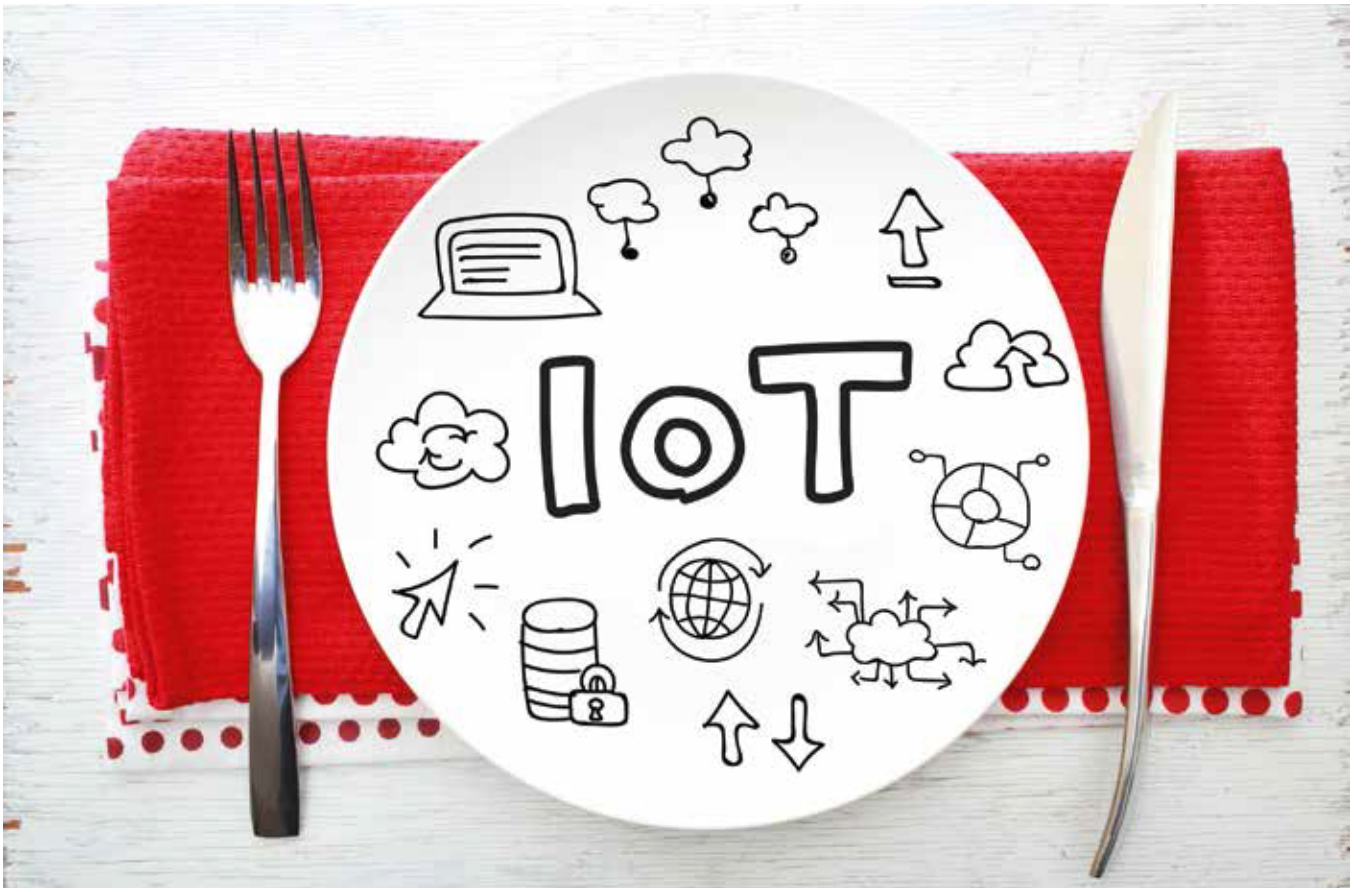


«Интернет вещей» на службе безопасности

К 2020 году количество подключенных устройств вырастет почти на 50% — до 50 млрд единиц самого различного оборудования. Большая часть из них непосредственно касается рынка технических средств безопасности (ТСБ) — камеры видеонаблюдения, системы контроля доступа, охранной сигнализации и даже пожарные датчики. Компании рынка ТСБ из рейтинга топ-50 за 2015 год, подготовленного журналом a&s International, рассказывают о своем видении будущего отрасли на фоне главного интернет-тренда.

