О кибербезопасности систем Интернета Вещей

Д.Е. Намиот, В.А. Сухомлин

***Аннотация*—В настоящей статье рассматриваются вопросы кибербезопасности систем Интернета Вещей (IoT). Такого рода системы всегда представляют собой интеграцию множества различных технологий. Это, естественным образом, увеличивает возможности для атакующих по воздействию как на программные, так и на аппаратные подсистемы проектов. Множество различных поставщиков со своими решениями и циклами по обновлению программного обеспечения многократно увеличивает возможности атак на цепочки поставок. Исторически, системы IoT использовали и продолжают использовать самые разнообразные коммуникационные решения, что усложняет защиту данных в этой плоскости. Оконечные устройства (сенсоры, актуаторы) также сильно различаются по своим возможностям и характеристикам, что исключает какие-то единые решения в этой области. Пожалуй, единственным "стандартным" элементом IoT систем служат облачные хранилища, кибербезопасностью которых необходимо заниматься и вне IoT проектов. Дополнительную сложность работам по кибербезопасности IoT придает то, что за термином IoT скрывается целое семейство подходов (архитектур) – промышленный Интернет Вещей, Интернет нано-вещей и т.д. К возможным атакам на Iot системы относят кражу конфиденциальных данных, кражу личных данных, повреждение инфраструктуры, повреждение данных, несанкционированное наблюдение, незаконное изменение данных и несанкционированное использование возможностей устройств.**

***Ключевые слова*—кибербезопасность, кибератаки, Интернет Вещей**

I. Введение

Эта статья написана для поддержки учебного процесса магистратуры Программное обеспечение вычислительных сетей факультета ВМК МГУ имени Ломоносова [1]. В учебную программу входит курс по Интернету Вещей (IoT), структура и задачи которого были достаточно подробно описаны в наших публикациях [2,3]. Одним из партнеров этой программы выступает Сбер, более конкретно – Департамент кибербезопасности Сбербанка [4], соответственно, учебные программы меняются со временем, чтобы учитывать пожелания и нужды партнеров.

Статья получена 10 декабря 2022. Исследование выполнено при поддержке Междисциплинарной научно-образовательной школы Московского университета «Мозг, когнитивные системы, искусственный интеллект»

Д.Е. Намиот – МГУ имени М.В. Ломоносова (email: dnamiot@gmail.com)
В.А. Сухомлин - МГУ имени М.В. Ломоносова (email: sukhomlin@mail.ru)

Компания Микрософт определяет кибербезопасность как набор процессов, передовых практик и технологий, которые помогают защитить критически важные системы и сети от цифровых атак. Соответственно, угроза кибербезопасности — это преднамеренная попытка получить доступ к системе со стороны человека или некоторой организации [5].

Википедия, со ссылкой на энциклопедию Britannica [б], пишет, что компьютерная безопасность, кибербезопасность или безопасность информационных технологий (ИТ-безопасность) — это защита компьютерных систем и сетей от атак злоумышленников, которые могут привести к несанкционированному раскрытию информации, краже или повреждению оборудования, программного обеспечения или данных, а также к нарушениям или неправильному предоставлению услуг [6]. Это, на наш взгляд, более точная формулировка, поскольку для нарушения работы системы вовсе не обязательно получать к ней доступ.

Лаборатория Касперского говорит о том, что кибербезопасность (или компьютерная безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных [7]. Похоже на определение из Википедии, хотя можно заметить, например, что в системах Интернета Вещей есть еще сенсоры и актуаторы, которые также могут быть атакованы злоумышленниками и нуждаются в защите. Кстати, атаки на такие устройства вовсе не обязательно будут цифровыми.

SAP придерживается схожего определения. Кибербезопасность — это практика защиты сетей, устройств, приложений, систем и данных от киберугроз. Основная цель заключается в отражении атак, которые пытаются получить доступ к данным или уничтожить их, вымогать деньги или нарушить нормальное выполнение бизнес-операций — независимо от того, исходят ли эти атаки изнутри или извне организации [8].

Определения кибербезопасности именно Интернета Вещей более конкретны. Кибербезопасность IoT — это технологический сегмент, посвященный защите связанных устройств и сетей в Интернете вещей (IoT).

Интернет вещей предполагает подключение системы взаимосвязанных вычислительных устройств, механических и цифровых машин, предметов, животных и/или людей к Интернету [9].

В целом, само название Интернет Вещей предполагает наличие распределенной системы, что, естественно, увеличивает поверхность атаки. Институт Fraunhofer, например, предлагает следующую иллюстрацию:

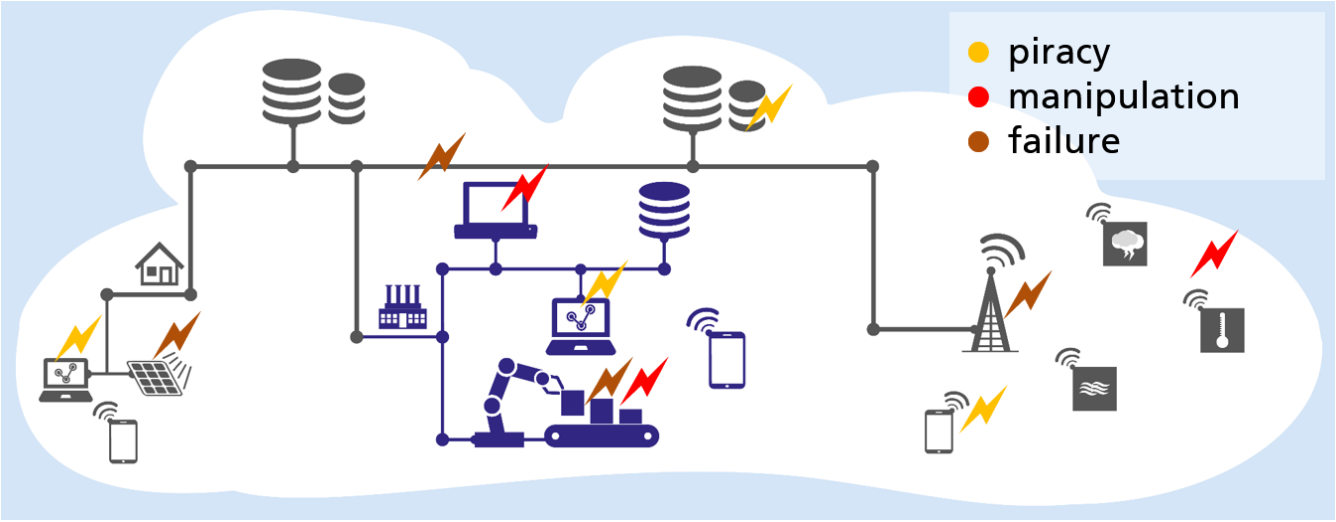

Рис. 1. Атаки на IoT [10].

Различные типы атак возможны для всех компонент системы.

Оставшаяся часть статьи структурирована следующим образом. В разделе II мы останавливаемся на архитектуре систем Интернета Вещей, необходимой для понимания системы безопасности. Раздел III посвящен атакам. И в разделе IV мы приводим обзор стандартов в области кибербезопасности IoT.

