DOI 10.36622/VSTU.2023.26.1.007
УДК 004.733

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ РЕАЛИЗАЦИИ АТАКИ «SINKHOLE» НА БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ, СОСТОЯЩИЕ ИЗ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, Ю.А. Ермаченко, А.А. Болгов, В.Н. Кострова, А.А. Сиделев

В данной статье предлагаются методики количественной оценки и регулирования рисков успешной реализации атаки «Sinkhole», направленной на нарушение конфиденциальности, целостности и доступности данных и влияющей на жизненно важные для сетей Интернета вещей показатели – энергоэффективность и пропускную способность устройства на этапе проектирования системы. Данная методика основана на применении четырехслойной риск модели, как оптимальном способе оценки риска. Разработаны алгоритмы для количественной оценки риска и регулирования рисков на этапе начала эксплуатации системы. Они основаны на получении информации об уязвимостях из публичных источников – реестров уязвимостей, экспертных оценок. Представлен программный инструментарий, для сравнения конфигурации сети, который позволяет выбирать и сравнивать различные наборы мер и средств защиты сети и устройств в соответствии с предложенными методиками и алгоритмами оценки и регулирования рисков, как итог, выбрать наиболее оптимальную относительно риска и используемых материальных ресурсов для использования конфигурацию с точки зрения риска успешной реализации атаки «Sinkhole».

Ключевые слова: Интернет вещей, беспроводная сенсорная сеть, риск, экспертные оценки, четырехслойная риск модель, энергоэффективность, защищенность.

Введение

В настоящее время технологии Интернета вещей становятся все более популярными: бизнес-процессы активно модернизируются технологиями контроля качества; выполняется мониторинг работы персонала и удаленного управления производством; граждане используют устройства Интернета вещей для автоматизации повседневных бытовых задач и отслеживания состояния своего здоровья; государственные органы внедряют «умные» устройства в системы документооборота и так далее [1].

Особую роль в разнообразии сетей Интернета вещей имеют беспроводные сенсорные сети (Wireless Sensor Networks далее – WSN). Эта технология стремительно развивается, потому что имеет широкий спектр применения в гражданской и военной промышленности, например, в сельскохозяйственных учреждениях для контроля состояния растений и животных, в военном деле для управления группами войск и техники, а также слаживания различных подразделений [2]. Беспроводные сенсорные сети, включающие устройства Интернета вещей, могут состоять из тысяч миниатюрных сенсорных узлов с ограниченными энергетическими и вычислительными ресурсами, а также из базовых станций, которые используются для мониторинга и управления сетью. В связи с тем, что узлы сети, как правило, располагаются в недружественной среде, они уязвимы к различным атакам маршрутизации.

При анализе существующих алгоритмов и методик, связанных с анализом и регулированием риска успешной реализации атаки в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей, были выявлены следующие противоречия [3]:

– между необходимостью оценки рисков реализации атаки «Sinkhole» на беспроводные сенсорные сети (WSN), состоящих из устройств Интернета вещей, и отсутствием методического обеспечения для этой задачи;

– между необходимостью регулирования рисков успешной атаки «Sinkhole» в беспроводных сенсорных сетях (WSN), состоящих из устройств Интернета вещей, и отсутствием методического обеспечения для этой задачи;

– между необходимостью автоматизировать оценку и регулирование риска успешной реализации атаки «Sinkhole» в беспроводных сенсорных сетях (WSN), состоящих из устройств Интернета вещей, и отсутствием программного обеспечения для этой задачи.

Объектом в данной работе являются беспроводные сенсорные сети (WSN), состоящие из устройств Интернета вещей, атакуемые DoS «Sinkhole».

Предметом в данной работе выступают оценка и регулирование рисков нарушения безопасности информации при реализации атаки «Sinkhole» на беспроводные сенсорные сети (WSN), состоящие из устройств Интернета вещей.

Целью проведенного исследования является повышение защищенности беспроводных сенсорных сетей (WSN), состоящих из устройств Интернета вещей, за счет создания инструментария оценки и регулирования рисков реализации атаки «Sinkhole».