Текст: Уильям Пао, a&s International

Интернет вещей (англ. Internet of Things, IoT) уже ни для кого не является феноменом, поскольку все большее количество устройств подключается ко всемирной Сети и генерирует необходимую пользователям информацию. Рынок систем безопасности не остался в стороне от этого тренда и также начал приспосабливаться к IoT, выпуская адаптированные под современные требования продукты и решения, которые становятся «дружественными» не только для интернета, но и для самого пользователя.

Термин «интернет вещей» был впервые предложен британским предпринимателем Кевином Эштоном в 1999 году, чтобы описать понятие глобальной сети RFID-устройств. Сегодня сетевое видеонаблюдение стало действительностью, поскольку IoT уже повсеместно применяется в «безопасных городах», «интеллектуаль-

ных» зданиях, «умных» домах. По различным оценкам, в настоящий момент во всем мире насчитывается около 25 млрд подключенных устройств при численности населения планеты 7,2 млрд человек. К 2020 году, как ожидается, количество умных гаджетов вырастет в два раза — до 50 млрд.

БЕЗОПАСНОСТЬ И IoT

Что означает этот тренд для рынка и служб безопасности? Для начала стоит отметить, что физическая безопасность уже неразрывно связана с IoT — в особенности после того, как сфера безопасности затронула IP-протокол, который позволяет интегрировать все устройства в единое целое при помощи интернета. Преимущества интеграции очевидны — повышение эффективности работы оборудования, повышение, в прямом смысле, уровня интеллекта всей системы и опыта пользователя.

При объединении в общую систему устройств видеонаблюдения, контроля доступа, охранной сигнализации и других также увеличивается уровень безопасности объекта. Интегрированная система делает помещение менее уязвимым для несанкционированных вторжений и различных угроз. «Традиционные системы контроля доступа легко могут быть взломаны при помощи поддельных карт с интегральной микросхемой или поддельных отпечатков пальцев. Поэтому сегодня производители активно работают над объединением видеонаблюдения, СКУД, сигнализации и прочих систем для того, чтобы получать достоверную, полную и объективную информацию о ситуации на объекте», — считает Аллен Лю, менеджер по продукту компании Dahua Technology.

Аллен Лю,
менеджер по продукту,
Dahua Technology

Продукция рынка безопасности сегодня является частью IoT. Видеонаблюдение, мобильные устройства, системы контроля доступа, охранной сигнализации — все современные системы связаны с IoT, который окружает нас в повседневной жизни.

Похожую мысль высказывает Мартин Грен, соучредитель Axis Communications: «Если использовать только камеры видеонаблюдения, то возможности по обеспечению безопасности крайне ограничены. Например, нет возможности общаться с человеком. Если добавить к системе видеонаблюдения рупорный громкоговоритель, то можно сразу предупредить непосредственно нарушителя, который находится в запрещенной зоне или слоняется без дела, если это сотрудник предприятия. В этом случае среагировать на ту или иную ситуацию можно при помощи одной системы — нет необходимости переключаться между разным оборудованием и интерфейсами». По словам Мартина Грена, подобная реализация интеграции является эффективным вариантом обеспечения безопасности предприятия, так как, согласно исследованиям Axis, около 74% людей прекращают противоправные действия, если узнают, что за ними наблюдают.

Ларс Норденлунд Фриис,
вице-президент по развитию и рискованным начинаниям,
Milestone Systems

Охранные системы будут привязаны к IoT при помощи датчиков. Таким же образом подключены телефоны, автомобили, холодильники и другие привычные всем вещи — устройства являются источником информации для датчиков, которые проводят мониторинг поступающих данных и затем передают пользователю. Соединительным звеном между отдельными технологиями выступают подключенные компоненты системы, которые работают как единое целое.

ВЫСОКИЙ IQ

Кроме вопросов обеспечения безопасности людей и имущества, IoT также позволяет решать задачи по бизнес-анализу. Например, в сегменте розничной торговли, когда камеры видеонаблюдения не только предотвращают кражи, но и изучают поведение покупателей, — какими проходами в магазине люди пользуются чаще всего, как они реагируют на определенные места и продукты. Вся эта информация может быть использована для принятия определенных маркетинговых решений и увеличения объемов продаж.

