УДК 004.9:004.75

Ю.М. ЛИСЕЦКИЙ[*], С.И. БОБРОВ[*]

НОВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИЛИ ОРУЖИЕ МАССОВОГО ЗАРАЖЕНИЯ

[*]ДП «ЭС ЭНД ТИ УКРАИНА», г. Киев, Украина

Анотація. *Розглянуто проблему використання Internet of Things як способу масового зараження вірусами інформаційних систем. Описано один із найбільш небезпечних засобів впливу, спрямований на відмову в обслуговуванні інформаційних систем як основний інструмент реалізації кібератак. Приведені рекомендації щодо організації комплексного підходу до інформаційної безпеки та протидії кіберзагрозам, що виникають у зв'язку з масовим використанням IoT-пристроїв. Показано, що можливості ефективної протидії цій новій загрозі інформаційній безпеці існують.*
Ключові слова: *інформаційна безпека, пристрої IoT, віруси, кібератака, інформаційна система, інфраструктура, кіберзагроза.*

Аннотация. *Рассмотрена проблема использования Internet of Things как способа массового заражения вирусами информационных систем. Описано одно из самых опасных средств воздействия, направленное на отказ в обслуживании информационных систем как основного инструмента реализации кибератак. Приведены рекомендации по организации комплексного подхода к информационной безопасности и противодействию киберугрозам, возникающим в связи с массовым использованием IoT-устройств. Показано, что возможности эффективного противодействия этой новой угрозе информационной безопасности существуют.*
Ключевые слова: *информационная безопасность, IoT-устройства, вирусы, кибератака, информационная система, инфраструктура, киберугроза.*

Abstract. *The problem of using Internet of Things, as a method of mass infections by information systems viruses is considered. One of the most dangerous influence means focused on the refusal of information systems maintenance is described as the main tool for the implementation of cyber-attacks. The recommendations on the organization of an integrated approach to information security and countering of cyber threats arising in connection with the mass using of IoT devices are given. It is shown that there are opportunities for effective counteraction to this new information security threat.*
Keywords: *information security, IoT devices, viruses, cyber-attack, information system, infrastructure, cyber threat.*

1. Введение

В настоящее время, благодаря стремительному развитию информационных технологий, информация стала товаром, который можно приобрести, продать, обменять. Как известно, информационная безопасность основана на трех базовых принципах: целостность, доступность и конфиденциальность [1]. Утечка конфиденциальной информации, как правило, приводит к значительным финансовым потерям. Кроме утечки конфиденциальной информации, существуют другие виды информационных угроз, направленные на частичную или полную остановку рабочих процессов организаций и предприятий, блокировку оперативного доступа к необходимым внешним и внутренним информационным ресурсам, снижение производительности информационно-технологической инфраструктуры или её полную остановку [2].

С каждым годом в мире увеличивается количество киберпреступлений и кибератак [3]. В последние годы в Украине также резко возросло количество преднамеренных вмешательств в работу информационных систем государственных и коммерческих структур. Практически во всех случаях, после осуществления кибератак, работа организаций и предприятий блокировалась от нескольких часов до нескольких дней, что приводило к очень

ISSN 1028-9763. Математичні машини і системи, 2018, № 1

серьезным последствиям. Поэтому от степени безопасности информационных технологий сейчас зависят не только стабильность и надёжность функционирования государственных институтов и коммерческих структур, а зачастую и жизнь многих людей [4].

2. Internet of Things

За последние годы появилось новое семейство устройств, подключенных к Интернет и объединенных в различные группы, получившее называние Internet of Things (IoT) [5]. В основном это бытовые или промышленные устройства, которые для управления или обмена информацией имеют возможность подключения к Интернет или к серверу управления и контроля через Интернет.

Эти специализированные устройства с подключением к сети (проводным или беспроводным) обладают рядом особенностей. Первая – это невысокая вычислительная мощность, небольшой объем памяти и ограниченный набор исполняемых команд. Второй особенностью является то, что пользователь, эксплуатирующий IoT-устройство, не является специалистом в области информационных технологий или экспертом по информационной безопасности и, соответственно, не может правильно настроить устройство для безопасной работы в сети. Именно поэтому оно должно быть изначально настроено управляться производителем при его эксплуатации, в противном случае может стать потенциальным источником сетевых проблем. Третьей особенностью является отсутствие каких-либо серьезных функций безопасности, потому что любые ограничивающие настройки или функции могут создать проблемы при эксплуатации неподготовленными пользователями, а, значит, в условиях жесткой конкуренции снизить привлекательность продукции и, как следствие, объемы продаж и доходы производителя.