II Архитектура IoT систем

Первым и самым главным моментом является тот факт, что Интернет Вещей – это не программный продукт и не какая-то четко очерченная технология. Такого программного продукта как IoT нет, и нет, соответственно, никаких инструментов для его проверки, верификации и т.п. IoT – это всегда интеграция множества различных систем (технологий). Именно в этой интеграции и состоит весь смысл и значение (value) IoT систем и проектов. На рисунке 2 представлен функциональный анализ IoT систем

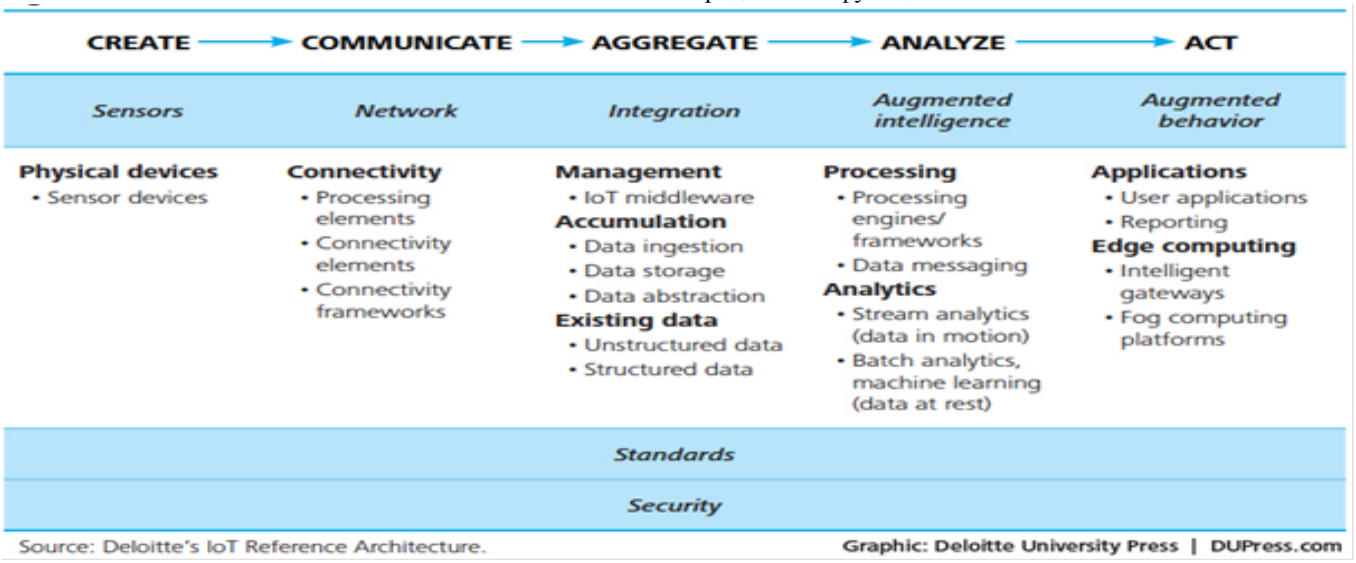

Рис. 2. Функциональный анализ IoT [11].

Очевидно, что вмешательство в работу системы (или нарушение работы системы) возможно на любом из этапов.

Следующий важный момент состоит в том, что термин IoT был придуман для простоты объяснения того факта, что у нас есть сеть связанных объектов. Эта сеть может использовать самые разные протоколы и термин Интернет, вообще говоря, здесь не подходит. Слово "Интернет" здесь использовалось как просто всем понятное описание сети. В связи с этим, такого рода "Интернет" систем существует уже довольно много. Например, мы можем говорить о:

- IIoT – Industrial Internet of Things [12]
- IoNT - Internet of Nano Things [13]
- IoST - Internet of Space Things [14]
- MIoT - Marine Internet of Things [15]
- OIoT - Oceans Internet of Things [16]

В этой связи NIST призывает использовать более корректный термин – NoT (Network if Things – сеть вещей) [17]. В более современной трактовке – это все примеры киберфизических систем (CPS) [18]. И, естественно, мы должны уже говорить о кибербезопасности кибер-физических систем [19].

Проект государственного департамента внутренней безопасности Cyber Physical Systems Security [20] говорит о безопасности киберфизических систем и устройств Интернета Вещей.

CPS поддерживает множество технологий, основные из них представлены на рисунке 3.

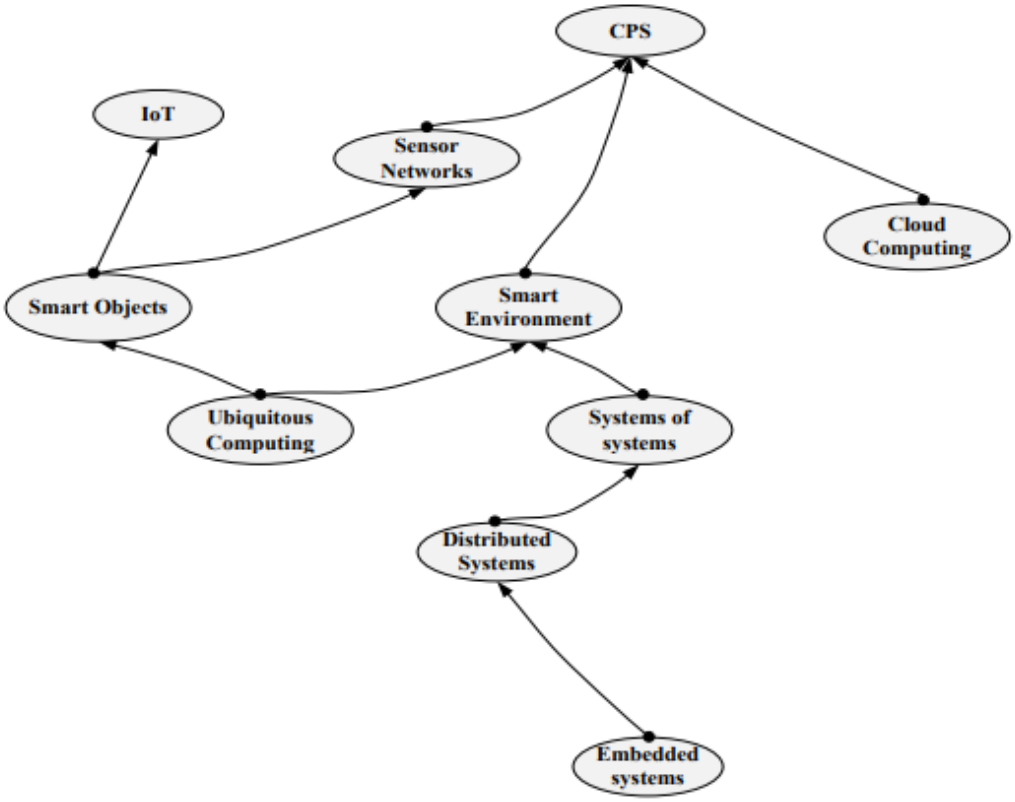

Рис. 3. Технологии CPS [21]

Роль IoT в таком случае сводится до оконечных устройств. При этом, согласно определению NIST, устройство IoT должно иметь физический и сетевой интерфейсы (рис. 4)

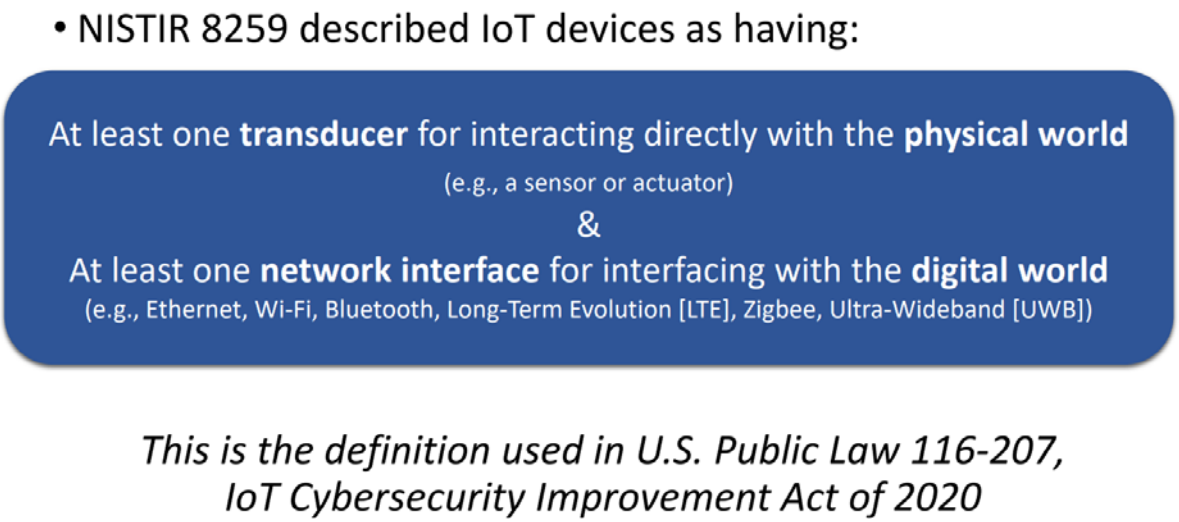

Рис. 4. IoT устройство

В работе [22] приводится схожая с рисунком 2.

