DOI 10.36622/VSTU.2022.25.3.011
УДК 004.735

РАЗРАБОТКА АЛГОРИТМА РАНЖИРОВАНИЯ НОСИМЫХ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ ПО СТЕПЕНИ ЗАЩИЩЕННОСТИ НА ОСНОВЕ АНАЛИЗА РИСКОВ В УСЛОВИЯХ РЕАЛИЗАЦИИ УГРОЗ НАРУШЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

С.А. Ермаков, И.В. Щетинина, А.А. Болгов, Е.А. Москалева

В данной статье предлагается алгоритм ранжирования носимых устройств интернета вещей по степени защищенности на основе анализа рисков в условиях реализации угроз нарушения целостности информации. В работе была разработана методика оценки рисков, учитывающая векторы атак на носимые устройства интернета вещей в условиях реализации угроз нарушения целостности. Определен перечень параметров для оценки риска, учитывающих условия реализации угроз целостности. В результате дальнейшей разработки методики обработки установленных параметров с применением систем нечеткого вывода была получена количественная оценка риска. Произведен пример расчёта защищенности носимых устройств интернета вещей для дальнейшего выбора устройства с максимальной степенью защищенности. На основе полученных значений было выполнено ранжирование. Результаты проделанной работы позволят повысить защищенность носимых устройств интернета вещей, упростить их разработку и внедрение с учетом обеспечения безопасности в условиях реализации угроз нарушения целостности.

Ключевые слова: интернет вещей, носимые устройства, защищенность, риск, атака.

Введение

За последние несколько лет экосистема интернета вещей (IoT) росла в геометрической прогрессии. Устройства IoT варьируются от устройств с высокой вычислительной мощностью, таких как камеры и голосовые помощники, до устройств с низкой вычислительной мощностью, таких как лампочки или выключатели света. По оценкам, в 2021 году потребители использовали более 20 миллиардов таких устройств. Взаимодействие человека с этими устройствами становится все более тесным [1].

Носимые устройства часто рекламируются как одно из величайших применений интернета вещей, и не без оснований, ведь они обладают потенциалом изменить образ жизни людей. В частности, часы, очки, украшения, повязки на голову, контактные линзы, одежда, имплантируемые устройства (используемые для измерения электрической активности организма) и т.д. обеспечивают постоянный, удобный, портативный и, в основном, свободный от рук доступ к электронике и компьютерам [2,3].

Использование носимых технологий имеют далеко идущие последствия и могут повлиять на сферы здравоохранения и медицины, фитнеса, образования, транспорта, предпринимательства, финансов, игр и музыки. Поскольку производители стремятся разработать следующее устройство, способное покорить рынок, время выхода разработки и выпуска в эксплуатацию снижается. Этот акцент на скорости разработки в сочетании с отсутствием опыта обеспечения безопасности у большинства компаний интернета вещей приводит к отсутствию соображений безопасности продукта [4].

Носимые устройства интернета вещей представляет собой огромную область атаки для хакеров, ведь в большинстве случаев они существуют вне защитных барьеров брандмауэров, не имеют вычислительных мощностей и ресурсов хранения для размещения традиционного программного обеспечения безопасности.

В настоящее время не определены практические рекомендации, направленные на реализацию обеспечения информационной безопасности носимых устройств интернета вещей, так как эта часть экосистемы молода и обширна. В данном исследовании предлагается практическая модель риска, основанная на определенном наборе параметров, логически объединенных между собой посредством аппарата математической логики и теории нечетких множеств.

В экосистемах интернета вещей концепцию классического определения риска сложно применить, так как ее основным требованием является статистика ущерба. Решение этой проблемы может быть реализовано за счет экспертных оценок данных параметров. Однако эти оценки имеют широкий диапазон значений, что сильно сказывается на точности оценки риска [5, 6].

Таким образом, понимание, расчет, оценка и управление рисками, порождаемыми устройствами интернета вещей, неизбежно становится одним из важнейших направлений исследований для специалистов информационной безопасности.

Несмотря на большое количество исследовательских усилий, затраченных на характеристику безопасности устройств IoT, не существует точных методик анализа риска, специализированно применимых к экосистеме носимых устройств интернета вещей и учитывающих распространенные векторы атак.