Виллем Райан,
менеджер по маркетингу продукции,
Avigilon

Для достижения максимального успеха IoT нужно использовать не только для увеличения объемов получаемых данных. Система должна обеспечивать преобразование этих данных в конкретную информацию, обеспечивать пользователю ее понимание — именно это и является самым ценным в IoT для бизнеса. Для этого требуются современные оборудование и программное обеспечение.

Все чаще анализ получаемых данных выполняется в облаке. Многие компании уже предоставляют в качестве услуги сетевую передачу данных от локальных до центральных серверов.

«В этом случае у пользователя появляются практически безграничные возможности для анализа данных и, как результат, для принятия решений на их основе. В этом процессе могут использоваться как частные, так и публичные облака, к которым подключаются все типы интеллектуальных датчиков», — считает Ларс Норденлунд Фриис.

МАКСИМАЛЬНЫЙ КОМФОРТ

При помощи IoT также можно сделать дома и целые города не только умными и безопасными, но и комфортными — например, используя интеграцию СКУД и системы управления зданием. «При помощи таких технологий сегодня можно контролировать температуру в зданиях или освещение. Скажем, когда вы заходите в помещение — еще на этапе прохождения СКУД, — свет в вашей

компаний планируют внедрение IoT в ближайшие три года*

*Компания Cisco, по результатам опроса участников форума, посвященного «интернету вещей», который состоялся в Чикаго в 2014 году.

квартире или на вашем рабочем месте автоматически включается, термостат сам выстраивает тот уровень температуры, который комфортен именно вам», — приводит пример Чул Хонг Парк, менеджер команды по разработкам компании Commax.

Роб Мартенс,
директор направления по связующим платформам, Allegion

IoT ориентирован на работу с самыми разными устройствами, чтобы максимально повысить уровень комфорта для пользователей. Наличие IoT-решений в системах безопасности также способствует эволюции самих устройств и услуг по обеспечению безопасности.

ТСБ + IoT = ...

На фоне распространения умных устройств сферы безопасности и IoT становятся все более взаимосвязанными. Они осуществили некоторые изменения в работе, чтобы соответствовать новому тренду. Например, компании-производители систем безопасности расширяют линейки IP-продукции, чтобы, в том числе, увеличить и количество дополнительных функций, которые могут предлагать их устройства пользователю.

Кевин Ванг,
директор бизнес-центра по развитию систем, Everspring Industry

Компания Everspring в настоящее время сменила свою позицию с производителя IoT-устройств на поставщика современных решений. Мы предлагаем комплексные решения для самых разных групп потребителей и поставщиков систем, в основе каждого предложения — продукты на основе IP-технологий. Для обеспечения работоспособности всех систем компания своими силами создала специальный облачный сервер и разработала соответствующие приложения. Прежде всего мы делаем акцент на простоте установки и использования для клиентов, высоком уровне надежности для профессиональных монтажников и возможности дистанционного управления для поставщиков услуг.

Чул Хонг Парк,
менеджер команды по разработкам, Commax

Наша цель — разработка и выпуск таких устройств, которые могут без проблем соединяться между собой и беспрепятственно обмениваться информацией. Наши системы сегодня поддерживают технологии беспроводной сети — Zigbee, Wi-Fi, BLE, и новые датчики базируются на этих стандартах. Кроме того, мы разработали интегрированную платформу и облачные серверы, которые помогают пользователю управлять беспроводными протоколами.

Мартин Грен,
соучредитель, Axis Communications

В 2013 году Axis представила первую сетевую систему контроля доступа, которая помогла расширить фокус компании не только на камерах как IoT-устройствах. Мы и сейчас продолжаем развивать это направление, разрабатывая IP-громкоговорители, IP-домофоны. Мы считаем, что подключенные IP-системы — назовем их IoT — могут обеспечить все виды безопасности, включая видеонаблюдение, управление функциями здания, не только на обычных объектах, но и на промышленных предприятиях.

Арьян Боутер,
руководитель отдела продаж, Nedap Security Management

Для бесперебойной работы устройств безопасности в системе IoT открытые платформы — это необходимость. При том что сами устройства безопасности становятся намного проще в обращении, требования к ним ужесточаются и усложняются. Мы предлагаем нашим клиентам платформу безопасности, построенную на универсальных системах контроля, где функционал полностью зависит от установленного ПО. Таким образом, система может легко справиться с любыми требованиями по безопасности в будущем.