Для эффективного достижения обозначенной выше цели были решены следующие задачи:

– разработка методического и алгоритмического обеспечения оценки рисков успешной реализации атаки «Sinkhole» на беспроводные сенсорные сети (WSN), состоящие из устройств Интернета вещей;

– разработка методического и алгоритмического обеспечения регулирования рисков успешной реализации атаки «Sinkhole» на беспроводные сенсорные сети (WSN), состоящие из устройств Интернета вещей;

– создание программного комплекса по методическому и алгоритмическому обеспечению оценки и регулирования рисков, включающего оценку эффективности по критерию увеличения защищенности/снижения риска.

Оценка риска на этапе проектирования системы:

Эмпирическим способом для оценки риска была выбрана четырехслойная риск-модель, как наиболее подходящая для количественной оценки риска в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей. Релевантность оценок, получаемых в результате применения данной методики, легко подтверждается соответствующими практическими экспериментами в источнике [4].

В данной работе для оценки рисков успешной реализации атаки «Sinkhole» в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей, применяется методика анализа иерархий риска (МАИР) с четырьмя слоями: риск, требования, атаки и конфигурации. Рассмотрим слои МАИР (рис. 1):

- Риск: этот слой содержит единственный узел, представляющий величину риска, который является результатом, вычисляемым на основе нижних слоев.
- Требования: этот слой содержит четыре узла, которые представляют собой критически важные для данного типа сетей характеристики, определяющие требования к безопасности сети: энергоэффективность, конфиденциальность, целостность, доступность и пропускная способность.
- Атаки: этот слой содержит атаки, которые могут оказать влияние на свойства, перечисленные в слое требований. В данной работе на этом слое будут находится шесть атак, которые наиболее разрушительны для беспроводных сенсорных сетей. Они оказывают основное воздействие на маршрутизацию.
- Настройки: этот слой содержит элементы, которые определяют информацию, которую нарушитель может использовать для реализации некоторых атак, а именно настройки устройств или сети, при необходимости его можно расширить.

Особое внимание нужно уделить требованиям энергоэффективности и пропускной способности так как они являются критически важными для этого типа сетей. В сети Интернета вещей

сенсорные узлы потребляют энергию во время передачи и приема пакетов данных [5]. Таким образом эффективное использование энергии сенсорными узлами обеспечивается в том числе и с помощью протоколов маршрутизации.

Для расчета вероятности наступления ущерба успешной реализации атаки «Sinkhole» в беспроводных сенсорных сетях (WSN), состоящих из устройств Интернета вещей необходимо вычислить отношение оценки уязвимости устройства, вычисляемое по методике анализа иерархий риска, и максимально возможной оценки уязвимости для исследуемой системы:

$$IPOC(dev) = \frac{I(dev)}{W_{gMAX} \times D \times W_r},$$

где $I(dev)$ – оценка уязвимости устройства;

W_{gMAX} – вектор максимальных приоритетов конфигураций;

D – матрица воздействия атак;

W_r – вектор приоритетов критических параметров.

В используемой методологии существует еще одно нововведение – учет стоимости узла в отношении всей сети при вычислении ущерба. Это необходимо из-за специфики протокола RPL [6], наиболее перспективного для использования, в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей. Данный протокол создает из подключенных узлов DODAG (ориентированный на назначение ациклический граф) в виду чего при успешной реализации атак маршрутизации высока вероятность того, что все дочерние узлы будут недоступны. Учитывая этот фактор стоимость узла включает в себя себестоимость узла и стоимость его дочерних узлов, то стоимость шлюза, как вершины графа, будет эквивалентна стоимости всей беспроводной сети. В связи с этим метрика ущерба рассчитывается так:

$$U(dev) = \frac{Cost(dev)}{Cost(Getway)},$$

где $Cost(dev)$ – стоимостная характеристика целевого узла;

$Cost(Getway)$ – стоимостная характеристика шлюза.

Мера риска, возможного от успешной реализации атаки через исследуемый узел в масштабах исследуемой гомогенной беспроводной сенсорной сети, состоящей из устройств Интернета вещей, через целевой узел вычисляется как произведение вероятности наступления ущерба на ущерб:

$$Risk(dev) = IPOC(dev) \times U(dev),$$

где $IPOC(dev)$ – вероятность наступления ущерба реализации атаки «Sinkhole» через целевой узел;

$U(dev)$ – ущерб от реализации атаки «Sinkhole» через целевой узел.