Таким образом, при анализе существующих методик, оценки риска носимых устройств интернета вещей были выявлены следующие противоречия между:

– отсутствием объектно-ориентированности в известных методиках и стандартах для оценки рисков носимых устройств интернета вещей и необходимостью в специализированной методике, учитывающем сложность и динамику данных устройств для более точной оценки рисков;

– ориентацией аналогов на получение качественных экспертных оценок риска и потребностью получения количественной оценки для сравнения различных носимых устройств интернета вещей;

– отсутствием алгоритма для реализации инструмента ранжирования, который автоматизирует различные аналитические действия присвоения оценки степени защищенности устройств, и необходимостью его создания для растущего рынка носимых устройств интернета вещей.

Таким образом, объектом исследования являются носимые устройства экосистемы интернета вещей, подвергающиеся атакам нарушения целостности информации.

В свою очередь, предметом исследования выступает процесс ранжирования носимых устройств интернета вещей в условиях реализации угроз нарушения целостности информации.

Постановка задач исследования

Основной целью следует считать в повышение защищенности носимых устройств интернета вещей за счет разработки алгоритма их ранжирования на основе анализа рисков в условиях реализации угроз нарушения целостности информации.

Для достижения сформулированной цели представляется необходимым решение следующих задач:

– разработать методику оценки риска, учитывающую векторы атак на носимые устройства интернета вещей, в условиях реализации угроз нарушения целостности информации;

– разработать методику количественной оценки риска носимых устройств интернета вещей в условиях реализации угроз нарушения целостности информации;

– на основе полученной числовой оценки риска в условиях реализации угроз нарушения целостности информации разработать алгоритм ранжирования носимых устройств по степени защищенности

Методика оценки риска носимых устройств интернета вещей

В рамках реализации методики оценки риска первым шагом является определение перечня носимых устройств, параметры которых будут оцениваться.

Носимые устройства по назначению эксплуатации можно разделить на несколько типов:

1. Диагностические. Наиболее популярный у врачей тип носимых устройств, применяющийся для диагностики заболеваний.

2. Профилактические. Применяются пользователями для самостоятельного отслеживания состояния здоровья. Устройства этого типа собирают большой объем данных.

3. Лечебные. К устройствам данного типа предъявляются высокие требования безопасности ввиду их непосредственной взаимосвязи с лечебным процессом пользователя.

4. Реабилитационные. Упрощают реабилитационные период пациента.

5. Аксессуарные. Устройства, которые облегчают жизнь своего владельца, выполняют функции ключа, бесконтактной оплаты и пр.

Вторым шагом является определение векторов атак на носимые устройства в условиях реализации угроз целостности.

Основные векторы атак в условиях реализации угроз целостности информации, а также соответствующие им возможные проблемы безопасности приведены табл. 1.

Таблица 1

Векторы атак на носимые устройства интернета вещей

Векторы атак	Возможные проблемы безопасности
Прошивка	Неисправленные уязвимости прошивки
	Возможность повышения привилегий
Приложения	Возможность подмены сервера обновлений
	Использование внешних или сторонних библиотек обновлений
	Отсутствие механизма проверки наличия обновлений
Библиотеки шифрования	Неисправленные уязвимости библиотек шифрования
	Отсутствие механизма проверки наличия обновлений
Протокол	Перехват трафика

Все четыре упомянутые выше вектора атак взаимосвязаны, и сбои безопасности одной, могут привести к сбоям в безопасности всего носимого устройства интернета вещей. Например, если устройство не проверяет должным образом, является ли сервер, к которому оно подключается одобренным его производителем, злоумышленники могут подделать сервер и отправить вредоносное ПО на это устройство. Это представляет собой точку отказа безопасности устройств, и даже если часть аспектов носимого устройства была спроектирована с высоким уровнем безопасности, это было бессмысленно при низком уровне безопасности других.

Третьим шагом является определение перечня атак, направленных на нарушение целостности данных.

1. Атаки эксплуатации привилегий;
2. SQL инъекции;
3. MITM атаки;
4. Вирусные атаки на сервера синхронизации данных;
5. Компрометация обновлений;
6. Использование уязвимостей протокола.

Четвертым шагом является определение параметров оценки риска, учитывающих условия реализации угроз целостности. Таким образом, на основе проанализированных векторов атак возможно определить первые четыре параметра оценки рисков: уровень

защищенности прошивки устройства, уровень защищенности приложений, уровень защищенности библиотек шифрования, уровень защищенности протокола.

Угроза является одним из главных факторов риска любого неблагоприятного воздействия на носимое устройство интернета вещей. Источниками угроз могут являться потенциальные злоумышленники различных компетентностей. В связи с этим, при анализе риска необходимо учитывать возможности потенциального злоумышленника и иметь представление о типах нарушителя, видах нарушителях и о потенциале нарушителя [7,8].

