Элементы информационной безопасности «интернета вещей»

Назаров Д.М.
Уральский государственный экономический университет, Екатеринбург, Россия
Автор-корреспондент: slup2005@mail.ru

Ключевые слова: Интернет вещей, информационная безопасность, уязвимость, угрозы безопасности.

Abstract: В связи с ярко выраженным ростом потребности пользователей технологии интернет вещей возникла необходимость качественной информационной защиты сети Internet of Thing. В статье рассмотрены наиболее важные вопросы, связанные с информационной безопасностью IoT, названы пути решения выявленных проблем.

Elements of information security of the "Internet of things"

Nazarov D.M.
Ural State University of Economics, Yekaterinburg, Russia
Corresponding author: slup2005@mail.ru

Keywords: Internet of Things, information security, vulnerability, security threats.

Abstract: In connection with the clearly expressed level of the needs of users of the Internet of Things, there is a need for high-quality information protection of the Internet of Thing. The article discusses the most important issues related to IoT information security, identifies ways to identify the identified problems.

В настоящее время большой теоретический и практический интерес представляют вопросы влияния взаимоотношений по типу «машина-машина» на бесперебойность и надежность функционирования систем, обеспечивающих жизнедеятельность социума.

Глобальные информационные сети активно развиваются в направлении, обеспечивающем организацию связи физических и виртуальных предметов на основе ИКТ в целях предоставления обществу инновационных услуг, к примеру, в сфере покупок (бесконтактная оплата), управления транспортными средствами посредством «умных» телефонов, энергопотребления (снижение объемов вследствие дистанционного наблюдения с помощью датчиков и видеокамер). Это явление получило название «Internet вещей».

Ключевые особенности «Internet вещей» заключаются в следующем.

1.Объединенные в гигантской вычислительной сети физические предметы могут контактировать друг с другом и с внешним миром.

2.В сети IoT взаимодействуют компьютеры, смартфоны, различные мощные вычислительные устройства и практически любые вещи.

3. Internet of Thing в значительной мере облегчает жизнь человека, не требуя от него вмешательства в функционирование совмещенных между собой устройств, осуществляющих контроль за окружающим миром с помощью цифровых средств [2, с. 341].

4.Основной задачей структуры является совершенствование образа жизни людей, повышение ее качества за счет обеспечения сплоченности посредством искусственного интеллекта во взаимодействии всех членов социума и власти.

5.Сеть предоставляет широкие перспективы:

- в аграрном секторе: относительное состояние почвы можно преодолеть, используя показания датчиков о влажности, температуре плодородного слоя земли, питании растений;

- в промышленности: сокращение числа планового осмотра оборудования за счет использования показаний датчиков [1, с.157];

- в логистике товаров: отслеживание посылки на всем ее пути позволяет упростить ее доставку от производителя в магазин или из магазина покупателю;

- в строительстве «умных домов»: обеспечение сбережения ресурсов воды, электроэнергии, газа посредством установки «умных» счетчиков; управление безопасностью жилища; программирование его функций под потребности конкретного пользователя;

- в медицине: работа собирающих и передающих в ИТ-базу данные для последующего анализа девайсов; мониторинг текущего состояния пациента, автоматическое предупреждение специалистов об изменениях; снижение применения медицинского оборудования энергоемких характеристик, сокращение расходов на операции; контроль за здоровьем человека посредством регулярного мониторинга физических показаний с помощью устройств, носимых на руке, «умной» одежды и обуви;

- в торговле: «точечная» работа с каждым «включенным» в сеть покупателем при поиске нужного товара; анализ объемов продаж, автоматическое повышение или понижение стоимости в целях обеспечения максимальных объемов реализации, исключения переизбытка продукции;

- в криминалистике: контроль заключенных под домашний арест преступников с помощью биометрических чипов;

- в охране окружающей среды: мониторинг популяций животных посредством обнаружения их на поверхности Земли по исходящему от размещенного на особи электронного устройства радиосигнала;

- на транспорте: ИИ сможет самостоятельно оценить ситуацию на проезжей части, не привлекая человека, самостоятельно построить и скорректировать маршрут движения.

