ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Коршунов Николай Сергеевич
Магистрант, Московский технический университет связи и информатики
111024, Россия, Москва, улица Авиамоторная 8а
Верба Вера Алексеевна
Кандидат технических наук, доцент, Московский технический университет связи и информатики
111024, Россия, Москва, улица Авиамоторная 8а

Аннотация. Рассмотрена проблема обеспечения безопасности информации в Интернете вещей (IoT). Предложена декомпозиция проблемы по типу взаимодействующих устройств и характеру взаимодействия. Рассмотрены серверные и встроенные («embedded») конечные системы, их специфика и множество возможных угроз. Проанализированы характерные для сетевого взаимодействия в Интернете вещей векторы атак. Атаки по этому направлению агрегированы в две категории: прослушивание сетевых данных и влияние на сетевые ресурсы.

Ключевые слова. Интернет вещей, безопасность, информация, IoT, информационные технологии.

Annotation. The problem of ensuring the security of information on the Internet of things is considered. The proposed decomposition of the problem according to the type of interacting devices and the nature of the interaction. The server and embedded “embedded” end systems, their specifics and many possible threats are considered. The attack vectors characteristic for network interaction in the Internet of Things are analyzed. Attacks in this direction are aggregated into two categories: listening to network data and the impact on network resources.

Keywords. Internet of things, security, information, IoT, information technology.

Интернет вещей (англ. Internet of Things, IoT) - это сеть, состоящая из взаимосвязанных физических объектов (вещей) или устройств, которые имеют встроенные датчики, а также программного обеспечения, позволяющего осуществлять передачу и обмен данными между физическим миром и

компьютерными системами, с помощью использования стандартных протоколов связи.

Согласно ITU-T Y.2060 [1], Интернет вещей (Internet of Things, IoT) - глобальная инфраструктура для информационного общества, которая включает передовые решения по объединению физических и виртуальных вещей на основе существующих и разрабатываемых информационных и коммуникационных технологий.

Вещи являются независимыми системами со встроенной электроникой, программным обеспечением (ПО) и сенсорами, способными к сетевому взаимодействию, сбору и/или переработки информации.

По информации Tech Navio [2], Интернет Вещей будет составлять все большее и большее число подключений, а общее их количество возрастет до 17 млрд. в ближайшие 5 лет. Процесс будет состоять из трех волн: сначала, объединятся устройства, которые служат потребителям, дальше IoT расширится до подключенных устройств на предприятиях, и наконец его использование станет массовым благодаря внедрению в государственных органах и органах исполнительной власти.

IoT позволит частным и общественным организациям оптимизировать управление, ускорить отклик системы производства на управляющие воздействия, и разрабатывать более новые и эффективные бизнес модели.

Задача обеспечения безопасности информации в IoT можно разделить на 2 подзадачи: обеспечение безопасности конечных систем и обеспечения безопасности их сетевого взаимодействия (рис.1).

Конечные системы удобно разделить на 2 категории: серверные системы и так называемые «embedded» системы. Согласно определению NC State University's Electrical and Computer Engineering Department,«embedded» system или «встроенная система» - это система специального назначения, в которой компьютер полностью встроен в устройство, которым он управляет. В отличие от компьютеров общего назначения, встроенные системы выполняют заранее определенные задачи, как правило, с очень конкретными требованиями.