Так как носимые устройства интернета вещей обрабатывают много данных, ценность и объем которых необходимо учитывать в условиях реализации угроз целостности, необходимо ввести еще два параметра оценки риска: ценность информации и объем информации.

Для рассмотренного объекта были заданы типовые вопросы на основании опросных листов носимых устройств интернета вещей:

– «Умные» часы Apple Watch – аксессуарное устройство интернета вещей, одно из самых популярных носимых устройств в мире;

– Браслет-стимулятор Quell 2.0 - устройство для удаленного непрерывного мониторинга пациентов в послебольничный период или людей с хроническими заболеваниями;

– Фитнес-трекер Xiaomi Band – профилактическое носимое устройство, позволяющее отслеживать активность, мониторинг сна и пр.

Методика оценки риска успешной реализации атак

На этапе объединения входных параметров не рационально подавать на вход алгоритма все семь для последующего вывода численного показателя риска, поэтому предлагается модель сетевого использования логического интерфейса Мамдани.

В предложенной методике промежуточные параметры объединяются с помощью нечеткого интерфейса.

1) «Средняя вероятность» = FIS1(«Уровень защищенности прошивки устройства; «Уровень защищенности приложений»; «Уровень защищенности библиотек шифрования»; «Уровень защищенности протокола»; «Возможности потенциального злоумышленника»)

2) «Оценка тяжести последствий» = FIS2(«Ценность информации»; «Объем информации»)

3) «Риск» = FIS3(«Средняя вероятность»; «Оценка тяжести последствий»)

На рис. 1 представлена схема работы данного алгоритма, где FIS - Fuzzy Inference Model (модель нечеткого вывода).

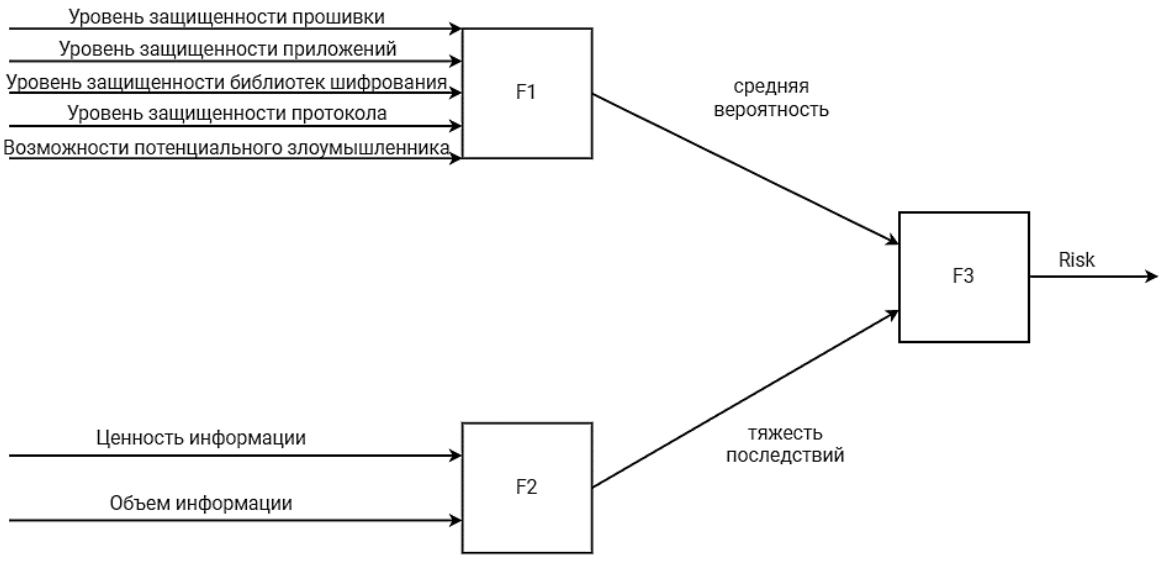

Рис. 1. Схема нечеткого алгоритма оценки риска

1) Средняя вероятность - параметр, который содержит оценку защищенности четырех векторов атак носимых устройств интернета вещей, а также возможности злоумышленника.

2) Тяжесть последствий – аналог параметра величины ущерба, который содержит оценку объема информации и ценности информации.

Для выбора наиболее подходящего носимого устройства интернета вещей возможно использовать разные параметры, однако, наиболее значимым для потребителя является оценка защищенности устройства.

$$D\% = \left(1 - \frac{R_{\text{защ}}}{R_{\text{нез}}}\right) * 100\%, \qquad (1)$$

где $R_{\text{защ}}$- риск защищенного устройства;

$R_{\text{нез}}$ - риск в незащищенного устройства.