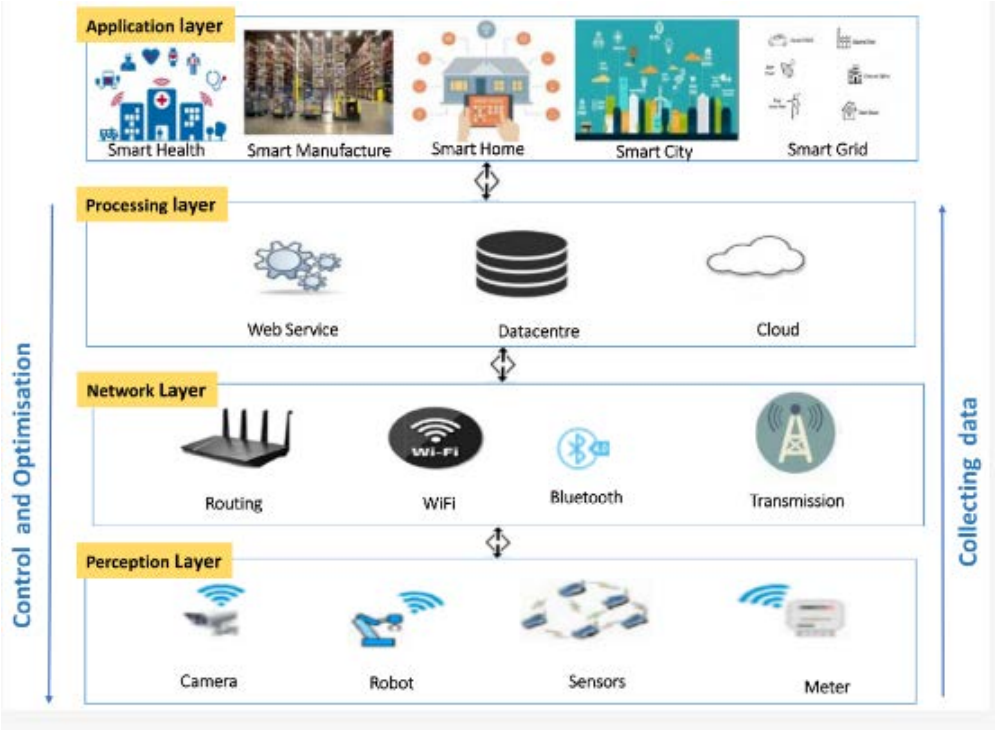

Рис. 4 Архитектура IoT [22]

Отметим, что Умный Город, Умный дом и т.д. выступают как приложения, использующие данные, собираемые IoT системой (отсюда – города, управляемые данными [23, 24]).

Элементы архитектуры (уровни архитектуры) систем IoT находятся на разных стадиях стандартизации. Очевидно, что сетевой уровень стандартизован полностью, IoT использует стандартные протоколы. Проблемой здесь является то, что не существует некоторого единого “протокола IoT”. По экономическим, в первую очередь, причинам (множество разных производителей) в IoT используются, пожалуй, все существующие сетевые протоколы и какой-либо унификации уже никогда не будет.

С другой стороны, оконечные устройства, помимо отсутствия каких-либо стандартных программных интерфейсов еще и принципиально разнятся по своих характеристикам (следовательно, и по возможностям атак). Например, если мы рассматриваем типичную IP камеру, то это компьютер со множеством интерфейсов, с веб-сервером для поддержки ONVIF и т.д. (рис. 5)

Compression Type	H.264, M-JPEG, JPEG
Network Properties	Interface: 10/100baseT Ethernet, RJ45 Network Protocols: RTP, Telnet, UDP, TCP, IP, HTTP, HTTPS, FTP, DHCP*
Physical Specifications	Weight g: 542 Dimensions mm: 58 x 66 x 122
Environmental Specifications	Operating Temperature °C: -20 ~ +50 Operating Humidity %: 20 ~ 93
Additional info	Dinion2X Day/Night IP cameras are progressive scan CCD cameras. They can tri-stream video simultaneously - on two H.264 streams and one M-JPEG stream. Equipped with 20-bit DSP with 2X-dynamic, they have a wide dynamic range for a sharper, more detailed image without standing color reproduction. * IGMP V2/V3, ICMP, ARP, SMTP, SNTP, SNMP, 802.1x, UPnP.

Рис. 5. IP камера

А некоторый датчик расхода с пьезоэлектрическим эффектом (рис. 6) вырабатывает энергию только на отправку простых сообщений в протоколе типа M-Bus

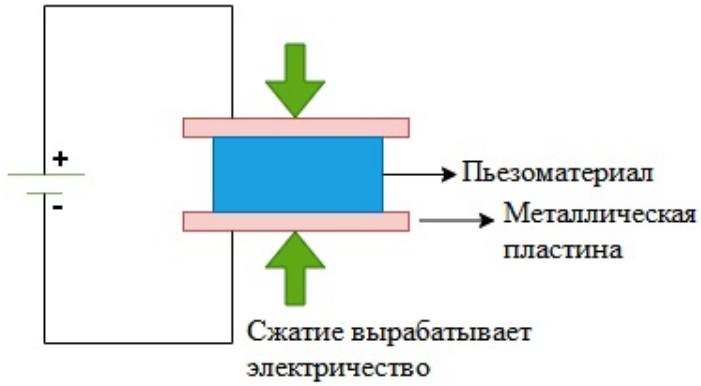

Рис. 6. Пьезоэлектрический датчик [25].

Очевидно, что возможности воздействия (и инструменты такого воздействия) на эти устройства разные.

А если обратиться к решениям для IoNT (nano things), то там и сенсоры и сети представляют собой совершенно отличные от других элементы (рис. 7).

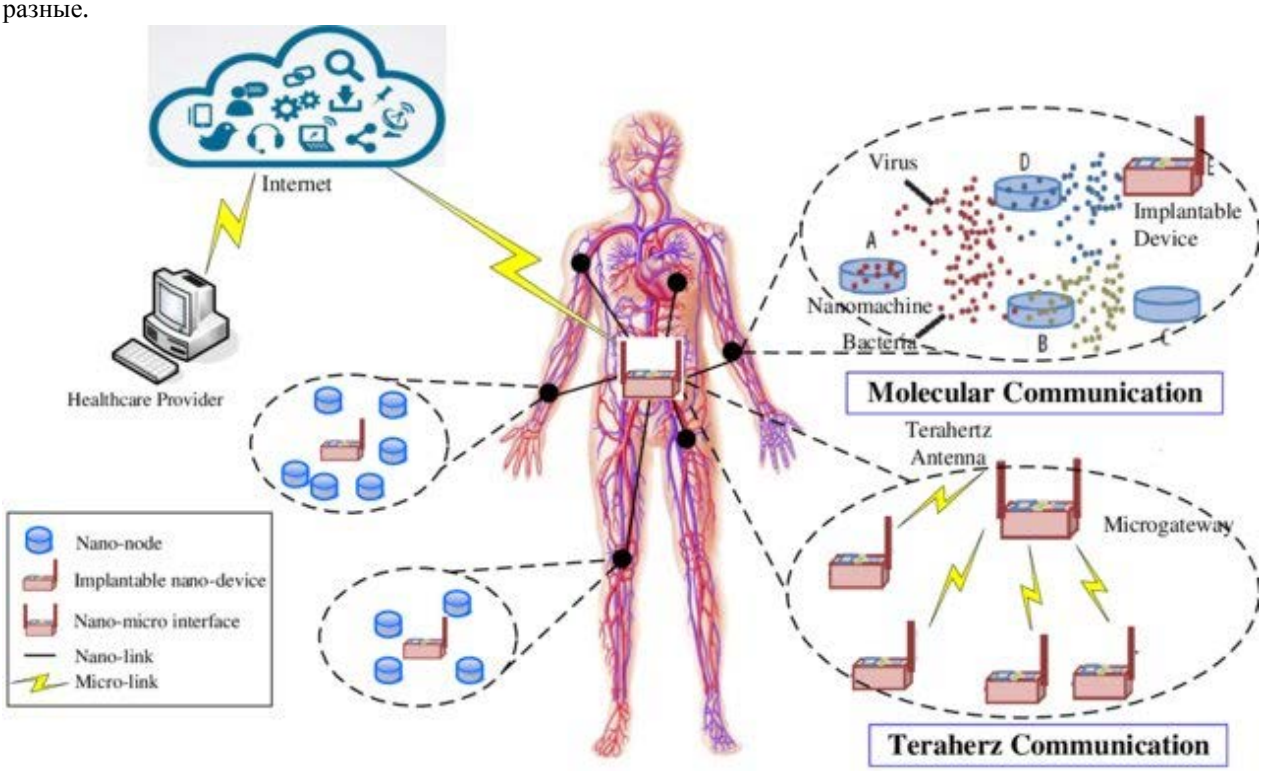

Рис.7. IoNT [26]

Коммуникационные возможности сенсорных узлов часто могут создавать побочные эффекты с точки зрения приватности, например. Так, информация о факте существования беспроводного узла (просто представление узла, без необходимости соединения с ним) может быть использована для оценки местоположения (сетевая пространственная близость) [27]. MAC-адрес беспроводного узла (Bluetooth, Wi-Fi) мультимедийной панели автомобиля (также безо всякого соединения) может быть использован для трекинга и т.п.

