietf.org/html/draft-garcia-core-security-04 (accessed 02 April 2012)

33. Wallgren, L., Raza, S., Voigt, T. Routing attacks and countermeasures RPL-based Internet of Things. Int. J. Distributed Sensor Networks, no. 210, 2010, pp. 278-285.

34. Douceur, J. R. The Sybil attack. Peer-to-peer Systems. Springer, no. 8, 2013, pp. 93–105.

35. Sudani, M., Al-Khafaji, Kharchenko, V.S. Method of IMECA-based security assessment: case study for building automation system. National Aerospace University KhAI, no. 210, 2010, pp. 15–26.

36. Strielkina, A., Kharchenko, V., Uzun, D. Modelling of Healthcare IoT Using the Queueing Theory. Proceedings IEEE of 9th International International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, no. 8, 2014, pp. 3–15.

37. Securing IoT Devices in the Increasingly Connected Hospital System. Available at: https://healthitsecurity.com/news/securing-iot-devices-in-the-increasingly-connected-hospital-system (accessed 02.06.2016).

38. Connected Medical Devices: Overcoming Key IoT Challenges System. Available at: https://www.sensorsmag.com/components/connected-medical-devices-overcoming-key-iot-challenges (accessed 08.12.2017).

Поступила в редакцию 29.05.2018

## Аналіз методів і засобів оцінювання і забезпечення кібербезпеки IoT системи

Описано кібербезпеку Internet of Things система (Інтернет вещей, IoT). Проведено аналіз основних атак на IoT системи на прикладі системи моніторингу стану здоров'я пацієнтів за допомогою методу IMECA (Intrusion Modes and Effects Criticality Analysis - аналіз видів, наслідків та критичності вторгнень) і на його основі побудувано дерево ATA (Analysis of Tree Attack – аналіз атак у вигляді дерева). Результатом роботи являється аналіз основних атак за допомогою методу IMECA для окремо взятих компонентів системи і системи в цілому.

***Ключові слова:*** IoT, охорона здоров'я, безпека, конфіденційність, IMECA, ATA.

## Analysis of Methods and Techniques of Estimation and Providing Cybersecurity of the IoT System

The cybersecurity of the Internet of Things system (Internet of things, IoT) has been investigated. The analysis of the main attacks on the IoT system was carried out using the IMECA method (Intrusion Modes and Effects Criticality Analysis) and based on it, the ATA tree (Attack Tree Analysis) was constructed. The result of this work is the analysis of the main attacks using the IMECA method for the individual components of the system and the system as a whole.

***Keywords****:* IoT, healthcare, safety, cybersecurity, IMECA, ATA.

**Сведения об авторах:**

**Ляхов Дмитрий Эдуардович** – студент кафедры компьютерных систем, сетей и кибербезопасности, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Украина.

**Стрелкина Анастасия Андреевна** – аспирант, ассистент кафедры компьютерных систем, сетей и кибербезопасности, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Украина.

**Узун Дмитрий Дмитриевич** – канд. техн. наук, доцент кафедры компьютерных систем, сетей и кибербезопасности, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Украина.