«ИНТЕРНЕТ ВЕЩЕЙ»: УПРАВЛЕНИЕ РИСКАМИ

ГИБ СОРЕБО (GIB SOREBO)

В настоящее время «Интернет вещей» (Internet of Things, IoT) стремительно развивается и все больше устройств имеет свой собственный выход в Интернет. Для защиты таких устройств, систем и самих пользователей необходимо, наравне с принятием мер в области кибербезопасности, разрабатывать умные индустриальные сети. В статье представлены рекомендации по уменьшению рисков, связанных с использованием «Интернета вещей».

Современные средства массовой информации часто используют термин «Интернет вещей» и его различные вариации. Очень часто можно увидеть рассказы о подключенных к Интернету автомобилях, системах домашней автоматизации, интеллектуальных приборах учета и носимых непосредственно на теле человека устройствах, имеющих связь с компьютерными сетями.

При таком большом интересе к этой теме можно было бы подумать, что это новейшее изобретение, но на самом деле связь машины с машиной, взаимодействующих с физическим миром с помощью коммуникационных сетей, — это пример типичного интерфейса. Менее яркие устройства в этом ряду, такие как промышленные системы управления, от которых зависит работа электрических сетей, нефтепроводов и самих производств, известны уже несколько десятилетий. Подобно тому как облачные вычисления частично обязаны своим происхождением изменению концепции обмена информацией между большими ЭВМ 1960-х и 1970-х гг., такое понятие, как «Интернет вещей», также претерпело своеобразный ребрендинг. Варианты его использования продолжают расширяться: от тривиальных и узконаправленных приложений до масштабных и жизненно важных, критических решений в области здравоохранения и транспорта.

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ «ИНТЕРНЕТ ВЕЩЕЙ»

Термин «Интернет вещей», вместо того чтобы родиться в ходе многолетнего труда по его стандартизации, получил свое название и попал в наш обиход из-за ажиотажа, поднятого в СМИ. Следовательно, это понятие относится к категории «Узнаю́, когда вижу» (англ. «I know it when I see it»)[1], то есть воспринимается как факт. На самом базовом уровне это понятие означает подключение устройства к сети с помощью встраиваемых устройств. Кроме того, оно обычно включает в себя некую связь с физическим миром, например измерение температуры, артериального давления или вибрации дорожного покрытия. По сути, имеется в виду подключение к сети современных устройств, которые в традиционном понимании компьютерами не считаются. Однако почти каждое применение технологии «Интернета вещей» включает в себя также использование некоторых компьютерных технологий. Например, эти небольшие встраиваемые устройства, как правило, сообщают о своем статусе и получают команды управления от рабочей станции, сервера, ноутбука или смартфона. Типичная архитектура «Интернета вещей» показана на рис. 1.

Лучше всего идентифицировать устройства из категории «Интернет вещей» как наименьшие в ряду небольших устройств, но при этом

[1] I know it when I see it – американское крылатое выражение, обозначающее готовность говорящего классифицировать наблюдаемое явление при отсутствии его точного определения.

более экосистемные с точки зрения их поведения внутри сети, что требует наличия нескольких компонентов для их корректной работы. Компоненты поддержки, т. е. обычные компьютерные устройства, должны быть настроены на работу в режиме реального времени, а уже большие данные (big data) часто ассоциируются с устройствами из категории «Интернет вещей». Для функционирования в среде «Интернета вещей» компьютерные сети должны быть повсеместными и, кроме того, оптимизированными для обработки большого объема данных и высокой скорости их передачи.

Ключевые компоненты, которые взаимодействуют с физическим миром, обычно включают в себя датчики для измерения таких параметров, как температура, скорость ветра, или просто определяют факт присутствия какого-нибудь объекта. Кроме того, такие компоненты часто содержат в себе и исполнительные элементы — актуаторы, которые инициируют некоторые заданные действия (например, беспилотное вождение автомобиля, выключение питания или введение инсулина). Компоненты поддержки часто размещены там же, где они определяют действия, но для больших автономных устройств принятие некоторых решений может выполняться независимо, лишь на основе данных, которые поступают на вход устройства.