С точки зрения кибербезопасности, популярное на сегодняшний день, направление цифровых двойников нужно также рассматривать вместе с IoT. В цифровом двойнике реальные данные физического объекта поступают в реальном времени в его (объекта) цифровую модель (имитационную систему) [28].

С одной стороны, цифровые двойники могут рассматриваться как инструментарий анализа кибербезопасности, поскольку представляют собой цифровую копию объекта. С другой стороны, обмен данными между физическим объектом и его виртуальным представлением выглядит так же, как и обмен данными в IoT системе. Соответственно, цифровой двойник также может стать объектом атаки [29].

Исходя из вышесказанного, можно утверждать, что не существует некоторого единого универсального подхода

к кибербезопасности систем Интернета Вещей. Именно эта идея – “No one-size-fits-all” и положена в основу подхода NIST к кибербезопасности IoT систем (рис. 8).

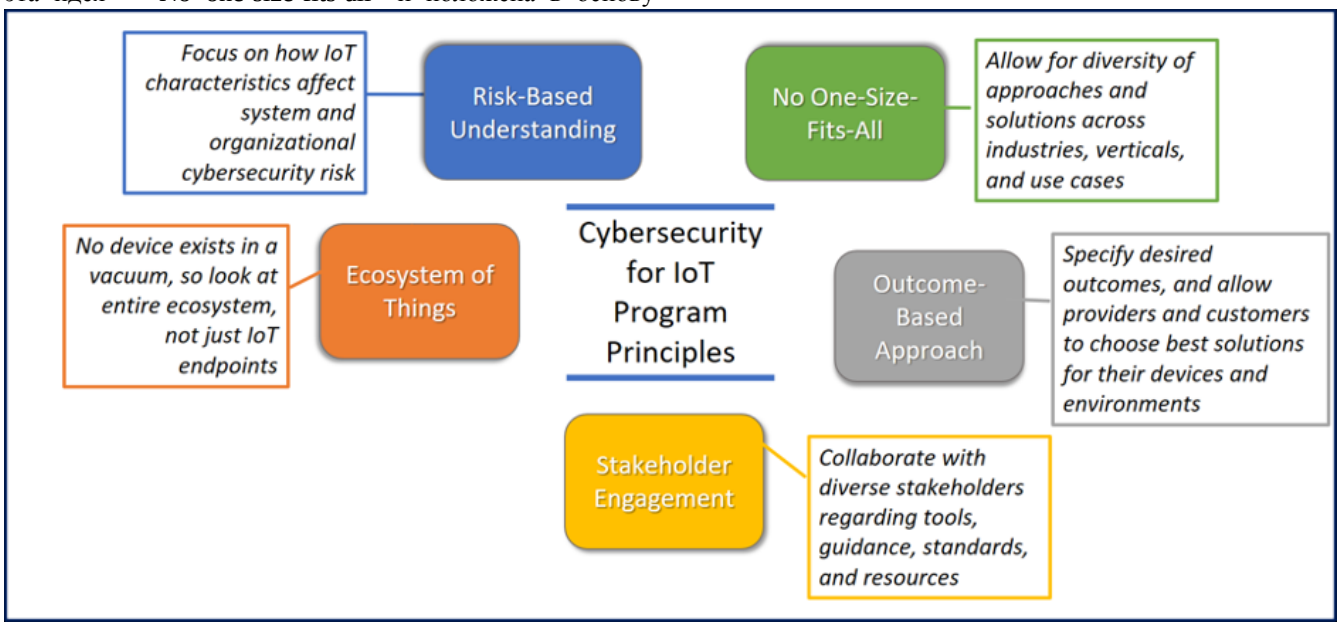

Рис. 8. NIST о кибербезопасности IoT [30].

Еще один момент, который непосредственно следует из интеграционного характера IoT систем – это опасность атак цепочки поставок, что многократно отмечается в литературе [31]. Множество компонент от разных вендоров, свои циклы обновления – все это увеличивает уязвимость к таким атакам [32].

III Угрозы и атаки

Можно отметить, что все таксономии здесь сосредоточены, в основном, вокруг атак сетевой компоненты IoT.

Кибербезопасность для облачных решений, конечно, исследуется и без связи с IoT.

Что касается оконечных устройств, то, как говорилось выше, они очень сильно различаются по своим возможностям. Очевидно, что первая проблема, с которой здесь приходится иметь дело, есть потенциальный физический доступ к устройствам. Очевидно, что во многих проектах (например, сбор данных в ЖКХ) нет возможности надежно контролировать доступ к датчикам.

Вектор возможных атак в киберфизических системах анализировался в работах [21, 33-38] - кража конфиденциальных данных, кража личных данных, повреждение инфраструктуры, повреждение данных, несанкционированное наблюдение, незаконное изменение данных, несанкционированное использование возможностей устройства (рис. 9).

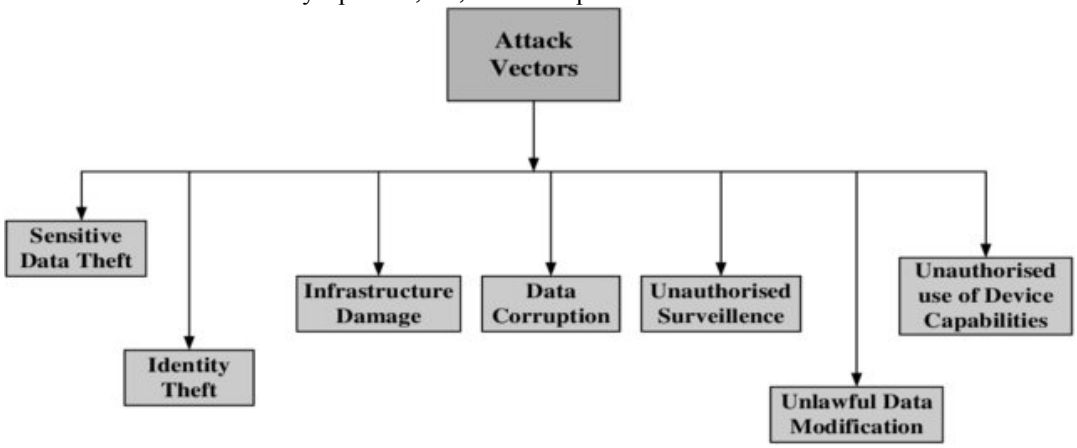

Рис. 9. Атаки на киберфизические системы [21]

Возможные атаки на CPS представлены на рисунке 10.