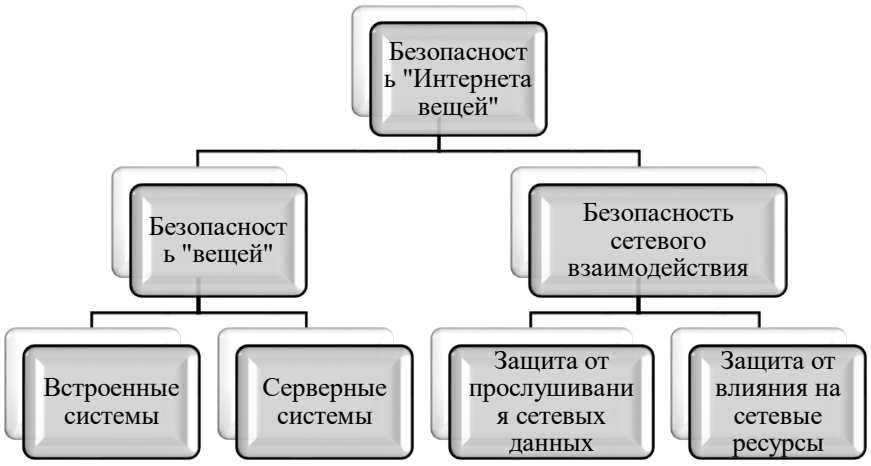

Рис. 1 Общая структура обеспечения ИБ в IoT

При наличии у злоумышленника доступа к таким системам может быть реализована модификация схемы устройства (платы / микросхемы), то есть установление физических закладок в само устройство или в разрыв кабеля (в случае Ethernet) способных образовывать каналы утечки информации.

Причиной возникновения в конечных устройствах программных закладок, способных влиять на данные, которые передаются в следующие устройства в сети, являются неправильные процессы обновления версий прошивки, или использование сторонних прошивок нелицензированных производителей.

Не менее остро стоит вопрос защиты серверных систем, которые представляют собой программно-аппаратные комплексы, выполняющие определенные сетевые службы и реализующие прием запросов от клиентов. Согласно отчета W3Techs [7], 35.98% серверных систем работают на базе ОС Linux (Debian, Ubuntu, CentOS, RHEL, Gentoo) 31.52% на базе BSD и других подобных Unix системах (FreeBSD, HP-UX, Solaris), и 32.5% на базе Windows Server. Проведенный анализ использования операционных систем позволяет определить угрозы их безопасности и сгруппировать их по следующим векторам:

- Использование известных (легальных) каналов получения информации (эксплуатация ошибок в конфигурации системы безопасности, несанкционированное использование легальных учетных записей и др.).

- Использование скрытых каналов получения информации (угроза использования злоумышленником недокументированных возможностей ОС, уязвимостей нулевого дня и др.).
- Создание новых каналов получения информации с помощью встроенного вредоносного кода (использование логических бомб, троянских программ и др.).

Несмотря на то, что существует множество современных технологий, с помощью которых можно построить IoT [3], широко принятых унифицированных стандартов для разработчиков все еще нет. Отсутствие стандартизированного подхода к построению IoT приведет к возникновению новых типов угроз и общей уязвимости системы.

Таблица 1. Сравнительный анализ средств оценки информационной безопасности

Критерии	Средство оценки защиты ИБ ИС			
	RiskWatch	ГРИФ	CRAMM	Аван Гард
Нормативная база	ISO 17799	ISO 27001	ISO 17799	ГОСТ Р 15408
Метод оценки	количественный			
Модель угроз	Нет ограничений	3-базовые угрозы	Нет ограничений	нет
Показатель защиты	риск			
Модель нарушителя	нет			
Использование прогнозных оценок	Не используется			
Адаптация к ИС	Есть	Есть	Есть	Частично

В роли математического аппарата предложено применять теорию случайных процессов, включающую в себя множество всевозможных элементов, из которых выбраны Марковские цепи, а также процессы, решающие задачу по оценке защищенности [4] киберфизических систем.

В качестве математического аппарата для оценки защищенности киберфизических систем, рассмотрим Марковские цепи и Марковский процесс.

В качестве Марковской цепи будем принимать последовательность случайных величин $X_1, X_2, \ldots, X_n$ с множеством возможных состояний (значений) E, [5], если в случае фиксированного значения X_{in} случайной величины X_n для текущего периода n значение для случайной величины $\mathbf{X_{ń}}$ для будущего периода

n> ń не будет зависеть от предыстории X_{i1}, X_{i2}, …, $X_{i(n-1)}$:

$$P\{X_{ń} = X_{in} / X_1 = X_{i1}, X_2 = X_{i2} \dots X_n = X_{in}\}$$

где n, ń - считаются начальным и конечным периодом времени выполнения испытания, n, ń = 0,1,2,…, ń>n**;** X_{i1}, $X_{i2}\dots X_{i\,(n-1)}$ - состояние процесса в период времени n X_{i1}, $X_{i2}\dots X_{i\,(n-1)} \in$ **E.**

Однородный процесс Маркова **X(t)** с дискретным множеством значений S_0, S_1, S_2, …, S_n можно определить постоянными интенсивностями перехода

$$\lambda_{ij} = \lim_{\Delta t \to 0} \frac{P(X(t+\Delta t)=j / X(t)=i)}{\Delta t}$$

из значения i в значение j, а также при помощи начального вектора распределения вероятностей $p_i(0) = P(X(0) = i)$, I = 0,1,2, …, m.