Ограничения, накладываемые на сетевое взаимодействие устройства, могут привести к тому, что конфигурация сетевых настроек устройства и сетевое окружение окажутся несовместимы и доступ к сети не будет установлен. Именно поэтому производители стараются сделать количество ограничений как можно меньше, а сетевые настройки как можно более простыми.

И совершенно очевидно, что такое, практически не защищенное, устройство, подключенное к сети, является «привлекательным» для разного рода киберзлоумышленников. Возможно, это и не представляло бы серьезной проблемы, если бы количество IoT-устройств не было таким массовым и не исчислялось миллиардами (табл. 1).

Таблица 1. Количество устройств IoT и прогнозные показатели

Категория	2016	2017	2018	2020
Бытовые	3 963,0	5 244,3	7 036,3	12 863,0
Промышленные/корпоративные	2 418,7	3 136,4	4 160,3	7 552,4
Всего, млн шт.	6 381,8	8 380,6	11 196,6	20 415,4

По данным Gartner (January 2017), сейчас в мире более 8 млрд подключенных устройств, а к 2020 их будет более 20 млрд. Данные Statista, приведенные на рис. 1, еще более впечатляющие.

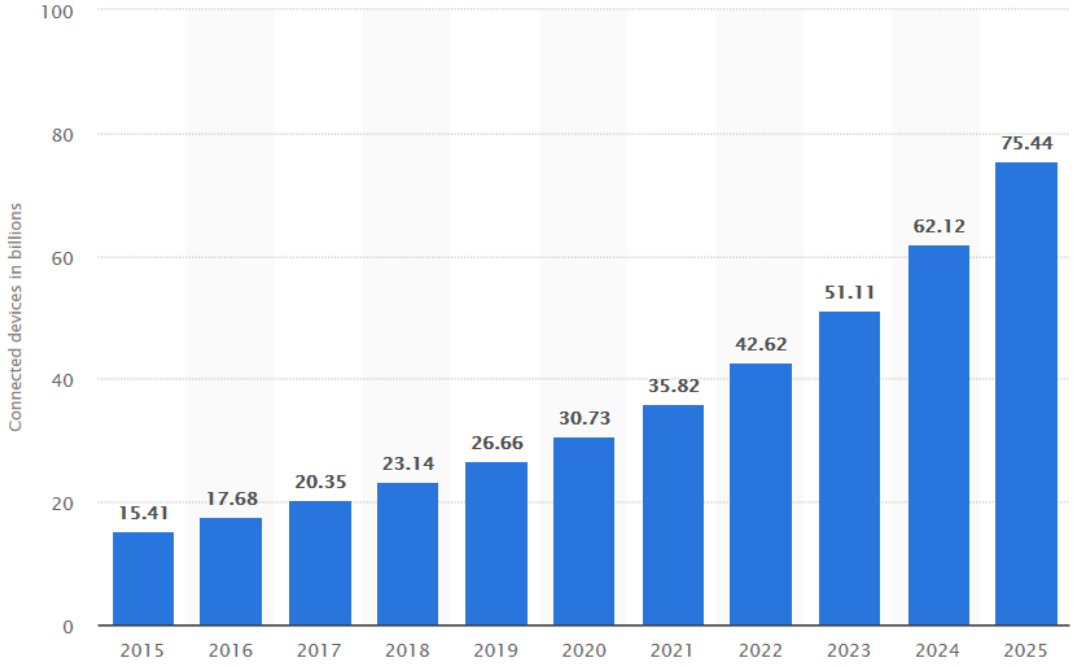

Рис. 1. Тренд увеличения IoT-устройств

Но даже если принимать во внимание только данные Gartner, то уже сейчас количество подключенных устройств превышает количество людей на Земле (7,5 млрд чел.), а к 2020 г. превысит почти в 3 раза. Поэтому игнорировать вопросы безопасности миллиардов устройств, несмотря на то, что каждое из них малопроизводительно, было бы ошибочно.