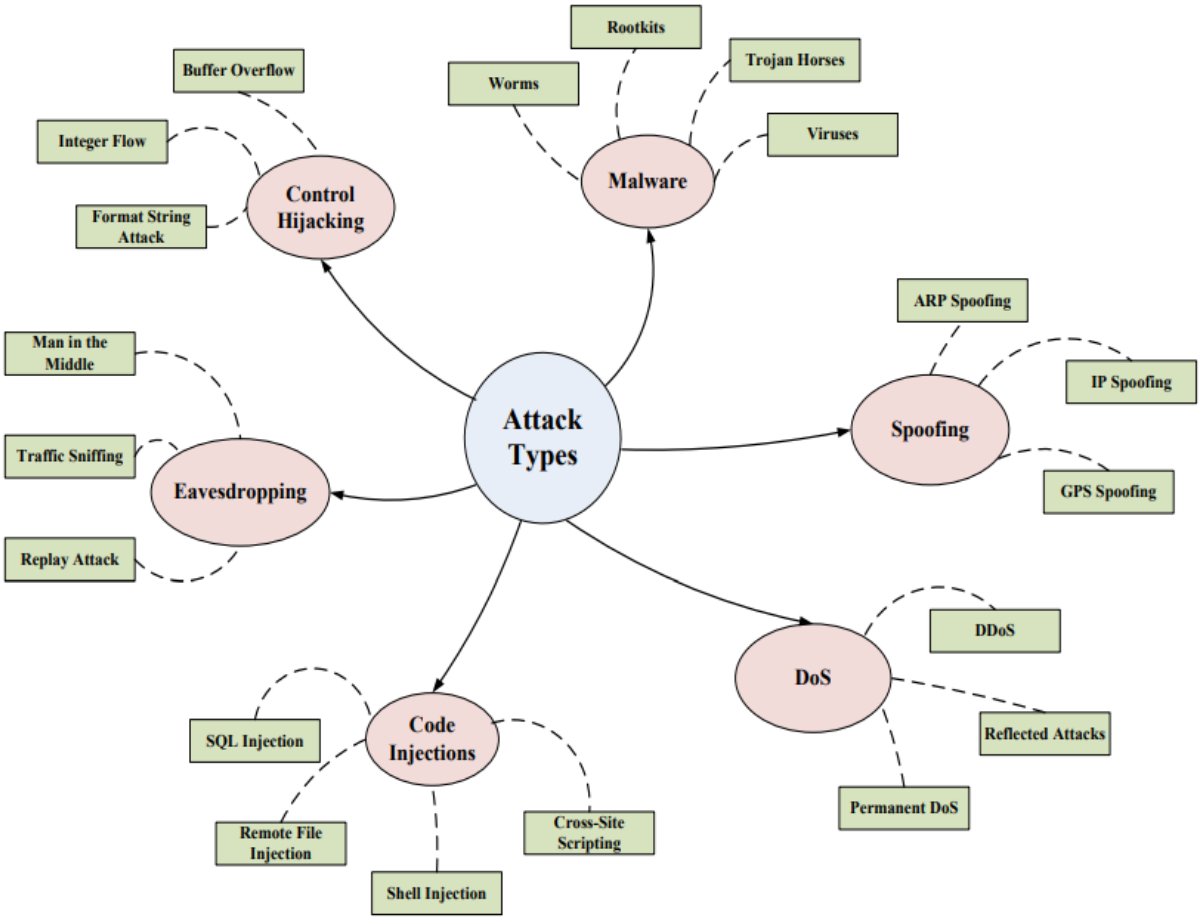

Рис. 10. Атаки на CPS [21]

Исследовательское подразделение компании Palo Alto Networks приводит следующую статистику по атакам на IoT системы (рис.11). По их статистике 57% IoT-устройств уязвимы для атак средней или высокой степени серьезности, что делает IoT легкой задачей для злоумышленников. 41% атак используют уязвимости устройств.

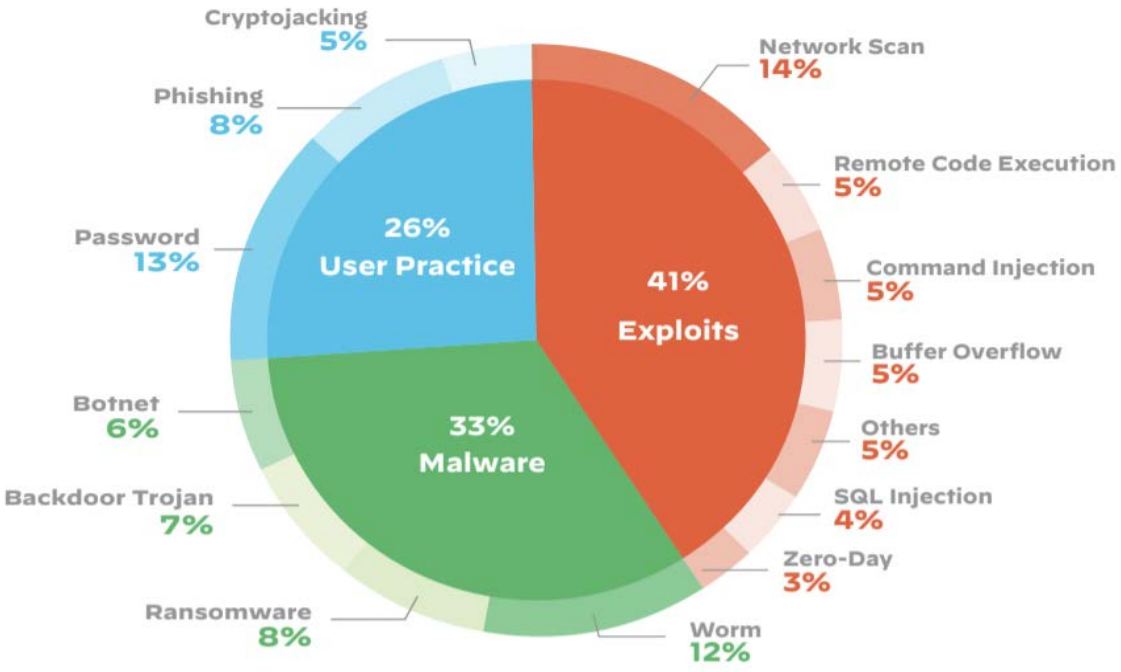

Рис. 11. Атаки на IoT системы [39]

В работе [22] приводится классификация атак по

уровням функциональной архитектуры IoT и способы отражения (предупреждения) атак (рис. 12)

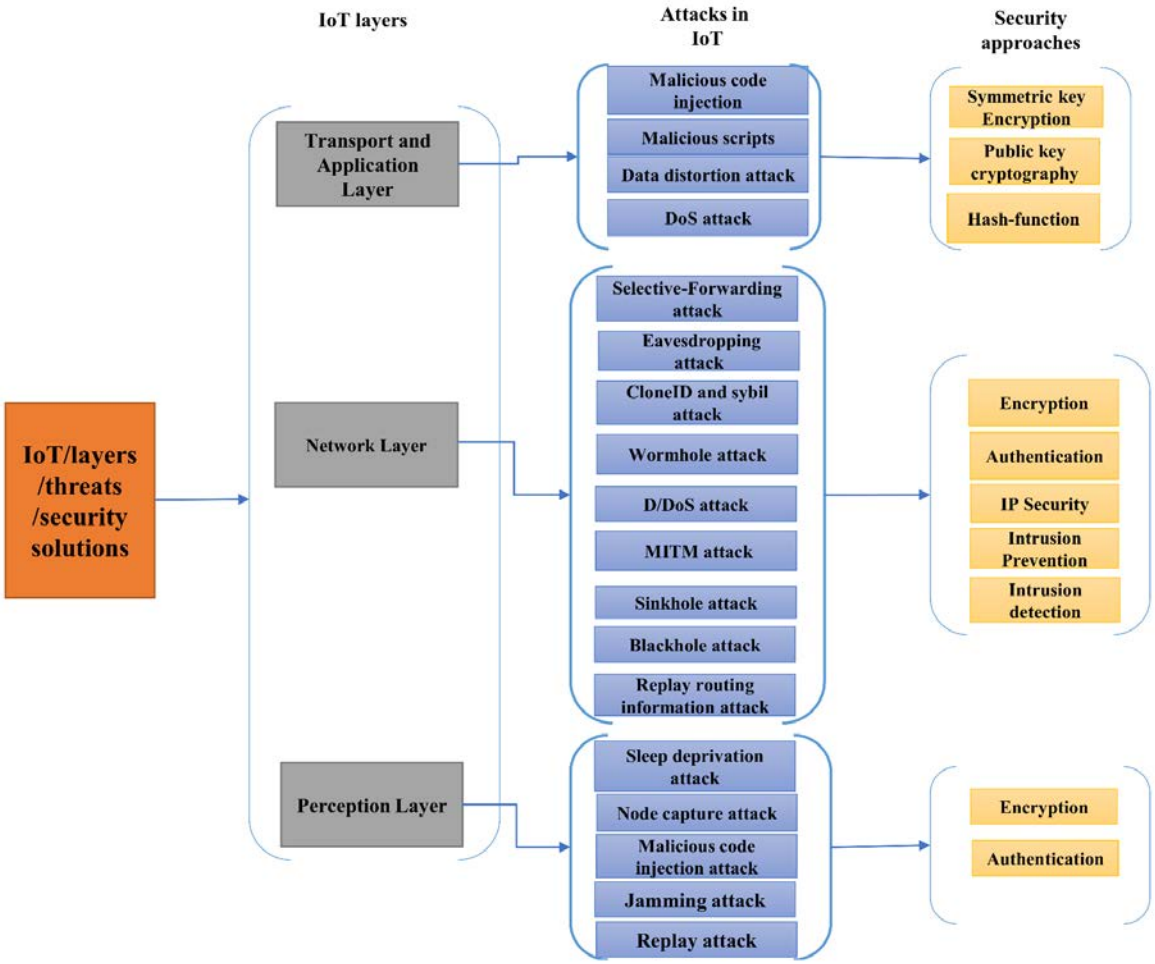

Рис. 12. Атаки по уровням IoT [22].