Регулирование риска на этапе проектирования системы:

Уязвимости релевантны архитектуре беспроводных сенсорных сетей, состоящих из устройств Интернета вещей, распределяются по трем уровням [7]:

- Прикладной уровень: это уязвимости аппаратной части узлов – сенсоров, маршрутизаторов и шлюзов.
- Сетевой уровень: это уязвимости протоколов маршрутизации.
- Представляющий уровень: это уязвимости программного обеспечения и приложений, использующихся на устройствах.

Меры и средства защиты информации в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей, разделяются на [8]:

- Меры и средства защиты от физического доступа – направлены на создание препятствий нарушителей на путях к защищаемой информации, например, на территорию, на которой располагаются объекты информатизации, в помещение с аппаратурой, носителями данных или обеспечивают контроль такого доступа.
- Средства защиты от непосредственного виртуального доступа и воздействия вредоносными программами – направлены на исключение или затруднение проникновения нарушителя с использованием программных средств в операционную систему вычислительного устройства и на защиту операционной среды от вредоносных программ.
- Меры защиты информации от несанкционированного доступа, обусловленного применением сетевых технологий взаимодействия – направлены на исключение или затруднение проникновения нарушителя в операционную систему информационной системы с использованием протоколов межсетевого взаимодействия.

Применение мер и средств защиты информации в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей, предлагается разделить на следующие категории:

- Узловые – способы защиты, применяемые индивидуально к выбранному узлу.
- Кластерные – способы защиты, применяемые к определенным кластерам сети. Под кластером понимается группа узлов, объединенных или проранжированных по какому-либо признаку или характеристикам.
- Общесетевые – способы защиты, применяемые ко всем узлам без исключения.

Критерием эффективности методологии и алгоритма регулирования риска в беспроводной сенсорной сети, состоящей из устройств Интернета вещей, является снижение риска успешной реализации атаки «Sinkhole».

Распределение приоритета узлов для применения мер и средств защиты осуществляется по более высокому уровню кластера. Кластеры представляют собой:

Уровень 1 – наименее важный узел с точки зрения необходимости защиты, потому что к нему физически трудно получить доступ и топологически узел не важен, потому что не является ключевым в графе.

Уровень 2 – чуть более важный узел с точки зрения необходимости защиты, потому что к нему физически легко получить доступ, но топологически он не является ключевым в графе.

Уровень 3 – важный узел с точки зрения необходимости защиты, потому что к нему физически трудно получить доступ, но топологически он является ключевым в графе.

Уровень 4 – самый важный узел с точки зрения необходимости защиты, потому что к нему физически легко получить доступ и топологически он является ключевым в графе.

Группа узлов с наибольшим уровнем приоритета оборудуются мерами и средствами защиты раньше остальных.

Алгоритм регулирования риска успешной реализации атаки «Sinkhole» в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей (рис. 1):

Шаг 1: Оценка рисков для существующей конфигурации информационной системы.

Шаг 2: Ранжирование узлов сети по четырем предложенным кластерам.

Шаг 3: Устанавливаются общесетевые меры защиты информации.

Шаг 4: Проверка наличия доступных средств для установки индивидуальных и кластерных средств защиты. Если средства в наличии происходит переход на Шаг 5, если нет – Шаг 6.

Шаг 5: Средства защиты устанавливаются на узлы незащищенного кластера с максимальным приоритетом. Переход на Шаг 4.

Шаг 6: Оценка риска информационной системы с установленными мерами и средствами защиты.

Шаг 7: Сравнение значений риска, полученного до внедрения мер защиты и

значений риска после внедрения средств защиты.

Шаг 8: По результатам сравнения значений рисков делаются выводы об эффективности примененных мер и средств защиты.