Оценка и прогнозирование инцидентов по субъективным дестабилизирующим факторам:

1. Первоначальные данные: Множество угроз ИБ X = $\{X_j\}$.

2. Вектор исходного значения Марковского процесса $\bar{a}$= (a_0, a_1, …, a_j), где j — считается количеством значений анализируемой системы.

3. Матрица переходных вероятностей Марковского процесса размерностью mxn

$$D = \begin{pmatrix} d_{0,1} & \dots & d_{0,m} \\ d_{1,1} & \dots & d_{1,m} \\ d_{n,1} & \dots & d_{n,m} \end{pmatrix}$$

4. Интенсивность потока отказа (угрозы ИБ $x_j \in X$) $\boldsymbol{\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{j-1})}$, где j – количество значений анализируемой системы.

Оценивание угроз ИБ для развития КФС производится с целью выделения угроз, которые необходимо контролировать в первую очередь.

Главной задачей методики проверки ИБ является оценивание вероятности применения выходных данных модели, с целью их применения в качестве входных для разработки рекомендаций для увеличения степени безопасности в КФС.

Базовые ограничения при проведении исследования:

- Период работы системы - 720 часов;
- Количество траекторий Марковского процесса равно 50;

- Наблюдаемая величина - время нахождения системы в состоянии t.

Результаты работы модели представлены на рисунке 2.

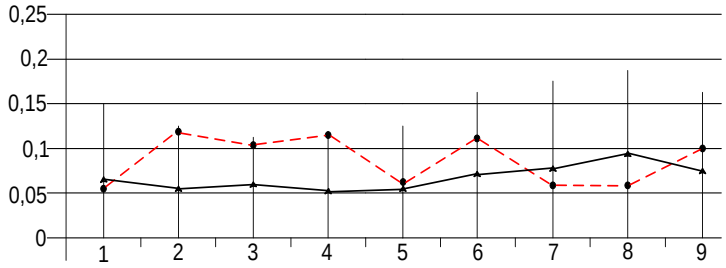

Рис. 2. Среднее время нахождения системы в n-ом состоянии по одной базовой угрозе

Результаты работы модели по всем угрозам изображены на рисунке 3.

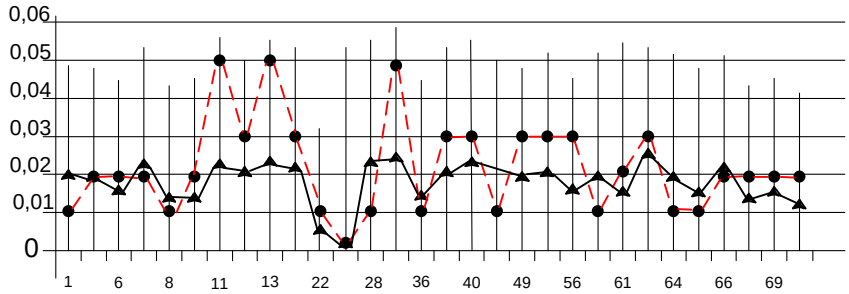

Рис. 3. Количество инцидентов по всем угрозам ИБ

Исходя из результатов исследования, можно судить о неустойчивости системы, что впоследствии приводит к слабому уровню защищенности. В первую очередь, необходимо обратить внимание на защищенность состояний 13, 28, 32, 62.

Характерной особенностью исследования является то, что процесс разработки контрмер является весьма неопределенным, что в первую очередь связано с тем, что результаты исследования не позволяют сделать конкретные выводы о том, кто именно реализует угрозы ИБ, а также какие средства необходимо применять для защиты.