3. DDoS как основной инструмент реализации кибератак

В настоящее время одним из самых опасных средств воздействия на информационные системы являются атаки, направленные на отказ в обслуживании (Distributed Denial of Service или DDoS) [6]. Первое упоминание о таких атаках встречается в 1999 г., но тогда они не привлекали особого внимания, так как считались нишевыми, не создающими особенных проблем по сравнению с другими атаками. Ситуация существенно изменилась, когда в 2011 г. группа хакеров Anonnymous начала использовать DDoS-атаки как основной инструмент реализации кибератак. DDoS-атака представляет собой поток ложных запросов на базе различных протоколов (TCP, UPD, ICMP, HTTP, DNS, SIP и др.). Основной целью ложного потока является блокировка ресурсов или сервиса жертвы. Атакуемым ресурсом жертвы может быть любой элемент информационно-технологической инфраструктуры: канал связи, сетевое устройство, устройство безопасности (firewall, IPS), сервер, приложение или база данных. DDoS-атаки направлены не на уязвимость отдельных элементов информационно-технологической инфраструктуры, а на превышение допустимых параметров их производительности, что блокирует работоспособность устройств и приводит к отказу работы сервисов. Основной опасностью DDoS-атак является то, что каждая отдельная составляющая такой атаки на первый взгляд ничем не отличается от легитимного запроса пользователя, что значительно усложняет блокировку атаки и увеличивает количество ложных срабатываний. Жертвой DDoS-атаки может быть любая организация, которая использует сеть Интернет (государственные и правительственные учреждения, банки, операторы связи, предприятия топливно-энергетического комплекса, транспортной инфраструктуры, почта и др.). Недоступность сервисов даже на короткий период времени может привести к значительным финансовым потерям, а на более длительный – даже к

коллапсу. За последние годы длительность DDoS-атак постоянно растет. Если в 2000 г. атаки продолжались несколько часов, то сейчас их длительность может измеряться неделями. По данным «Лаборатории Касперского», самая продолжительная атака длилась 81 день.

Развитие киберпреступности приводит к тому, что атаки становятся более усовершенствованными и многовекторными, нацеленными на несколько элементов инфраструктуры одновременно [7]. Такой сценарий значительно усложняет методы защиты и предъявляет новые требования к архитектуре систем информационной безопасности [2]. По результатам анализа Corero Network Security, в 3-ем квартале 2017 г. количество DDoS-атак выросло на 91% по сравнению с первым кварталом этого же года и составило в среднем 237 атак на организацию в месяц. Источниками достаточно большой части этих атак являются IoT-устройства, подчиненные злоумышленником и объединенные в сети, называемые ботнетами (botnet). Так, в сентябре 2016 г. на сайт журналиста Брайана Кребса была совершена DDoS-атака мощностью до 620 Гб/с. Затем атаке подвергся французский хостинг-провайдер OVH, который оказался под атакой 1 Тб/с. Как сообщил технический директор провайдера, источником атаки оказались 152 тыс. «умных устройств», в основном уличные видеокамеры и видеорегистраторы. Позднее, в октябре 2016 г. была осуществлена DDoS-атака на крупнейшего в США провайдера DNS – компанию Dyn. Атака была осуществлена ботнетом, состоящим из сотен тысяч IoT-устройств. Мощность атаки 1,2 Тб/с. Атака привела к недоступности или перебоям в работе около сотни крупнейших Интернет-сервисов в течение нескольких часов по всему миру и вызвала такой резонанс, что даже получила персональное название по дате – 10/21, по аналогии с атакой на WTC – 9/11. И таких примеров множество. Причем, это не явление 2017 г. Такие атаки, но меньшего масштаба, наблюдаются, начиная с 2014 года.

4. IoT-устройства – оружие массового заражения

Включение любого устройства в ботсеть происходит после заражения его вирусом. В случае IoT обычно имеют дело с вирусом семейства Mirai (дано по имени бинарного файла) или подобным ему. Данный вирус атакует Linux-устройства, использующие набор утилит Busybox. Вирус использует, так сказать, «социальную инженерию», а именно, пробует получить доступ к устройству через telnet, перебирая 50 вариантов имен/паролей (табл. 2), которые используются по умолчанию в IoT-устройствах крупнейших производителей (Ubiquiti, Raspberry, Ubuntu based, Dahua, Hikvision,...).