На уровне коммуникаций рекомендации в академической литературе достаточно очевидные – использовать безопасные версии протоколов (рис. 13).

IoT Layers	Protocols	Security Solution
Application layer	CoAP, MQTT	CoAPs, MQTTs
Transport layer	UDP, TCP	DTLS, TLS
Network layer	IPv6, RPL	IDS, Secure RPL, IPsec
Perception layer	IEEE 802.14.5	IEEE 802.24.5 security

Рис. 13. Безопасные протоколы [22].

Однако приведенная картина касается IP-протоколов и их производных. Мы уже отмечали выше, что IoT использует, на самом деле, самые разные протоколы и реальная картина будет гораздо сложнее. На практике, решения по безопасности для LoRaWAN и NB-IoT, например, будут разными.

Еще один момент, на котором необходимо остановиться – это внедрение моделей машинного обучения в IoT системы. В первую очередь, конечно, в анализ собираемых данных. Дискриминантные модели машинного обучения подвержены состязательным атакам [40]. В определенных случаях, именно системы машинного обучения могут стать слабым звеном IoT систем.

IV Стандарты кибербезопасности IoT

Говоря о стандартах в данной области можно отметить следующие моменты.

Во-первых, это, конечно, NIST с серией NISTIR 8259 [41]. Это руководство для производителей и сторонних разработчиков IoT устройств. Определяет набор действий, которым должны следовать производители IoT при разработке и поддержке устройств IoT. Итоговые документы:

- NISTIR 8259: Рекомендации для производителей устройств IoT
- NISTIR 8259A: базовый уровень кибербезопасности основных устройств

- NISTIR 8259B: Основные базовые возможности нетехнической поддержки Интернета вещей

Последний пункт говорит о том, что необходимо обеспечить поддержку и администрирование устройств IoT конечными пользователями.

Европейский документ ETSI EN 303 645 [42] определяет высокоуровневую модель безопасности и защиты данных для потребительских устройств IoT, которые подключены к сетевой инфраструктуре (такой как Интернет или домашняя сеть) и их взаимодействие с соответствующими сервисами.

Стандарт предназначен для подготовки потребительских устройств IoT к защите от наиболее распространенных угроз кибербезопасности.

Содержит набор требований и рекомендаций по безопасности и конфиденциальности, которые производители должны внедрять в свои продукты. Эти рекомендации сформулированы в 13 позициях:

1. Нет универсальных паролей по умолчанию.
2. Должны быть средства управления отчетами об уязвимостях.
3. Обновляемое программное обеспечение.
4. Надежное хранение конфиденциальных параметров безопасности.
5. Безопасный обмен данными
6. Минимальные открытые поверхности атаки (количество способов, с помощью которых хакеры могут проникнуть в устройство или сеть).
7. Обеспечение целостности программного обеспечения.
8. Обеспечение безопасность персональных данных.
9. Устойчивость к сбоям
10. Сбор и анализ телеметрии
11. Простота удаления персональных данных пользователями
12. Простота установки и обслуживания устройств.
13. Проверка входных данных.

Следующим стоит отметить проект OWASP [43]. Open Web Application Security Project (OWASP) — это некоммерческая организация, работающая над повышением безопасности программного обеспечения.

Проект OWASP Internet of Things предназначен для того, чтобы помочь производителям, разработчикам и потребителям лучше понять проблемы безопасности, связанные с Интернетом вещей, и дать возможность пользователям в любом контексте принимать более обоснованные решения в области безопасности при создании, развертывании или оценке технологий IoT. В рамках проекта был подготовлен список IoT Top 10 – основные проблемы с безопасностью IoT. В этот список входят следующие позиции (угрозы).

1. Слабые, угадываемые или жестко закодированные пароли. Устройства IoT со слабыми паролями по умолчанию подвержены кибератакам. Производители устройств IoT должны обращать внимание на настройки пароля при запуске устройства. Либо устройство не позволяет пользователям изменять пароль по умолчанию, либо пользователи предпочитают не менять его, даже если могут.

Кроме того, успешная попытка получить несанкционированный доступ к одному устройству делает другие устройства уязвимыми, поскольку устройства IoT часто используют одни и те же пароли по умолчанию.

2. Небезопасные сетевые сервисы. Сетевые службы, работающие на устройстве, могут представлять угрозу безопасности и целостности системы. При наличии доступа к Интернету они открывают путь для несанкционированного удаленного доступа и утечки данных.

Злоумышленники могут успешно поставить под угрозу безопасность конечной точки IoT, воспользовавшись недостатками модели сетевого взаимодействия.

3. Небезопасные программные интерфейсы экосистемы. Существует несколько интерфейсов, таких как веб-интерфейс, серверный API, облачный и мобильный интерфейс, которые обеспечивают плавное взаимодействие пользователя с устройством. Однако отсутствие надлежащей аутентификации, плохое шифрование и фильтрация данных могут негативно сказаться на безопасности устройств IoT.

4. Отсутствие безопасных механизмов обновления. Невозможность безопасного обновления устройства — четвертая уязвимость в списке.

Отсутствие проверки прошивки, незашифрованная передача данных, отсутствие механизмов защиты от отката, отсутствие уведомлений об обновлениях безопасности — причины скомпрометированной безопасности IoT-устройств.

5. Использование небезопасных или устаревших компонент. Это подразумевает использование стороннего оборудования или программного обеспечения, которое сопряжено с рисками и угрожает безопасности всей системы.

На промышленный интернет вещей (IIoT) особенно сильно влияют системы, которые сложно обновлять и обслуживать. Такие уязвимости могут быть использованы для запуска атаки и нарушения бесперебойной работы устройства.

6. Недостаточная защита конфиденциальности. Устройствам IoT может потребоваться хранить и сохранять конфиденциальную информацию пользователей для правильной работы.

Однако эти устройства часто не обеспечивают безопасного хранения, что приводит к утечке важных данных при взломе киберпреступниками.

Помимо устройств атакам подвержены и базы данных производителя. Зашифрованный трафик по-прежнему подвержен угрозам, поскольку были случаи, когда пассивные наблюдатели также могли извлекать информацию.

7. Небезопасная передача и хранение данных. Отсутствие шифрования при обработке

конфиденциальных данных во время передачи, обработки или в состоянии покоя дает хакерам возможность украсть и раскрыть данные.

Шифрование необходимо везде, где речь идет о передаче данных.

8. Отсутствие управления устройствами. Это относится к невозможности эффективно защитить все устройства в сети.

Незащищенное устройство подвергает систему многочисленным угрозам. Независимо от количества задействованных устройств или их размера, каждое из них должно быть защищено от утечки данных.

9. Небезопасные настройки по умолчанию. Существующие уязвимости в настройках по умолчанию подвергают систему множеству проблем с безопасностью. Это могут быть фиксированные пароли, невозможность следить за обновлениями безопасности и наличие устаревших компонент.

10. Отсутствие физической защиты. Отсутствие физической защиты может легко помочь пользователям со злым умыслом получить удаленный контроль над системой. Если не удалить порты отладки на плате, например, система может подвергнуться атакам из-за отсутствия физической защиты.