Одной из основных проблем IoT на сегодняшний день является обеспечение интернет-безопасности этой сети. Обусловлена проблема следующими факторами: стремительно меняющейся ситуацией в отрасли; стремлением многочисленных лиц и организаций завладеть влиянием на сеть, установить свои порядки и законы; нереальными прогнозами. Особую роль играет при этом техническая уязвимость, которую составляют: не обязательно явное, либо имеющее обратную связь активное влияние субъекта на объект; негативное воздействие совокупности условий и факторов, представляющих собой опасность для информационной безопасности; намеренные злоумышленные действие, направленные на нарушение доступности, целостности, конфиденциальности данных.

Зная проблемы и недочеты конфигурации в прикладном или управляющем программном обеспечении системы, лицо, заранее замыслившее противоправное действие, может овладеть устройством, внедрить в него вредоносный элемент, изменить программу [3, с. 12].

Существенный вред компьютерным системам могут нанести угрозы природного свойства – землетрясения, пожары, наводнения. Для минимизации их негативного влияния лучше всего использовать резервное копирование.

Огромный злонамеренный ущерб IoT возможен со стороны людей, как имеющих разрешенный доступ к сети, так и работающих вне ее пределов. Это могут быть неопытные хакеры, применяющие легко доступные инструменты взлома, а также специалисты, хорошо знающие уязвимости системы, предвидящие ее реакцию на применение

конкретных кодов и скриптов. В новое поколение девайсов Internet of Thing уже встроены новые угрозы информационной безопасности, обеспечивающих доступ атакам производителей.

Злоумышленные действия, направленные на нарушение доступности, целостности, конфиденциальности данных, зачастую предназначены для удовлетворения личных амбиций атакующего или на получение вознаграждения. У таких действий могут быть самые разные формы: активное нападение в сети в целях выявления возможности просмотра интернет - провайдером пакета данных, чтобы увидеть просматриваемые сайты и используемые веб – приложения; пассивные нападения на сеть с целью поиска доступной для похищения информации; ближние нападения с веб-сайтов по инициативе компьютеров; использование лиц, имеющих доступ к данным, недоступным широким массам.

Наиболее часто встречаются следующие типы хакерских нападений:

А. Нарушение работы аппаратных элементов. Связано с тем, что большинство устройств Intrnet вещей работает в наружной среде, легко может быть подвержено негативному физическому воздействию.

Б. Нападение в разведывательных целях, для незаконного обнаружения слабых мест в функционировании систем и служб.

В. Обеспечение недоступности пользователей к машине или сетевому ресурсу, который впоследствии очень трудно восстановить по причине низких возможностей памяти, ограниченных вычислительных возможностей.

Г. Доступ к физическому или подключенному IP – устройству неавторизованных субъектов в целях

- перехвата, подмены сообщений при сохранении анонимности доступа хакера к каналу обмена информацией корреспондентами;

- компрометации канала посредством нарушения протокола передачи искажением или изменением информации;

- использования доступа к сайту, полученного от пользователя, не владеющего основами сетевой безопасности, мошенническим путем на поддельной странице [5, с. 39].

Д. Нарушение неприкосновенности личной жизни, выражающееся в

- интеллектуальном анализе информации, позволяющем выявить факты, не подлежащие обнародованию в базах данных;

- получение секретных сведений о частных лицах или организациях путем взлома, применения вредоносного программного обеспечения;

- несанкционированное прослушивание разговоров пользователей;

- отслеживание местоположения, передвижения пользователей, желающих остаться анонимными, посредством UID;

- нападение путем дублирования пароля пользователя путем угадывания комбинации букв и цифр, проверки всех возможных комбинаций посредством специального инструментария.

Е. Неправомерное использование сети в целях получения материального дохода путем кражи результатов творческого труда, персональных данных, комплекса ассоциаций и представлений о продукте или услуге.