Используя полученную формулу расчета защищенности носимого устройства (1), рассчитаем данное значение для вышеупомянутых устройств. езультаты расчета представлены в табл. 2.

Таблица 2

Переменные для расчета защищенности носимых устройств

Носимое устройство интернета вещей	$R_{\text{защ}}$	$R_{\text{нез}}$
«Умные» часы Apple Watch:	0,235	0,562
Браслет-стимулятор Quell 2.0	0,168	0,793
Фитнес-трекер Xiaomi Band	0,375	0,680

Определим процентный уровень защищенности для трех носимых устройств интернета вещей, используя данные табл.2.

Расчет защищенности для «умных» часов Apple Watch:

$$D\% = \left(1 - \frac{R_{\text{защ}}}{R_{\text{нез}}}\right) * 100\% = 58\%,$$

Расчет защищенности для браслета-стимулятор Quell 2.0:

$$D\% = \left(1 - \frac{R_{\text{защ}}}{R_{\text{нез}}}\right) * 100\% = 78\%,$$

Расчет защищенности для фитнес-трекера Xiaomi Band:

$$D\% = \left(1 - \frac{R_{\text{защ}}}{R_{\text{нез}}}\right) * 100\% = 55\%,$$

Таким образом, упорядочивая носимые устройства интернета вещей от большего уровня защищенности к меньшему получим проранжированный ряд носимых устройств по степени защищенности на основе анализа рисков (табл. 3):

Таблица 3

Проранжированный ряд носимых устройств интернета вещей

Носимое устройство интернета вещей	D%
Браслет-стимулятор Quell 2.0	78%
«Умные» часы Apple Watch:	58%
Фитнес-трекер Xiaomi Band	55%

В случае, когда двум устройствам соответствует одинаковый уровень защищенности, возможно применение дополнительного критерия «цена», при условии, что стоимость является приоритетной величиной.

Однако, возможен вариант введения критерия «уровень значимости устройства». В таком случае его значение размещено на универсальной шкале от 0 до 1 и зависит от типа носимого устройства интернета вещей.

При условии соответствия двух устройств одного типа одинаковому уровню защищенности возможно введение двух дополнительных критериев: «цена» и «уровень значимости устройства».

Частные рекомендации по повышению защищенности носимых устройств интернета вещей

Многие из носимых устройств интернета вещей разрабатываются с учетом функциональности в качестве приоритета, а функции безопасности часто отсутствуют или рассматриваются запоздало. Однако, очень важно, чтобы эти устройства, которые регулярно находятся рядом с человеком, имели средства кибербезопасности, защищающие от потенциальных угроз нарушения целостности информации и злонамеренных кибератак. Повышение защищенности носимых устройств интернета вещей для потребителей представляет собой шаг к обеспечению минимального стандарта безопасности.

В связи с вышесказанным, для повышения уровня защищенности существует необходимость в определении минимального стандарта безопасности для носимых устройств интернета вещей:

1. Запрет дублирующихся паролей по умолчанию или слабых паролей;
2. Внедрение политики раскрытия уязвимостей;
3. Своевременное обновление программного обеспечения;
4. Безопасное хранение учетных данных;
5. Сведение к минимуму открытые поверхности атаки;
6. Обеспечение целостности программного обеспечения;
7. Упрощение для потребителей удаление персональных данных.

Заключение

Таким образом, на обозрение научной общественности в настоящей работе выносятся следующие результаты:

– методика оценки риска, которая включает в себя набор параметров, учитывающих векторы атак на носимые устройства интернета вещей в условиях реализации угроз нарушения целостности информации;

– методика обработки установленных параметров с применением систем нечеткого вывода, позволяющая получить числовую оценку риска носимых устройств интернета вещей в условиях реализации угроз нарушения целостности информации;

– алгоритм ранжирования носимых устройств интернета вещей по степени защищенности на основе оценки рисков в условиях реализации угроз нарушения целостности информации.

При этом новизна вышеперечисленных результатов просматривается в том, что:

– в отличие от аналогов, разработанная методика за счет введения дополнительных параметров позволяет увеличить точность оценки рисков носимых устройств интернета вещей в условиях реализации угроз нарушения целостности информации;

– в отличие от аналогов, предложенная методика предусматривает получение числовой оценки риска для носимых устройств интернета вещей в условиях реализации угроз нарушения целостности информации путем применения нечетких сетей, элементы и совокупности элементов, которые реализуют различные компоненты нечетких моделей и этапы нечеткого вывода;

– в отличие от аналогов, разработанный алгоритм ранжирования носимых устройств интернета вещей позволяет адекватно сравнить их по степени защищенности и на основе его применения могут быть рекомендованы к применению более безопасные устройства.