Таблица 2. Наиболее часто используемые имена и пароли

Имена	Пароли
admin	admin
root	xc3511
root	vizxv
root	juantech
root	default
admin	admin1234
root	password
root	root
root	xmhdipc
admin	smcadmin
root	Admin
admin	Root
DUP root	123456

Продолж. табл. 2

ubnt	12345
access	Ubnt
DUP admin	Password
test	1234
oracle	Test
postgres	Qwerty
pi	Raspberry

Как только доступ к устройству получен, вирус инсталлируется в систему, связывается с контроллером ботнета и сообщает о себе, далее стирает себя с носителя для уменьшения вероятности обнаружения, оставаясь в оперативной памяти, сканирует диапазон IP-адресов, проверяя на наличие уязвимых устройств, и отправляет эту информацию контроллеру ботнета. Несмотря на то, что вирус достаточно прост, использует тривиальную методику перебора пароля «brut force», но, как оказалось, и этого достаточно для организации ботнет на сотни тысяч IoT-устройств.

Сейчас новые заражения Mirai возникают все реже, но это не значит, что вирус побежден. Во-первых, существует множество мутаций и вариантов вируса (Hajime, LuaBot,…), а во-вторых, устройство, превращенное в члена ботнета, никак себя не проявляет и может быть использовано контроллером ботнета в следующих атаках, то есть мы можем только предполагать, насколько вирус распространился и какое количество устройств он контролирует, но эксперимент осенью 2016 года показал, что «незащищенное» устройство, выставленное в Интернет, подверглось атаке уже через 40 мин, а за последующие 11 часов его пытались атаковать 300 раз. Плюсом является то, что избавиться от вируса Mirai и предохраниться от последующего заражения довольно просто: отключить устройство от Интернет, перезагрузить его, поменять имя/пароль на устойчивые к взлому, по возможности запретить подключение к устройству через Интернет по telnet/ssh и прочим возможным способам управления и после этого подключить устройство к Интернет опять. Хорошей рекомендацией будет также проверить наличие и установить обновление ПО. Снижение активности Mirai происходит за счет того, что «кормовая база» вируса уменьшается: устройства, зараженные одним контроллером ботнета, не поддаются заражению другим, а после завершения атаки случается, что контроллер просто выключают и сеть остается в пассивном состоянии. Кроме того, количество «беззащитных» IoT-устройств уменьшается за счет выполнения рекомендаций ИТ-безопасности.

Этот пример свидетельствует о практически нулевом уровне ИТ-безопасности IoT-устройств, так как даже такой не сложный вирус, который получает доступ к устройству путем простого перебора 50 паролей «по умолчанию», смог проникнуть в сотни тысяч устройств и выполнить вредоносные действия. Проблема также и в том, что владельцы таких устройств не только не занимаются защитой, но и не подозревают, что их устройство подвергалось атаке, тем более что и проблемы возникают не у них.

Но существует еще один класс вирусов – BrickerBot. Пока он представлен двумя версиями: BrickerBot.1, BrickerBot.2. Вирус был обнаружен и описан компанией Radware весной 2017 г. Результатом действия этих вирусов является PDoS (Permanent Denial of Service), а именно невозможность использования этого устройства, превращение его в кирпич (от слова кирпич/Brick и происходит название вируса). Вирус атакует устройства IoT на базе Linux с набором Busybox (рис. 2). При атаке проверяется открытый TCP порт 23 (telnet) и происходит подбор пароля, начиная с пары 'root'/'vizxv'. Как видно, в этом BrickerBot полностью похож на Mirai. Различия начинаются в действиях вируса после проникновения. BrickerBot оправдывает свое название. Он пытается удалить все содержимое любого хранилища – внутреннего или непосредственно подключенного к устройству,

нарушает связь с Интернет (net.ipv4.tcp_timestamps=0) и препятствует выполнению операций ядра (kernel.threads-max=1). Таким образом, данный вирус, по сути, делает устройство недоступным, что приводит либо к замене устройства, либо, в лучшем случае, к полному его обнулению и восстановлению прошивки.