Ж. Нападение на управление технологическим режимом работы, эксплуатационное состояние аппаратов: отказ в обслуживании,

следствием которого является прекращение работы системы; управление структурой с помощью троянов или вирусов.

На сегодняшний день в мире нет ни одной действительно безопасной системы Internet of Thing. Основными причинами этого являются: желание производителя минимизировать стоимость своего продукта; отсутствие необходимых стандартов и рекомендаций по обеспечению информационной безопасности сети; невозможность авторизации и аутентификации многих применяемых в системе компонентов в глобальную сеть [4, с. 280].

Необходима систематическая и целенаправленная работа по созданию эффективной информационной безопасности Internet вещей, включающая:

- мониторинг уязвимости устройств на этапе их производства;

- применение современных стандартов разработки безопасных приложений в процессе создания программного обеспечения;

- создание возможностей и условий для обновления ПО;

- минимизацию уязвимости аппаратно-зависимого кода посредством управления логистикой начиная от стадии производства, заканчивая стадией установки оборудования на объекте;

- предотвращение физического захвата структур, принимающих, обрабатывающих информацию определенного типа, формирующих ощущения;

- повышение уровня защиты безопасности развернутых в среде, не обслуживаемой людьми, различных узлов восприятия сенсорной сети;

- профилактику проблем сенсора (захват узла шлюза, утечка информации, нарушение целостности данных, истощение обеспечения

энергией, перегрузки, отказ в обслуживании, установка нелегитимных устройств, несанкционированное копирование узла);

- защиту сетей связи от незаконного доступа, перехвата сведений, нарушения секретности, вирусов, сетевых червей, использования уязвимостей в ПО в целях нападения на вычислительную систему, применения набора программных средств для маскировки процессов, файлов, драйверов, а также происходящих в системе событий и ее параметров;

- исключение проблемы аутентификации, следствием которой может стать информационные атаки на сеть;

- устранение уязвимостей ПО, вызванных ошибками разработчиков и ядра программы, неполной обработкой исключений, применением кода, имеющего слабую защиту, недостаточной обработкой массивов, которые могут переполнить хакеры, ошибками в обработке Big Data и БД, недолжной индексацией или неправильными запросами БД, нарушениями в распределенной работе приложений, виртуальных платформ, облаков;

- создание для серверов в процессе проектирования ПО имитаторов внешней среды;

- избежание значительных расхождений между эмулятором и прибором в ходе энергообеспечения, производительности процессора, памяти;

- комплексное тестирование: нагрузки, производительность, взаимодействие модулей;

- исключение доступа к данным в результате применения сочетания клавиш или осуществления определенных действий.

Применение Internet вещей во многих сферах пока существенно ограничено проблемами информационной безопасности. Однако

тщательный анализ ситуации, достижений в этой области и предложений специалистов позволят решить накопившиеся вопросы, способствовать дальнейшему внедрению данной технологии в практику.

Список литературы

1. Буянов Б.Я., Верба В.А. Мультиагентные модели сложных социо - технических систем // В сборнике: Системный анализ в проектировании и управлении. Сборник научных трудов XX Международной научно-практической конференции. 2016. С. 155-158.
2. Калинин А. С. Интернет вещей. Принципы, технологии, перспективы развития/ А. С. Калинин. – Текст: непосредственный // Молодой ученый. – 2019 – № 2 (240. – С. 341 – 342.
3. Кожевникова И. С. Тенденции безопасности интернет-вещей / И. С. Кожевникова. – Текст: непосредственный // Молодой ученый. – 2017. - № 13 (147). – С. 11-14.
4. Шиков С. А., Ивлиев С. Н. Интернет вещей: новые угрозы информационной безопасности // Мат-лы XX науч.-практ. конф. молодых ученых, аспирантов и студентов Национального исследовательского Мордовского государственного университета им. Н. П. Огарева : в 3 ч. Саранск, 2016. С. 278–283.
5. Шиков С. А. Проблемы информационной безопасности интернет вещей // Вестник Мордовского университета. 2017. Т. 27, № 1. С. 27–40