Основной целью исследования методов аудита угроз ИБ согласно оценке экспертов [6], является анализ работы, моделируемой и реальной систем в сфере ИБ. Для этого необходимо:

- Построение графа КФС;
- Построение матрицы переходных вероятностей;
- Вектор начального состояния;

- Интенсивность потока отказов.

Оценка случаев нарушения ИБ в КФС согласно объективным угрозам ИБ (отказ в работе технических средств), производится при помощи показателя надежности системы - средний интервал времени для наработки отказа. Данные для оценивания были получены от разработчиков технической части системы и представлены в программе Excel.

Исходные результаты обработки представлены на рисунке 4 в виде сводной диаграммы.

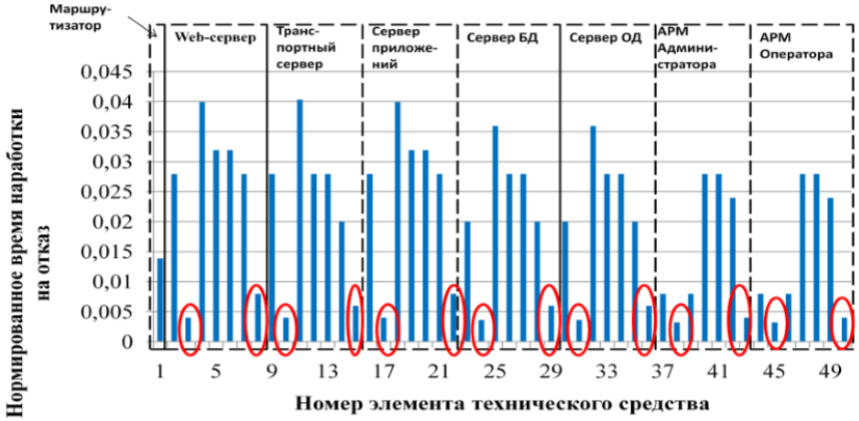

Рис. 4. Среднее время наработки на отказ компонентов КФС

Исходя из полученных результатов, наименее надежными компонентами являются блоки питания, жесткие диски и видеокарты ПК, значит, необходимо задействовать в работе резервирование данных компонентов, к примеру, организовать RAID-массивы. [7]

Заключение

К вопросу обеспечения защищенности информации в пределах IoT необходимо подходить комплексно и особенно уделять внимание таким аспектам как безопасность конечных информационных систем и безопасность их взаимодействия.

Конечные системы в целях декомпозиции можно разделить на встроенные и серверные системы, соответственно и подходы к их защите будут отличаться. Основной задачей этого направления является построение защищенных операционных систем, которые смогут эффективно противостоять

информационным атакам, как по открытым, так и закрытым каналам передачи информации.

С точки зрения сетевого взаимодействия следует уделять внимание защите от прослушивания сетевых данных и влияния на сетевые ресурсы.

Литература

1. Overview of the Internet of things.// ITU-T Recommendation Y.2060. – 2015.

2. Global IoT Security Market 2015-2019 // Tech Navio, 2015.

3. Буянов Б.Я., Верба В.А. Мультиагентные модели сложных социотехнических систем. В сборнике: Системный анализ в проектировании и управлении сборник научных трудов XX Международной научно-практической конференции. 2016. - С. 155-159

4. Barnett R.C., Grossman J. Web Application Defender's Cookbook: Battling Hackers and Protecting Users - John Wiley & Sons, Inc., 2013. — 552 p.

5. Буянов Б.Я., Верба В.А. Некоторые вопросы определения пространства состояний параметров сложных систем. В сборнике: Системный анализ в проектировании и управлении/ сборник научных трудов XXII Международной научно-практической конференции. 2018. С. 224-228.

6. Usage of operating systems for websites [Электронный ресурс] // W3Tech // Режим доступа: http://w3techs.com/technologies/overview/operating_system

7. Usage statistics and market share of UNIX for websites [Электронный ресурс] // W3Tech. // Режим доступа: http://w3techs.com/technologies/details