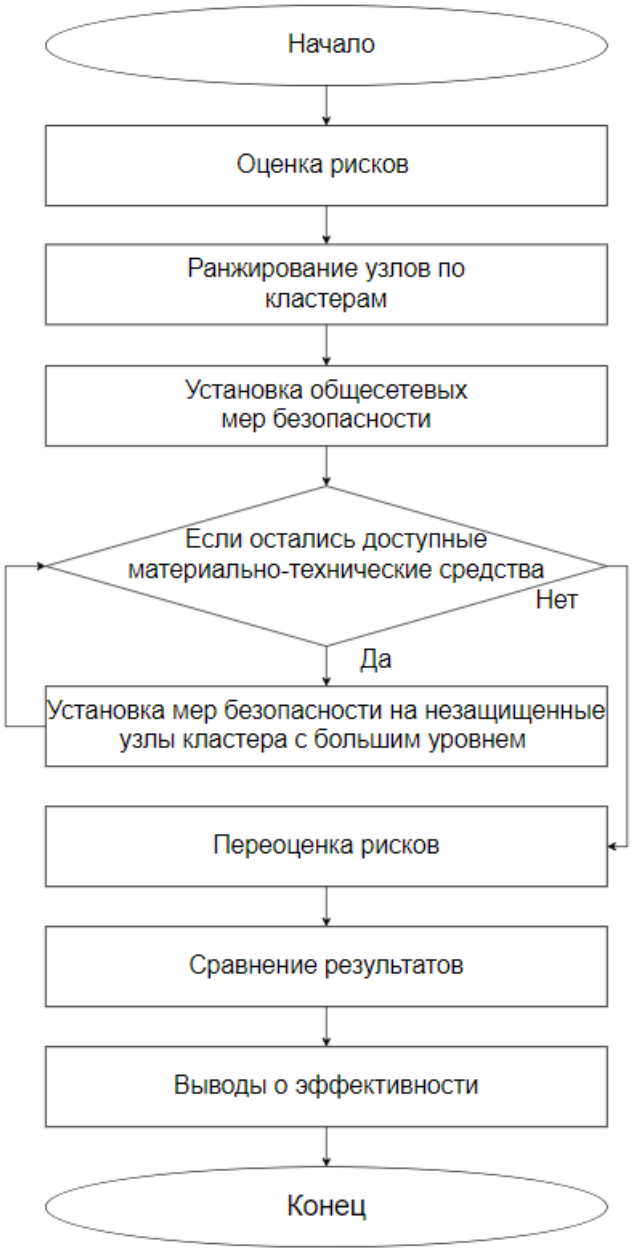

Рис. 1. Блок-схема алгоритма регулирования рисков

Программа для оценки и регулирования рисков проектируемой сети

Для автоматизации оценки и регулирования рисков успешной реализации атаки «Sinkhole» была создана программа (рис. 2). Программа выгружает информацию об существующих уязвимостях из базы данных SQLite3. В ней содержится идентификатор из БДУ ФСТЭК [9], дата обнаружения, опасность CVSS3, частота возникновение, описание уязвимости и т.д. В окне программы существуют четыре вкладки, при запуске программы три из четырех вкладок являются неактивными, активна только вкладка «Уязвимости». Во вкладке уязвимости происходит получение данных из файла базы данных. После чего активируются остальные вкладки. Во вкладке «Атаки» пользователю предоставляется возможность

задать матрицу влияния каждой атаки на параметры сети в соответствии с иерархической моделью. Во вкладке «Меры и Средства защиты» пользователю предоставляется указать какие меры и средства защиты используются в оцениваемой сети, в окне они разделены на категории, которые были описаны выше. Во вкладке «Расчет» пользователю необходимо указать стоимость узла, который является объектом атаки и стоимость шлюза, который ввиду специфики топологии является отражением стоимости всей сети. Далее заполняются вектора приоритетов, если пользователь не заполнит их, то будут установлены усредненные значения по умолчанию. После проведения всех приготовлений необходимо нажать на кнопку «Рассчитать» и программа, используя веденые данные произведет вычисления значения меры риска в соответствии с предложенной методикой и по описанному выше алгоритму. Оценка эффективности используемых мер, проводится путем сравнения значений в поле «Риск» - чем меньше значение, тем система более защищена.