Теоретическая ценность результатов:

– разработанная методика оценки риска имеет перспективу своего научно-методического совершенствования в направлении риск-оценок в условиях реализации угроз нарушения доступности и конфиденциальности информации;

– разработанная методика обработки параметров может быть дополнена математической реализацией нейронных алгоритмов для снижения субъективности экспертных оценок за счет машинного обучения;

– разработанный алгоритм ранжирования носимых устройств интернета вещей по степени защищенности на основе оценки рисков в условиях реализации угроз нарушения целостности информации может быть адаптирован применительно к интернету медицинских вещей (IoMT) различного назначения.

Практическая ценность результатов:

– разработанная методика оценки риска облегчит работу экспертов, занимающихся оценками риска носимых устройств интернета вещей, поскольку данные параметры просты в оценке и учитывают векторы атак на носимые устройства интернета вещей, в условиях реализации угроз нарушения целостности информации;

– разработанная методика получения числовой оценки риска для носимых устройств интернета вещей обладает широкими возможностями и позволяет адаптировать ее к уже имеющимся методикам оценки риска путем модернизации нечеткой сети;

– результаты применения алгоритма ранжирования по степени защищенности для носимых устройств интернета вещей могут помочь потребителю с выбором более безопасного устройства с целью повышения эффективности его эксплуатации в условиях реализации угроз целостности информации.

Список литературы

1. Skarmeta A. A decentralized approach for security and privacy challenges in the internet of things. // Internet of Things (WF-IoT). 2014. P. 67-72.

2. The Internet of things is the basis of the new economy. URL: https://www.pcweek.ru/iot/article/ detail.php?ID=182807 (дата обращения: 20.07.2022).

3. Кучерявый А.Е. Интернет вещей. / А.Е. Кучерявый. // Электросвязь. 2013. № 1. С. 21-24.

4. Rghioui A. The internet of things for healthcare monitoring: Security review and proposed solution. // Information Science and Technology (CIST). 2014. P. 384-389.

5. Primova H. Approaches to solving the problem of risk assessment with fuzzy initial information. / H. Primova, D. Sotvoldiev, L. Safarova. // Dynamics of Systems. 2018. P. 137-150.

6. Zhu W. A security and privacy model for mobile RD systems in the internet of things. // Communication Technology (ICCT). 2012. P. 726-732.

7. I. Erguler, A potential weakness in R-D-based internet-of-things systems, Pervasive and Mobile Computing. URL: http://www.sciencedirect.com/science/ article/pii/S1574119214001825 (дата обращения: 20.07.2022).

8. Vucinic M. Oscar: Object security architecture for the internet of things. 2014. P. 3-22.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 22.07.2022

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, начальник отдела, Концерн «Созвездие», e-mail: s.a.ermakov@sozvezdie.su

Щетинина Ирина Владимировна – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Болгов Андрей Александрович – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

DEVELOPMENT OF AN ALGORITHM FOR RANKING WEARABLE DEVICES OF THE INTERNET OF THINGS ACCORDING TO THE DEGREE OF SECURITY BASED ON RISK ANALYSIS IN THE CONTEXT OF THE IMPLEMENTATION OF THREATS TO THE INTEGRITY OF INFORMATION

S.A. Ermakov, I.V. Shetinina, A.A. Bolgov, E.A. Moskaleva

This article proposes an algorithm for ranking wearable devices of the Internet of Things according to the degree of security based on risk analysis in the context of the implementation of threats to the integrity of information. The paper developed a risk assessment methodology that takes into account the vectors of attacks on wearable Internet of Things devices in the context of threats to integrity violations, as well as a methodology for obtaining a quantitative risk assessment based on the parameters obtained. When using the results of the results obtained, the security of the Internet of Things wearable devices presented in this paper was calculated. Based on the values obtained, their ranking was performed. The results of the work done will increase the security of wearable devices of the Internet of Things, simplify their development and implementation, taking into account security in the context of the implementation of threats of integrity violations

Keywords: Internet of things, wearable devices, security, risk, attack.

Submitted 22.07.2022

Information about the authors

Sergey A. Ermakov – Cand. Sc. (Technical), Head of Department, Concern «Sozvezdie», e-mail: s.a.ermakov@sozvezdie.su

Irina V. Shetinina – student, Voronezh State Technical University, email: mnac@comch.ru

Andrey A. Bolgov – graduate student, Voronezh State Technical University, e-mail: mnac@comch.ru

Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: mnac@comch.ru