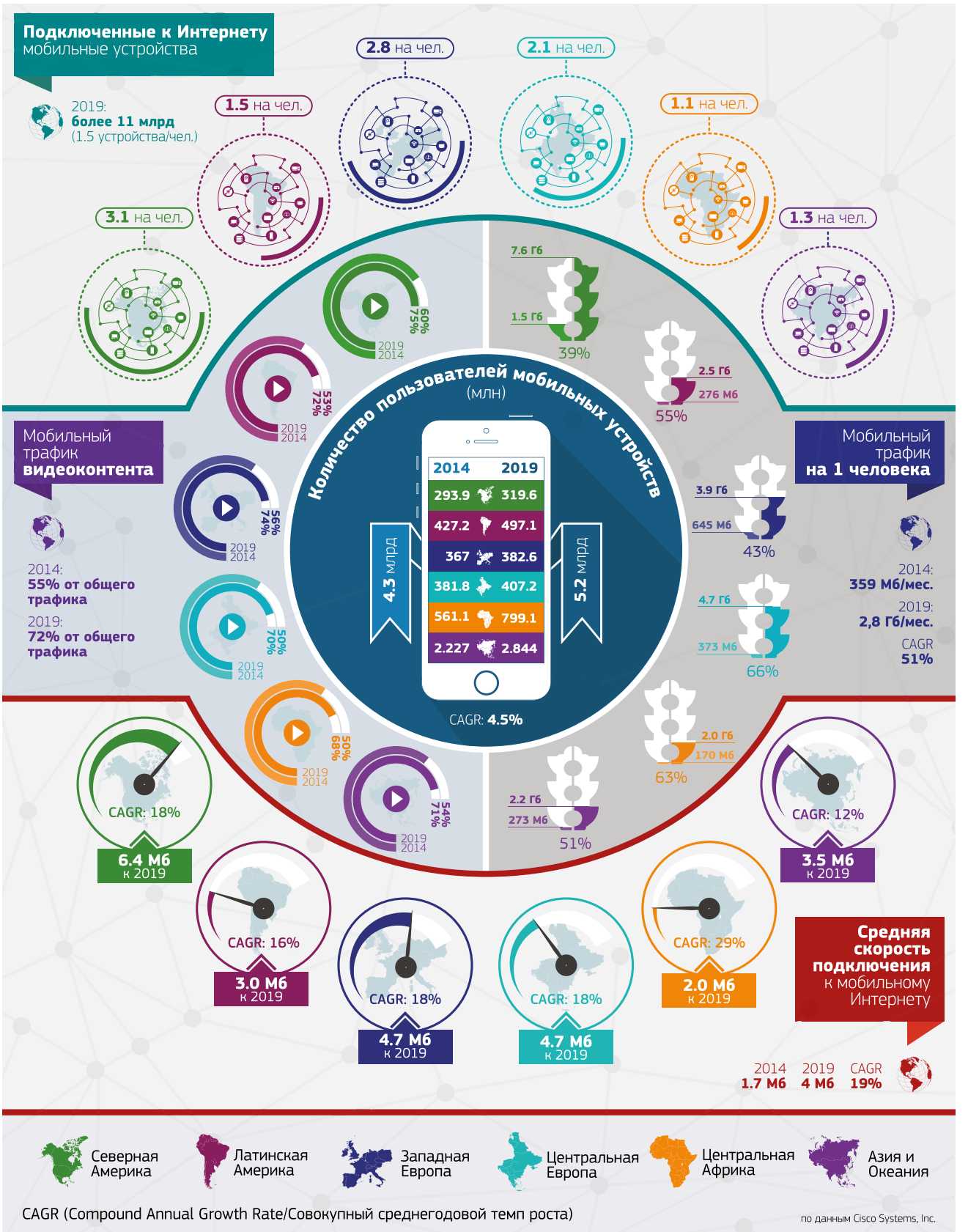
Инвестиции в IoT в Центральной и Восточной Европе, млрд долларов США*

*По данным Cisco Systems, Inc.