Хотя сам по себе «Интернет вещей» все еще является относительно новой концепцией, его основные компоненты находили широкое применение в промышленных сетях на протяжении многих десятилетий, и этот факт предсказывает некоторые потенциальные риски, с которыми уже реально сталкиваются. В отличие от традиционных компонентов информационных технологий, они являются более уязвимыми. Причина кроется в том, что многие промышленные сети никогда не были предназначены для подключения к общим сетям, которые связаны с враждебной для них средой Интернета, и считали реальной угрозой только физическое нападение.

Помимо проблем межсетевого взаимодействия, могут возникнуть трудности и с основными промышленными устройствами, такими как программируемые логические контроллеры (ПЛК, PLC): они имеют базовые коммуникационные протоколы, которые могут «падать», если ПЛК получают какие-либо непредусмотренные данные. Кроме того, ПЛК были предназначены лишь для обработки команд от того, кто их посылал, чаще всего без какой-либо аутентификации.

Даже с использованием самых лучших сетевых протоколов и более строгого контроля кибербезопасности, природа многих из этих устройств подразумевает, что робастное, более устойчивое к воздействиям различных факторов управление, которое характерно для типичных рабочих станций, ноутбуков, серверов или даже смартфонов, вряд ли будет реализовано в конструкции устройств «Интернета вещей». Кроме того, эти устройства сильно различаются по применению в приложениях, своему размещению и архитектуре. Из-за связи с другими сетевыми компонентами устройства из категории «Интернет вещей» предрасположены к распространению вирусов, а также могут служить платформой для хакерской атаки на другие участки сетевой системы. Масштабы сети делают устройства «Интернета вещей» весьма перспективными, но одновременно являются для них источником наибольшего риска.

ПОДХОДЫ К УСТРАНЕНИЮ РИСКОВ

Распространение новых устройств и непрерывный рост соответствующих угроз — решающий фактор для того, чтобы попытаться понять виды будущих угроз и разработать решения по их управлению. Традиционная стратегия управления рисками указывает сразу на множество самых разных способов уменьшения риска и зависит от того, как используются новые устройства.

Другой подход — это сосредоточиться на тех рисках, которые отличаются наиболее разрушительными последствиями. В то время как само по себе воздействие, безусловно, важно, первое, что надо оценить, это то, что именно данное устройство из категории «Интернет