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Рис. 2. Атака вируса BrickerBot.1

Отличие между BrickerBot.1 и BrickerBot.2 наблюдается в инициаторах заражения, в способе действия после заражения и в продолжительности атак. Если первый атаковал с определенного набора IP-адресов, то второй атаковал из сети TOR и соответственно отследить его инициаторов не так просто. Кроме того, он не использует набор BusyBox, что делает его более универсальным. Считается, что BrickerBot.2 активен до сих пор. Многие полагают, что BrickerBot был запущен для уменьшения «популяции» устройств, доступных для атаки типа Mirai, так как оба вируса используют одинаковые алгоритмы проникновения в устройство и BrickerBot просто уничтожает устройство, которое доступно для заражения Mirai. Есть сообщения, что вирус вначале пытается помочь зараженному устройству, устранив уязвимости, ничего при этом не повреждая, но если это не получается, то происходят деструктивные действия, но эти сообщения пока невозможно ни подтвердить, ни опровергнуть. Но, несмотря на такие, возможно, благородные побуждения, BrickerBot несет реальную угрозу безопасности и жизни людей. Представим выведенные из строя камеры видеонаблюдения или NVR на объектах критической инфраструктуры, неработоспособное медицинское оборудование во время операции или системы управления тепло- и электроснабжением в зимний период и т.п. Конечно, перечень вирусов IoT-устройств не ограничивается Mirai, Hajime, LuaBot, BrickerBot.1 и BrickerBot.2. Они стали наиболее известными из-за общественного резонанса, вызванного крупными DDoS-атаками с массовым заражением IoT-устройств.

Дальнейшим трендом атак на IoT-устройства являются усложнение способов атаки и благодаря этому новые возможности получения прибыли. Незащищенность IoT-устройств и наличие криптовалюты делают вымогательство при помощи взлома бытовых IoT устройств «привлекательным» для кибермошенников. Уже проводились экспериментальные взломы домашних регуляторов температуры с их блокировкой и требованиями оплаты за разблокировку (действие, аналогичное широкоизвестному в нашей стране вирусу Petya), а с учетом того, что в среднестатистическом доме в благополучных странах находится около 12 устройств с подключением к Интернет (в том числе маршрутизаторы,

ТВ, холодильники, «умный дом», термостаты и пр.), то найти незащищенное устройство и, перехватив управление над ним, потребовать денег, не будет чем-то невозможным [8].

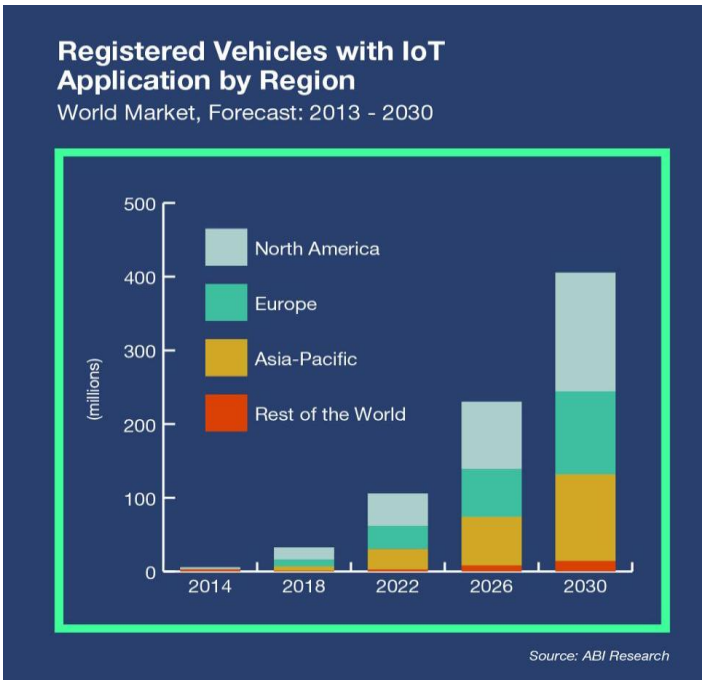

Рис. 3. Транспортные средства с IoT

Говоря о «перехвате управления», необходимо упомянуть об «умных автомобилях». По сообщениям ABI Research по дорогам мира ездит около 20 млн зарегистрированных транспортных средств, которые тем или иным способом подключены к Интернет (для диагностики, обновления дорожной информации и пр.), а к 2030 году их количество увеличится до 400 млн (рис. 3).

Они также могут стать объектом атаки, которая может иметь катастрофические последствия. Так, например, в 2015 году были продемонстрированы успешный перехват управления, блокировка дверей и отправка в кювет Jeep Cherokee с водителем. Атака была выполнена через информационно-развлекательную систему автомобиля, подключенную к Интернет.