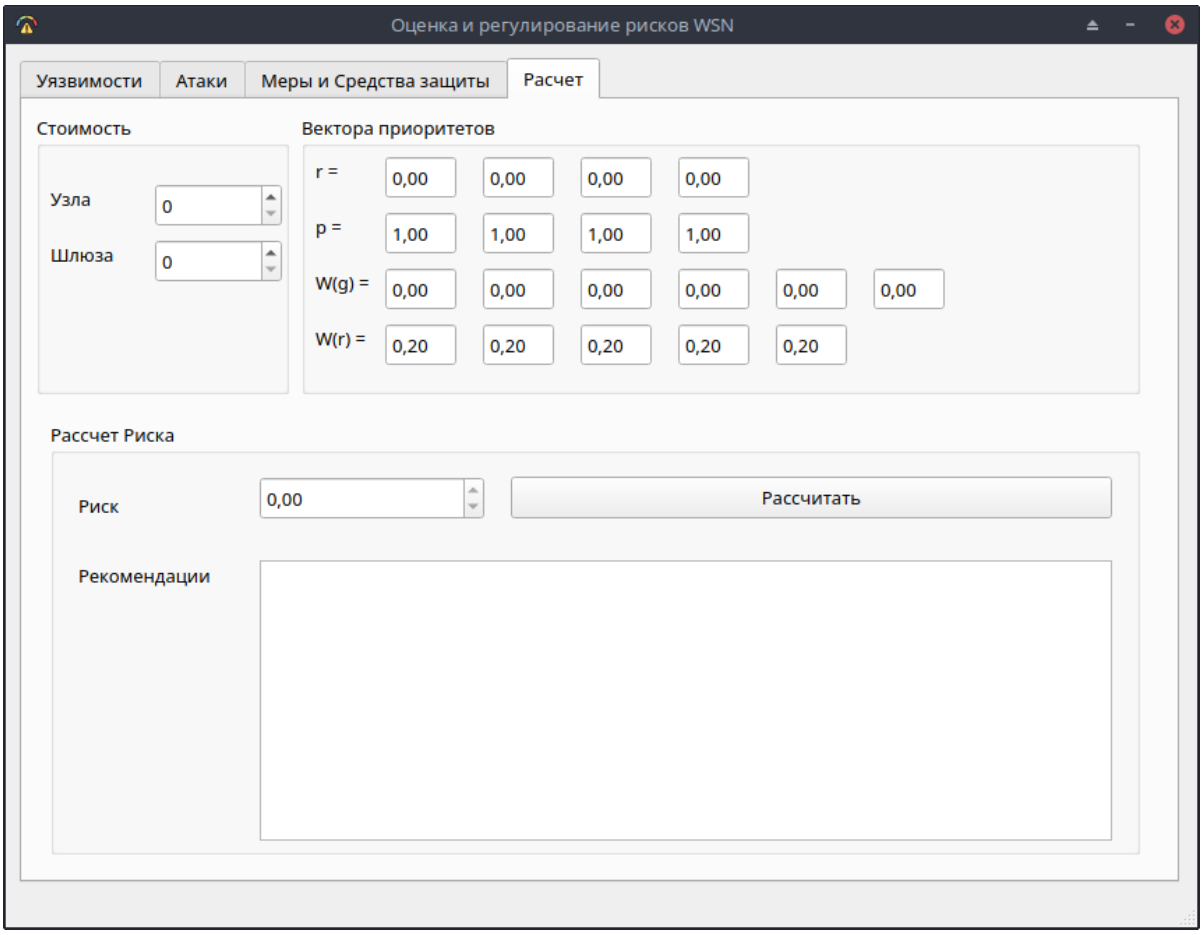

Рис. 2. Окно программы для оценки и регулирования рисков WSN

Заключение

Таким образом, по результатам проделанной работы можно сделать вывод о том, что предложенное методическое и алгоритмическое обеспечение оценки рисков успешной реализации атаки «Sinkhole» в беспроводных сенсорных сетях (WSN), состоящих из устройств Интернета вещей, позволяет выявлять наиболее уязвимые участки в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей. В перспективе данное обеспечение может быть применено для беспроводных сенсорных устройств, состоящих из других типов устройств.

Предложенное методическое и алгоритмическое обеспечение регулирования рисков успешной реализации атаки «Sinkhole» в беспроводных сенсорных сетях, состоящих из устройств Интернета вещей, в

процессе применения повышает защищенность беспроводных сенсорных сетей от успешной реализации атаки «Sinkhole» и в дальнейшем поможет исследованию беспроводных сенсорных сетей.

Разработанный программный комплекс автоматизированной оценки и регулирования рисков успешной реализации атаки «Sinkhole» на беспроводные сенсорные сети, состоящие из устройств Интернета вещей, позволяет осуществлять оценку и регулирование риска в беспроводных сенсорных сетях и в дальнейшем может быть дополнено модулями для других типов атак маршрутизации.