V Заключение

В этой статье мы остановились на основнях проблемах кибербезопасности систем Интернета Вещей. Основные проблемы здесь связаны с тем, что IoT системы – это интеграция множества технологий. В любой реализации, как правило, присутствует и множество различных коммуникационных решений, так и множество оконечных устройств с самыми разными характеристиками. Также необходимо учитывать тот факт, что в большинстве проектов полный контроль за оконечными устройствами (сенсорами) может быть невозможным.

Мы продолжим рассмотрение вопросов кибербезопасности IoT, CPS и цифровых двойников в последующих публикациях.

Благодарности

Мы благодарны сотрудникам кафедры Информационной безопасности факультета Вычислительной математики и кибернетики МГУ имени М.В. Ломоносова за ценные обсуждения данной работы. Также хотелось бы отметить работы В.П. Куприяновского и его многочисленных соавторов, которые описывали различные практические аспекты применения систем Интернета Вещей и послужили стимулом для написания данной статьи [44,45,46].

Библиография

[1] Магистратура ПОВС https://cs.msu.ru/news/3368 Retrieved: Dec, 2022

[2] Namiot, Dmitry, Manfred Sneps-Sneppe Ventspils, and Yousef Ibrahim Daradkeh. "On internet of things education." 2017 20th conference of open innovations association (FRUCT). IEEE, 2017.

[3] Namiot, Dmitry, and Manfred Sneps-Sneppe. "On internet of things and big data in university courses." International Journal of Embedded and Real-Time Communication Systems (IJERTCS) 8.1 (2017): 18-30.

[4] Lebed, Sergey. "Инновационные технологии в сфере кибербезопасности." Современные информационные технологии и ИТ-образование [Онлайн], 18.2 (2022): 383-390.

[5] What is cybersecurity https://www.microsoft.com/ru-ru/security/business/security-101/what-is-cybersecurity Retrieved: Dec, 2022

[6] Computer Security https://en.wikipedia.org/wiki/Computer_security Retrieved: Dec, 2022

[7] What is cyber-security https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security Retrieved: Dec, 2022

[8] What is cyber security https://www.sap.com/cis/insights/what-is-cybersecurity.html Retrieved: Dec, 2022

[9] IoT Cybersecurity https://www.knowledgehut.com/blog/security/Iot-cyber-security Retrieved: Dec, 2022

[10] Fraunhofer IoT Cybersecurity https://www.iis.fraunhofer.de/en/ff/lv/iot-system/tech/cybersecurity.html Retrieved: Dec, 2022

[11] Namiot, Dmitry. "On internet of things and smart cities educational courses." International Journal of Open Information Technologies 4.5 (2016): 26-38.

[12] Boyes, Hugh, et al. "The industrial internet of things (IIoT): An analysis framework." Computers in industry 101 (2018): 1-12.

[13] Akyildiz, Ian F., and Josep Miquel Jornet. "The internet of nano-things." IEEE Wireless Communications 17.6 (2010): 58-63.

[14] Akyildiz, Ian F., and Ahan Kak. "The internet of space things/cubesats." IEEE Network 33.5 (2019): 212-218.

[15] Xia, Tingting, et al. "Maritime internet of things: Challenges and solutions." IEEE Wireless Communications 27.2 (2020): 188-196.

[16] Oceans Internet of Things https://www.media.mit.edu/projects/oceans-internet-of-things/overview/ Retrieved: Dec, 2022

[17] Voas, Jeffrey. "Networks of 'things'." NIST Special Publication 800.183 (2016): 800-183.

[18] Nguyen, Thanh Hai, et al. "Specifying and reasoning about CPS through the lens of the NIST CPS framework." Theory and Practice of Logic Programming (2022): 1-41.

[19] Mahmoud, Magdi S., Mutaz M. Hamdan, and Uthman A. Baroudi. "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges." Neurocomputing 338 (2019): 101-115.

[20] Cyber Physical Systems Security https://www.dhs.gov/science-and-technology/cpssec Retrieved: Dec, 2022

[21] Nazarenko, Artem A., and Ghazanfar Ali Safdar. "Survey on security and privacy issues in cyber physical systems." AIMS Electronics and Electrical Engineering 3.2 (2019): 111-143.

[22] Abosata, Nasr, et al. "Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications." Sensors 21.11 (2021): 3654.

[23] Namiot, Dmitry, and Manfred Sneps-Sneppe. "On internet of things programming models." Distributed Computer and Communication Networks: 19th International Conference, DCCN 2016, Moscow, Russia, November 21-25, 2016, Revised Selected Papers 19. Springer International Publishing, 2016.

[24] Namiot, Dmitry, and Elena Zubareva. "Data-driven Cities." International Journal of Open Information Technologies 4.12 (2016): 79-85.

[25] Пьезодатчик http://digitrode.ru/articles/2761-chto-takoe-pezoelektricheskiy-datchik-kak-on-rabotaet-oblasti-primeneniya.html Retrieved: Dec, 2022

[26] Yang, Ke, et al. "A comprehensive survey on hybrid communication for internet of nano-things in context of body-centric communications." arXiv preprint arXiv:1912.09424 (2019).

[27] Namiot, Dmitry, and Manfred Sneps-Sneppe. "Context-aware data discovery." 2012 16th International Conference on Intelligence in Next Generation Networks. IEEE, 2012.

[28] Kurganova, Nadezhda, et al. "Digital twins' introduction as one of the major directions of industrial digitalization." International Journal of Open Information Technologies 7.5 (2019): 105-115.

[29] Holmes, David, et al. "Digital Twins and Cyber Security–solution or challenge?." 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE, 2021.

[30] NIST IoT principles https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/principles Retrieved: Dec, 2022

[31] Rao, V. Venkateswara, R. Marshal, and K. Gobinath. "The IoT Supply Chain Attack Trends-Vulnerabilities and Preventive Measures." 2021 4th International Conference on Security and Privacy (ISEA-ISAP). IEEE, 2021.
[32] How the IoT Intensifies Software Supply Chain Risks https://www.cyberark.com/resources/blog/how-the-iot-intensifies-software-supply-chain-risks Retrieved: Dec, 2022
[33] Wurm J, Jin Y, Liu Y, et al. (2017) Introduction to Cyber-Physical System Security: A Cross-Layer Perspective. IEEE Transactions on Multi-Scale Computing Systems 3: 215–227.
[34] Puttonen, Juha, et al. "Enhancing security in cloud-based cyber-physical systems." (2016).
[35] Ntalampiras S (2016) Automatic identification of integrity attacks in cyber-physical systems.Expert Syst Appl 58: 164–173.
[36] Altawy R, Youssef AM (2016) Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. IEEE Access 4: 959–979.
[37] Brunner, Michael, et al. "Towards an integrated model for safety and security requirements of cyber-physical systems." 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2017..
[38] Lun, Yuriy Zacchia, et al. "Cyber-physical systems security: a systematic mapping study." arXiv preprint arXiv:1605.09641 (2016).
[39] IoT Threats https://unit42.paloaltonetworks.com/iot-threat-report-2020/ Retrieved: Dec, 2022
[40] Ilyushin, Eugene, Dmitry Namiot, and Ivan Chizhov. "Attacks on machine learning systems-common problems and methods." International Journal of Open Information Technologies 10.3 (2022): 17-22
[41] NISTIR 8259 https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series Retrieved: Dec, 2022
[42] ETSI EN 303 645 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf Retrieved: Dec, 2022
[43] OWASP https://owasp.org/www-project-internet-of-things/ Retrieved: Dec, 2022
[44] Куприяновский, В. П., et al. "Розничная торговля в цифровой экономике." International Journal of Open Information Technologies 4.7 (2016): 1-12.
[45] Куприяновская, Ю. В., et al. "Умный контейнер, умный порт, BIM, Интернет Вещей и блокчейн в цифровой системе мировой торговли." International Journal of Open Information Technologies 6.3 (2018): 49-94.
[46] Николаев, Д. Е., et al. "Цифровая железная дорога-инновационные стандарты и их роль на примере Великобритании." International Journal of Open Information Technologies 4.10 (2016): 55-61.