5. Рекомендации по обеспечению безопасности IoT-устройств

По мнению аналитиков, для решения проблемы безопасности IoT-устройств необходимо пользоваться принципами, используемыми для организации корпоративной системы информационной безопасности, поэтому для IoT-устройств рекомендуется сделать следующие первоочередные шаги:

- изменить имя/пароль устройства на взломостойкое (требование к паролю – не менее 8 символов, должен содержать цифры, буквы верхнего регистра и специальные символы);
- установить все обновления безопасности производителя;
- при приобретении устройства проверить репутацию производителя с точки зрения ИТ-безопасности и периодичность выхода обновлений настроек безопасности;
- отключить UPnP-протокол и доступ по telnet из Интернет, если это возможно;
- отключить все неиспользуемые протоколы и сетевые функции;
- анализировать аномалии трафика устройства;
- контролировать известные сигнатуры атак для предотвращения заражения;
- контролировать конфигурацию устройств и сигнализировать о ее изменении.

На сегодняшний день есть четкое понимание, как реализовать эти рекомендации в корпоративной среде. Но стоит задача – реализовать это для конечного пользователя, подключенного к Интернет непредсказуемым образом, у которого все настройки безопасности в лучшем случае установлены «по умолчанию», а в худшем – отключены вовсе.

Решение данной проблемы возможно только при комплексном подходе, в котором пользователь не будет играть ключевую роль ввиду естественного отсутствия компетенции. Таким образом, задача обеспечения безопасности IoT-устройств делится на две составляющие: настройка безопасности на самом устройстве и сетевая безопасность.

Внесение изменений в настройки и добавление функций безопасности – задача производителя. Более того, это касается как новых устройств, на которых необходимо просто поменять настройки по умолчанию, так и существующих. Производитель должен внести следующие изменения в устройства:

• выполнить требование по установке надежного пароля как обязательный шаг при первом включении системы;

• установить защиту от повторного набора пароля (таймаут перед очередной попыткой входа и блокировка эккаунта на время после 3-х неудачных попыток);

• отключить по умолчанию все необязательные сетевые протоколы и внешний telnet;

• отключить WiFi по умолчанию и включить его только после настройки безопасности не хуже WPA-PSK или хотя бы WEP.

Решение вопросов сетевой безопасности должно быть задачей производителя IoT-устройств как компании, заинтересованной в успехе продвижения своих устройств. Если мы говорим, что производитель берет на себя все функции обеспечения безопасности, в том числе и информационную безопасность сетевого периметра устройства, то весь трафик устройства должен проходить через датацентр, в котором будут предусмотрены защита от сетевых атак и защита от вирусов. Для этого, после подключения к Интернет, устройство устанавливает SSL-туннель на заранее установленный адрес кластера концентраторов в датацентре производителя, и любой другой трафик, кроме трафика VPN, во внешний мир запрещается. Действуя таким образом, производитель может на устройстве:

• обеспечивать защиту от заражения;

• обеспечивать защиту от сетевых атак;

• контролировать состояние и ошибки на устройстве для проактивной поддержки;

• производить контроль актуальности ПО, контроль изменения настроек.

Недостатком такого решения является то, что весь трафик устройства идет не по оптимальному маршруту, то есть вносится высокая задержка, так как ему необходимо проходить через глобальный или региональный Центр обработки данных (ЦОД) производителя.

Наиболее целесообразным для производителя будет обеспечение сетевой безопасности IoT-устройства, особенно для тех устройств, которые не используют подключение к Интернет для передачи тяжелого контента (видео, аудио,…). Так, некоторые страны запретили определенные типы устройств из-за их небезопасности и уязвимости к взлому, который может привести к тяжелым последствиям [9]. Например, в начале 2017 г. власти Германии запретили продажу куклы Cayla, так как использовался незащищенный канал в Интернет, а осенью 2017 г. под запрет попали детские смартчасы в силу уязвимости для несанкционированного прослушивания и подмены информации о местонахождении ребенка. Этот запрет, безусловно, снизит объемы продаж производителя, что должно будет привлечь его внимание к повышению информационной безопасности устройств.

В случае невозможности или неготовности производителя к созданию своего ЦОДа с центром очистки трафика, эту функцию может взять на себя оператор связи, который, как правило, обладает необходимыми ресурсами и которые могут быть адаптированы под защиту IoT-трафика, тем более существует опасность, что трафик оператора может быть заблокирован из-за большого потока DDoS или других атак с его IP-адресов.