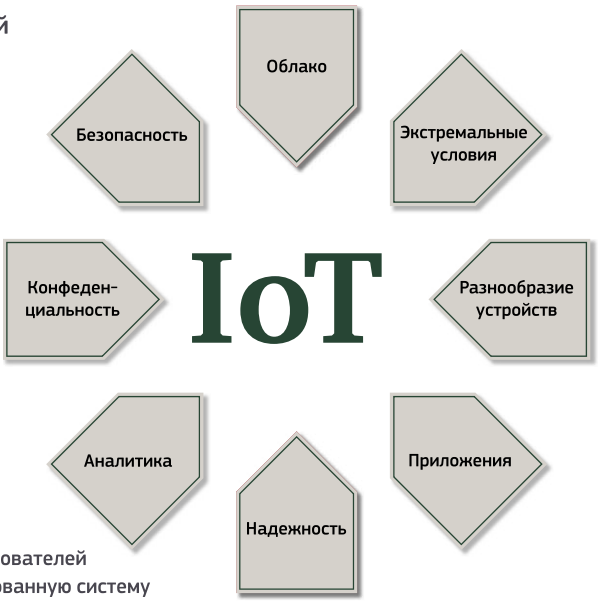
18,7% CAGR

Фото: ©Depositphotos/ljsphotography

Глобальный прогноз по мобильному трафику на период 2014–2019 гг.



Интернет вещей



Большинство пользователей IoT хотят интегрированную систему

ИЗМЕНЕНИЕ РОЛИ СИСТЕМНЫХ ИНТЕГРАТОРОВ

На рынке IoT активную роль играют не только производители систем безопасности, но и интеграторы, дилеры и консультанты в данной области. Поддержка IoT требует плотного взаимодействия между ИТ-составляющей и физической безопасностью.

Роб Мартенс,
директор направления по связующим платформам, Allegion

Мы разработали ряд новых продуктов и решений, которые предназначены для поддержки потребителей в IoT-пространстве. Например, для жилых помещений были разработаны подключенные двери. Использование новейших технологий устраняет необходимость в традиционных ключах, жильцы пользуются специальными смарт-картами и идентификаторами в своих смартфонах. В общей зоне есть возможность управлять дверями при помощи той же системы, что используется и для личных квартир, так как она построена на открытой платформе.

По словам Роба Мартенса из Allegion, для успешной реализации IoT-проектов очень важно налаживание и развитие отношений между департаментами информационных технологий и производства. Как считает Мартенс, ключевым моментом является взаимное обучение этих департаментов новым технологиям и устранение пробелов в знаниях о принципах работы смарт-устройств — координатором этой работы должна выступать инициативная группа в компании, ответственная за IoT. Она будет посредником между ИТ-службами и службами по управлению зданием.

ПРОБЛЕМЫ

Соединение большого объема данных в едином месте и хранение их в Сети естественным образом становится уязвимым для несанкционированного доступа или взлома. Поэтому перед рынком стоит важная задача по ужесточению методов борьбы с кибератаками.

Кевин Ванг,
директор бизнес-центра по развитию систем, Everspring Industry

Независимо от того, какая системная платформа используется, встроенные протоколы должны включать в себя эффективную защиту. Как минимум — это протоколы аутентификации и шифрования. Они должны быть надежными и достаточно умными, чтобы реагировать на действительно нужные события, не становясь обузой для пользователя.

Виллем Райан,
менеджер по маркетингу продукции, Avigilon

Организацию защиты следует проводить по многоуровневой схеме. Таким образом, если злоумышленник проникает за первый барьер, далее он встречает новые и новые преграды, и вероятность того, что он пройдет дальше, снижается. Первая линия для защиты данных — использование надежных паролей, вторая — актуальное программное обеспечение для IoT-устройств, своевременное обновление прошивки.

БУДУЩЕЕ IoT

Сегодня существует заметный разрыв между той шумихой, которая возникла вокруг IoT, и реальностью. «В ходе недавнего опроса выяснилось, что более 70% ИТ-специалистов уверены во влиянии IoT как на потребителей, так и на сами компании. Треть опрошенных либо фокусируются на IoT-направлении, либо уже фактически инвестируют в смарт-технологии», — отмечает Ларс Норденлунд Фриис из Milestone Systems.

С падением стоимости IoT-технологий, пропускной способности сетей, генерирования данных рынок «интернета вещей» ожидает взрывной рост уже в течение ближайших нескольких лет, что откроет новые возможности для служб безопасности. Их устройствами можно будет управлять из любой точки мира при помощи не только специализированных контроллеров, но и обычных мобильных гаджетов. В будущем — а некоторые компании, например HID Global, реализовали это уже сейчас — пользователи смогут применять телефоны и планшеты для управления системами контроля доступа и другими функциями на объектах.

Многие традиционные устройства безопасности сейчас получают «вторую жизнь» благодаря IoT-технологиям, которые внедряются в привычное оборудование. По мнению большинства компаний, те игроки, которые не обратят внимание на данный тренд, станут неактуальными для клиентов и просто потеряют рынок.