On cybersecurity of the Internet of Things systems

Dmitry Namiot, Vladimir Sukhomlin

***Abstract*— This article discusses the issues of cybersecurity of the Internet of Things (IoT) systems. Such systems are always an integration of many different technologies. This, naturally, increases the opportunities for attackers to influence both software and hardware subsystems of projects. The multitude of different vendors with their solutions and software update cycles greatly increases the possibility of supply chain attacks. Historically, IoT systems have used and continue to use a wide variety of communication solutions, which complicates data protection in this area. End devices (sensors, actuators) also differ greatly in their capabilities and characteristics, which excludes any unified solutions in this area. Perhaps the only "standard" element of IoT systems is cloud storage, the cybersecurity of which must also be dealt with outside of IoT projects. The IoT cybersecurity work is further complicated by the fact that the term IoT hides a whole family of approaches (architectures) - the industrial Internet of Things, the Internet of nano-things, etc. Possible attacks on IOT systems include confidential data theft, identity theft, infrastructure damage, data corruption, unauthorized surveillance, illegal data modification, and unauthorized use of device capabilities.**

***Keywords*— cyber security, cyber attacks, Internet of Things**

REFERENCES

[1]Magistratura POVS https://cs.msu.ru/news/3368 Retrieved: Dec, 2022
[2]Namiot, Dmitry, Manfred Sneps-Sneppe Ventspils, and Yousef Ibrahim Daradkeh. "On internet of things education." 2017 20th conference of open innovations association (FRUCT). IEEE, 2017.
[3]Namiot, Dmitry, and Manfred Sneps-Sneppe. "On internet of things and big data in university courses." International Journal of Embedded and Real-Time Communication Systems (IJERTCS) 8.1 (2017): 18-30.
[4]Lebed, Sergey. "Innovacionnye tehnologii v sfere kiberbezopasnosti." Sovremennye informacionnye tehnologii i IT-obrazovanie [Onlajn], 18.2 (2022): 383-390.
[5]What is cybersecurity https://www.microsoft.com/ru-ru/security/business/security-101/what-is-cybersecurity Retrieved: Dec, 2022
[6]Computer Security https://en.wikipedia.org/wiki/Computer_security Retrieved: Dec, 2022
[7]What is cyber-security https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security Retrieved: Dec, 2022
[8]What is cyber security https://www.sap.com/cis/insights/what-is-cybersecurity.html Retrieved: Dec, 2022
[9]IoT Cybersecurity https://www.knowledgehut.com/blog/security/Iot-cyber-security Retrieved: Dec, 2022
[10] Fraunhofer IoT Cybersecurity https://www.iis.fraunhofer.de/en/ff/lv/iot-system/tech/cybersecurity.html Retrieved: Dec, 2022
[11] Namiot, Dmitry. "On internet of things and smart cities educational courses." International Journal of Open Information Technologies 4.5 (2016): 26-38.
[12] Boyes, Hugh, et al. "The industrial internet of things (IIoT): An analysis framework." Computers in industry 101 (2018): 1-12.
[13] Akyildiz, Ian F., and Josep Miquel Jornet. "The internet of nano-things." IEEE Wireless Communications 17.6 (2010): 58-63.
[14] Akyildiz, Ian F., and Ahan Kak. "The internet of space things/cubesats." IEEE Network 33.5 (2019): 212-218.
[15] Xia, Tingting, et al. "Maritime internet of things: Challenges and solutions." IEEE Wireless Communications 27.2 (2020): 188-196.
[16] Oceans Internet of Things https://www.media.mit.edu/projects/oceans-internet-of-things/overview/ Retrieved: Dec, 2022
[17] Voas, Jeffrey. "Networks of 'things'." NIST Special Publication 800.183 (2016): 800-183.
[18] Nguyen, Thanh Hai, et al. "Specifying and reasoning about CPS through the lens of the NIST CPS framework." Theory and Practice of Logic Programming (2022): 1-41.
[19] Mahmoud, Magdi S., Mutaz M. Hamdan, and Uthman A. Baroudi. "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges." Neurocomputing 338 (2019): 101-115.
[20] Cyber Physical Systems Security https://www.dhs.gov/science-and-technology/cpssec Retrieved: Dec, 2022
[21] Nazarenko, Artem A., and Ghazanfar Ali Safdar. "Survey on security and privacy issues in cyber physical systems." AIMS Electronics and Electrical Engineering 3.2 (2019): 111-143.
[22] Abosata, Nasr, et al. "Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications." Sensors 21.11 (2021): 3654.
[23] Namiot, Dmitry, and Manfred Sneps-Sneppe. "On internet of things programming models." Distributed Computer and Communication Networks: 19th International Conference, DCCN 2016, Moscow, Russia, November 21-25, 2016, Revised Selected Papers 19. Springer International Publishing, 2016.
[24] Namiot, Dmitry, and Elena Zubareva. "Data-driven Cities." International Journal of Open Information Technologies 4.12 (2016): 79-85.
[25] P'ezodatchik http://digitrode.ru/articles/2761-chto-takoe-pezoelektricheskiy-datchik-kak-on-rabotaet-oblasti-primeneniya.html Retrieved: Dec, 2022
[26] Yang, Ke, et al. "A comprehensive survey on hybrid communication for internet of nano-things in context of body-centric communications." arXiv preprint arXiv:1912.09424 (2019).
[27] Namiot, Dmitry, and Manfred Sneps-Sneppe. "Context-aware data discovery." 2012 16th International Conference on Intelligence in Next Generation Networks. IEEE, 2012.
[28] Kurganova, Nadezhda, et al. "Digital twins' introduction as one of the major directions of industrial digitalization." International Journal of Open Information Technologies 7.5 (2019): 105-115.
[29] Holmes, David, et al. "Digital Twins and Cyber Security–solution or challenge?." 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE, 2021.
[30] NIST IoT principles https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/principles Retrieved: Dec, 2022
[31] Rao, V. Venkateswara, R. Marshal, and K. Gobinath. "The IoT Supply Chain Attack Trends-Vulnerabilities and Preventive Measures." 2021 4th International Conference on Security and Privacy (ISEA-ISAP). IEEE, 2021.
[32] How the IoT Intensifies Software Supply Chain Risks https://www.cyberark.com/resources/blog/how-the-iot-intensifies-software-supply-chain-risks Retrieved: Dec, 2022
[33] Wurm J, Jin Y, Liu Y, et al. (2017) Introduction to Cyber-Physical System Security: A Cross-Layer Perspective. IEEE Transactions on Multi-Scale Computing Systems 3: 215–227.
[34] Puttonen, Juha, et al. "Enhancing security in cloud-based cyber-physical systems." (2016).
[35] Ntalampiras S (2016) Automatic identification of integrity attacks in cyber-physical systems.Expert Syst Appl 58: 164–173.
[36] Altawy R, Youssef AM (2016) Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. IEEE Access 4: 959–979.

[37] Brunner, Michael, et al. "Towards an integrated model for safety and security requirements of cyber-physical systems." 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2017..
[38] Lun, Yuriy Zacchia, et al. "Cyber-physical systems security: a systematic mapping study." arXiv preprint arXiv:1605.09641 (2016).
[39] IoT Threats https://unit42.paloaltonetworks.com/iot-threat-report-2020/ Retrieved: Dec, 2022
[40] Ilyushin, Eugene, Dmitry Namiot, and Ivan Chizhov. "Attacks on machine learning systems-common problems and methods." International Journal of Open Information Technologies 10.3 (2022): 17-22
[41] NISTIR 8259 https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series Retrieved: Dec, 2022
[42] ETSI EN 303 645 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf Retrieved: Dec, 2022
[43] OWASP https://owasp.org/www-project-internet-of-things/ Retrieved: Dec, 2022
[44] Kuprijanovskij, V. P., et al. "Roznichnaja torgovlja v cifrovoj jekonomike." International Journal of Open Information Technologies 4.7 (2016): 1-12.
[45] Kuprijanovskaja, Ju. V., et al. "Umnyj kontejner, umnyj port, BIM, Internet Veshhej i blokchejn v cifrovoj sisteme mirovoj torgovli." International Journal of Open Information Technologies 6.3 (2018): 49-94.
[46] Nikolaev, D. E., et al. "Cifrovaja zheleznaja doroga-innovacionnye standarty i ih rol' na primere Velikobritanii." International Journal of Open Information Technologies 4.10 (2016): 55-61.