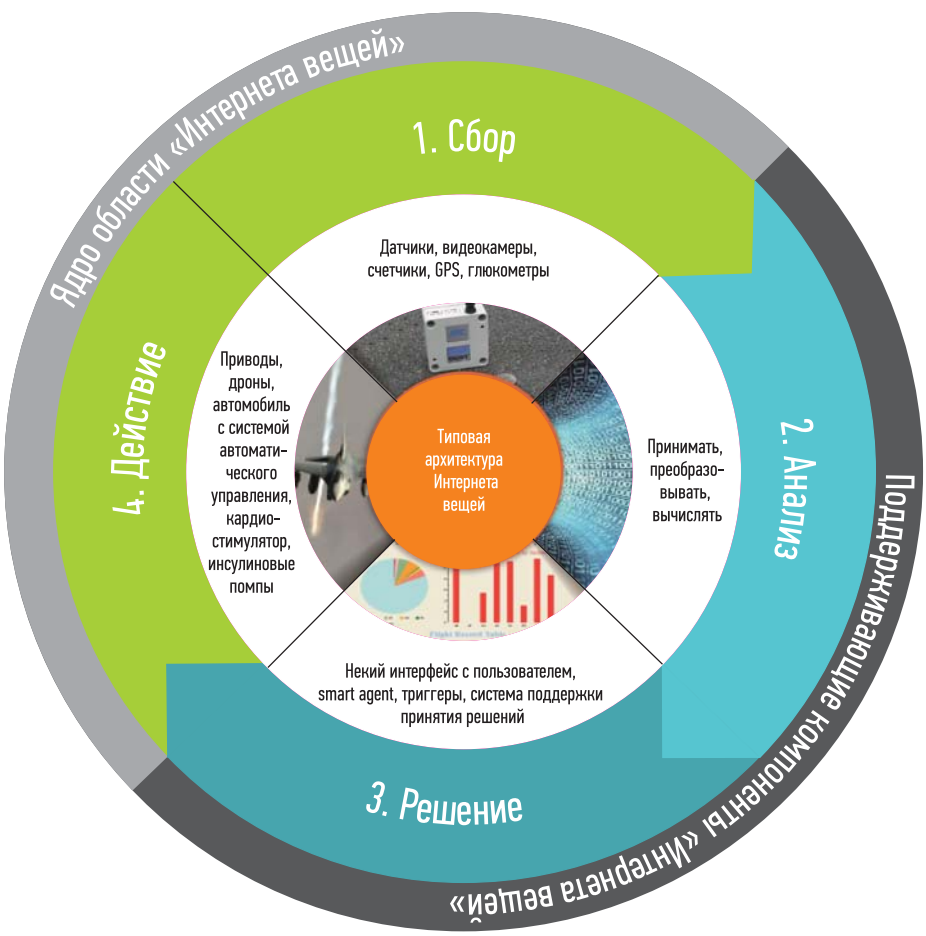

РИС. 1. ▼ Взаимодействие программного обеспечения «Интернета вещей» с подключенными устройствами

вещей» предназначено делать. Чтобы использовать результаты анализа прецедентов, необходимо также учитывать и цель самого бизнеса. Если устройство впоследствии будет эксплуатироваться иначе, то команде по анализу рисков нужно будет выполнить анализ еще раз.

Угрозы для «Интернета вещей» — реальные факты

- Примерно два десятилетия назад один недовольный компанией работник использовал удаленный доступ к сети и сбросил канализационные стоки.
- В 2007 г. исследователи показали, что электрогенератор может быть дистанционно выведен из строя путем его быстрого включения-выключения с помощью автоматического выключателя.
- В 2014 г. хакеры взломали промышленную сеть немецкого сталелитейного завода и заблокировали остановку доменной печи.
- Что касается более современных устройств из категории «Интернет вещей», то один исследователь взломал свою инсулиновую помпу, кому-то удалось получить доступ к смарт-счетчикам, а в общественно-политическом телешоу «60 минут» ученые Агентства по перспективным оборонным научно-исследовательским разработкам США (англ. Defense Advanced Research Projects Agency, DARPA) дистанционно управляли автомобильными тормозами.

Эти примеры показывают, насколько важно обеспечить надлежащую защиту миллиардов устройств из категории «Интернет вещей».

ПОСТРОЕНИЕ МОДЕЛИ ДЕЙСТВИЯ ФАКТОРОВ РИСКА

Чтобы оценить риски «Интернета вещей», необходимо определить, как будут использоваться устройства и поддерживающая их инфраструктура. Причем в этом вопросе нужно уделить внимание не столько техническому описанию, сколько бизнес-процессам и ожидаемым от них результатам. В отличие от планирования бюджетных расходов, которое направлено на общую цель, но не касается конкретных способов ее достижения, в анализе рисков необходимо продумать точные и подробные сценарии действий. Для этого нужны самые разнообразные данные: контактируют ли люди с этими устройствами непосредственно, т. е. физически (например, устройства могут осуществлять контроль состояния здоровья пациента), самостоятельное (без участия человека) ли это управление транспортными средствами или это компьютерная система управления банка. Кроме того, важно знать, будут ли устройства взаимодействовать с уже существующими технологиями, а также необходимо иметь полную информацию о существующей инфраструктуре, которая к моменту внедрения должна быть уже готова.

Нужно также использовать разработанное решение, учитывая его инвариантность, то есть потенциальные возможности. Например, подключение интеллектуального счетчика электроэнергии, который является лишь прибором учета и отправки отчетов по использованию энергии, может стать причиной очень серьезных последствий, потому что он поддерживает возможность удаленного отключения электропитания.

ПРИОРИТЕТНОСТЬ ПО УЯЗВИМОСТИ

Идентификация уязвимостей обычно начинается с изучения всех интерфейсов и потенциальных направлений для атак, причем как программных, так и физических. Поскольку часто их число весьма велико, то целесообразно сосредоточить внимание на наиболее вероятных и разрушительных угрозах. Например, вряд ли какое-либо стороннее лицо заинтересовано в сборе общей информации о чьем-то энергопотреблении, если это, конечно, не энергопотребление некоей важной военной базы.