Совокупность всех результатов работы является отправной точкой в анализе и регулировании рисков в слабо исследованной области беспроводных сенсорных сетей, состоящих из устройств Интернета вещей. Существует уверенность, что данная тема получит развитие в дальнейших исследованиях, потому что беспроводные сенсорные сети – это перспективное направление не только как часть Интернета вещей, но и как технология в общем. Возможна гибридизация с другими видами сетей, такие как Mash – сети, которые тоже уже активно внедряются в военной и гражданской инфраструктуре.

Список литературы

1. K. L. Lueth. IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally. URL: https://iot- analytics.com/iot-platform- companies- landscape2020/. Accessed: 2020-04-09 (дата обращения 14.01.23).

2. Detection and Isolation Technique for Sinkhole Attack in WSN / Urvashi Dhaked, Dr. Ashok Kumar, Dr. Brajesh Kumar Singh // Journal of University of Shanghai for Science and Technology.

3. Qi J. Detection and defence of Sinkhole attack in Wireless Sensor Network / J. Qi, T. Hong, K. Xiaohui, L. Qiang // Communication Technology (ICCT), 2012. IEEE 14th International Conference on, 2012, pp. 809-813.

4. Щербаков В.Б. Риск-анализ атакуемых беспроводных сетей: монография / В.Б. Щербаков, С.А. Ермаков, Н.С. Коленбет; под ред. чл.-корр. РАН Д.А. Новикова. Воронеж: Научная книга, 2013. 160 с.

5. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. Internet of things (IoT) security: Current status, challenges and prospective measures // 2015 10th International Conference for Internet Technology and Secured Transactions(ICITST). IEEE. 2015. P. 336–341.

6. RPL. URL: https://en.wikipedia.org/wiki/RPL_(IPv6_Routing_Protocol_for_LLNs) (дата обращения 14.01.23).

7. Vashi S. Internet of Things (IoT): A vision, architectural elements, and security issues / S. Vashi, J. Ram, J. Modi, S. Verma, C. Prakash. // 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE. 2017, pp. 492–496.

8. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография. Воронеж: Кварта, 2018. 588 с.

9. БДУ – Уязвимости. [сайт ФАУ ГНИИ ПТЗИ ФСТЭК России] URL: https://bdu.fstec.ru/vul (дата обращения 14.01.23).

Концерн «Созвездие»
Concern «Sozvezdie»

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 21.01.2023

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, начальник отдела, Концерн «Созвездие», e-mail: mnac@comch.ru

Ермаченко Юрий Александрович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

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

Кострова Вера Николаевна – д-р техн. наук, профессор, Воронежский государственный технический университет», e-mail: mnac@comch.ru

Сиделев Алексей Ахмадович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

ASSESSMENT AND REGULATION OF THE RISKS OF IMPLEMENTING «SINKHOLE» ATTACKS ON WIRELESS SENSOR NETWORKS CONSISTING OF INTERNET OF THINGS DEVICES

S.A. Ermakov, Y.A. Ermachenko, A.A. Bolgov, V.N. Kostrova, A.A. Sidelev

This article proposes methods for quantifying and managing the risks of a successful «Sinkhole» attack aimed at violating confidentiality, integrity and availability of data and affecting vital indicators for the Internet of Things networks – energy efficiency and device throughput at the system design stage. This technique is based on the use of a four-layer risk model as the optimal way to assess risk. Algorithms have been developed for quantitative risk assessment and risk management at the start-up stage of the system. They are based on obtaining information about vulnerabilities from public sources – vulnerability registries, expert assessments. A software toolkit is presented to select the optimal network configuration, which allows you to select and compare different sets of measures and means of protecting the network and devices in accordance with the proposed methods and algorithms for risk assessment and management, as a result, to choose the most optimal configuration for use in terms of the risk of successful implementation of the «Sinkhole» attack.

Keywords: Internet of things, wireless sensor network, risk, expert assessments, four-layer risk model, energy efficiency, security.

Submitted 21.01.2023

Information about the authors

Sergey A. Ermakov – Cand. Sc. (Technical), Head of Department, Concern «Sozvezdie», e-mail: mnac@comch.ru

Yurii A. Ermachenko – student, Voronezh State Technical University, e-mail: mnac@comch.ru

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

Vera N. Kostrova – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Alexey A. Sidelev – student, Voronezh State Technical University, e-mail: mnac@comch.ru