Оператор связи может пропускать весь трафик через сетевую систему безопасности и взять на себя следующие функции:

• выделение трафика IoT-устройств;

• проверку трафика IoT-устройств на вирусы и на аномалии трафика при помощи системы Advanced Mailware Protection;

• блокирование трафика к известным контроллерам ботнета.

Оператор связи также может предоставить услугу по управлению и контролю IoT-устройствами абонентов на базе семейства протоколов TR-69, разместив в своей корпоративной сети управляющий сервер и передав его адрес в настройки абонентских устройств. В этом случае возникает вопрос безопасности самого сервера, контроля доступа к нему и защиты от вредоносного программного обеспечения, но данная проблема решается системой корпоративной информационной безопасности на высоком уровне.

Для выполнения этих мероприятий:

• производителю понадобится встроить в IoT-устройства файерволы, TR-69 и VPN-клиенты, поменять настройки безопасности и усложнить первоначальную настройку устройств пользователем, построить ЦОД для обеспечения сетевой безопасности, установить управляющий сервер, расширить службу поддержки производителей группой по проблемам безопасности;

• оператору может понадобиться расширить свою подсистему malware protection;

• пользователю понадобится пройти более сложную процедуру настройки устройств и потратить немного больше средств на сетевую безопасность от производителя или оператора связи.

Но в конечном счете затраты на эти мероприятия на порядки меньше, чем потенциальные потери от возможных DDoS-атак с использованием IoT-устройств как оружия массового заражения.

6. Выводы

Рассмотренная проблема использования Internet of Things в качестве весьма простого и массового способа заражения вирусами информационных систем является достаточно новой, а необходимость организации эффективного противодействия этой угрозе информационной безопасности – чрезвычайно актуальной и важной.

В статье приведены рекомендации по организации комплексного подхода к информационной безопасности и противодействию кибератакам, возникающим в связи с массовым использованием IoT-устройств. Показано, что возможности эффективной защиты от данного вида киберугроз существуют.

Однако маловероятно, что производители IoT-устройств и тем более операторы связи захотят самостоятельно предпринять необходимые меры для их информационной защиты. Скорее всего, учитывая всю серьезность проблематики новых видов киберугроз, решение регуляторных вопросов в этой области должно взять на себя государство, так как для обеспечения информационной безопасности при массовом использовании IoT-устройств необходимо внести соответствующие изменения в национальную нормативно-правовую базу, включающие в себя вопросы защиты информации на всех уровнях.

СПИСОК ИСТОЧНИКОВ

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / Домарев В.В. – К.: ООО «ТИД» ДС, 2001. – 688 с.

2. Раткин Л.С. Средства защиты информации как часть инфраструктурной системы глобальной национальной безопасности / Л.С. Раткин // Защита информации. Инсайд. – 2016. – № 4 (70). – С. 25 – 29.

3. Шейн Х. Кибервойн@. Пятый театр военных действий / Шейн Х. – Москва: Альпина нонфикшн, 2016. – 392 с.

4. Стрельцов А.А. К вопросу о цифровом суверенитете / А.А. Стрельцов, П.Л. Пилюгин // Информатизация и связь. – 2016. – № 2. – С. 25 – 30.

5. Сабанов А.Г. Некоторые проблемы обеспечения безопасности интернета вещей / А.Г. Сабанов // Защита информации. Инсайд. – 2016. – № 4 (70). – С. 54 – 58.

6. Лисецкий Ю.М. Информационная безопасность: защита от DDoS-атак / Ю.М. Лисецкий // 16-th International Conference «System Analysis and Information Technologies SAIT 2014», (Київ, 26–30 May 2014). – Kyiv, 2014. – P. 405 – 406.
7. Maximum Security (Anonnymous). – Ondianapolis: Sams Publishing, 2003. – 945 p.
8. Курчеева Г.И. Угрозы для информационной безопасности в высокоорганизованных системах типа «умный город» / Г.И. Курчеева, В.В. Денисов // Науковедение. – 2016. – Т. 8, № 3 (34). – С. 45.
9. Малюк А.А. Зарубежный опыт формирования в обществе культуры информационной безопасности / А.А. Малюк, О.Ю. Полянская // Безопасность информационных технологий. – 2016. – № 4. – С. 25 – 37.

Стаття надійшла до редакції 05.12.2017