Необходимо также учитывать то, что рассматриваемая задача выходит за рамки стандартного анализа риска, потому что «Интернет вещей» не будет стоять на месте. Такие технологии, как датчики дорожного движения и интеллектуальные средства учета, не предназначены для частой замены, поэтому для обновления их программного обеспечения и внесения изменений, связанных с сетью, нужно будет использовать стационарно установленное оборудование. Это означает, что такие факторы, как возможность модернизации и расширения, которые не были основными с точки зрения кибербезопасности, становятся важной проблемой для «Интернета вещей». Следовательно, будущие риски и варианты ненадлежащего использования устройств «Интернета вещей» должны быть четко определены.

Аналогичным образом должны быть рассмотрены и учтены последствия, связанные с расширением сети. Например, безопасность движения нескольких самоуправляемых беспилотных автомобилей обеспечивает один человек, который при управлении этим процессом в ручном режиме может допустить случайную оплошность. Когда количество автомобилей вырастет до нескольких тысяч, то, даже если нанять больше людей, система обеспечения безопасности не будет работать, так как число данных и направлений для кибератак растет экспоненциально. В этом случае единственным решением является большая степень масштабности и автоматизации кибербезопасности, которая уже затем оказывается под надзором и контролем со стороны людей. Возможный вред от других заинтересованных в его нанесении сторон или факторы внешнего порядка тоже должны быть частью этого уравнения. На рис. 2 представлен результат такого подхода, экстраполяция того риска, который несет в себе устройство «Интернета вещей» или совокупность таких устройств.

СМЯГЧЕНИЕ РИСКОВ

Бесспорно, что само по себе выявление рисков является лишь частью проблемы. Из-за того, что потенциальные последствия от взлома не всегда в достаточной и полной мере

Шесть шагов по снижению риска для «Интернета вещей»

1. Владельцы устройств из категории «Интернет вещей» должны определить текущую имплементацию таких устройств, то есть места, где они уже находятся или будут находиться. Это могут быть, например, системы управления отоплением здания и кондиционирования воздуха или управление механизмами, используемыми для движения лифтов.
2. Необходимо определить политику или процедуру обеспечения безопасности, связанную с использованием «Интернета вещей». Если ее нет, то компании должны по крайней мере разработать документ, определяющий некоторые элементы управления высокого уровня и указывающий все, что должно в обязательном порядке находиться на своих местах (как, например, замок на машинном отделении лифта).
3. В течение трех месяцев владельцы устройства должны применить модель управления рисками, описанную выше, и результаты такой проверки должны быть рассмотрены на уровне руководства.
4. Должны быть определены шаги по смягчению последствий и связанные с ними расходы.
5. В течение шести месяцев следует определить риски «Интернета вещей», которые не контролируются, но оказывают влияние.
6. Для того чтобы стимулировать развитие стандартов безопасности для устройств, нужно участвовать в промышленных группах по разработке таких стандартов.

оценены (например, в «умных» домах), становится ясно, что для адекватного уменьшения уязвимости потребуется достаточно большая работа. Пожалуй, наиболее важным фактором является то, что устройство должно быть идентифицировано для определенной цели. Например, сетевой беспилотный летательный аппарат — дрон — может быть продан только для определенного и одобренного использования, такого как нужды сельского хозяйства или обслуживание буровых вышек в незаселенных местах.

Для физических и юридических лиц, приобретающих устройства категории «Интернета вещей», смягчение рисков начинается с четко определенного механизма возможного развития прецедентов. Для сферы бизнеса это означает политику наличия специальных разрешений на использование устройства в конкретной среде или для определенной цели. Там, где обрабатывается персональная информация, должна быть выработана четкая политика сбора данных и их хранения. Это, в соответствующих случаях, касается и более крупных систем, участвующих в этом процессе.

Наконец, владельцы устройств должны понимать, что выполнения лишь одной разовой ревизии для обеспечения безопасности недостаточно. Они должны проводить текущие анализы по мере того, как расширяется использование устройства и модифицируются различные серверные инфраструктуры, которые с ним взаимодействуют. Модель управления рисками необходимо пересматривать с каждым изменением границ действия системы. ⬣

РИС. 2. ▼ Формула риска для «Интернета вещей»