**DOI 10.36622/VSTU.2022.25.4.003**
**УДК 004.735**

# НЕЧЕТКО-МНОЖЕСТВЕННАЯ МЕТОДИКА ОЦЕНКИ РИСКОВ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ «УМНЫЙ ДОМ» С ДИНАМИЧЕСКОЙ ТОПОЛОГИЕЙ

**С.А. Ермаков, А.Г. Чурсин, А.А. Болгов**

Рост числа новых устройств на рынке «Интернета вещей» вынуждает пользователей с каждым подключением в систему нового устройства настраивать топологию заново, причем эту проблему можно решить внедрением динамической топологии, однако в связи с широким распространением устройств интернета вещей растут и возможные риски безопасности систем, в том числе связанные с угрозой перехвата телекоммуникационного трафика. Цель работы – это повышение защищенности подсистемы обмена трафиком системы «Умный дом» с динамической топологией от атак, направленных на перехват трафика, посредством модернизации существующего методического обеспечения оценки и регулирования рисков. Предложена усовершенствованная методика оценки рисков для автоматизированной системы с динамической топологией. В качестве дополнительного параметра для оценки риска добавлен нечетко-множественный показатель доступности. Повышена объективность оценок рисков, что позволило точнее оценить безопасность системы. Рассчитан риск во время атаки на сеть с показателем доступности и доказана актуальность данного параметра. Разработаны методические рекомендации к построению безопасной автоматизированной системы «Умный дом». Использование данных рекомендаций повысило защищенность автоматизированной сети от атак.

Ключевые слова: нечеткая логика, риск, динамическая топология, количественная оценка, безопасность, Интернет вещей.

## Введение

С появления на рынке первых устройств Интернета вещей прошло более 15 лет, за это время в мире было произведено и подключено свыше 8 миллиардов устройств, функционирующих в рамках концепции Интернета вещей. В настоящее время рынок Интернета вещей продолжает стремительно развиваться и становиться всё доступнее для населения [1, 2]. Уже к 2030 году аналитики прогнозируют увеличение количества «умных» устройств, которых в мире будет насчитываться более 24 миллиардов [3].

Расширение рынка Интернета вещей, привлекает к этой отрасли злоумышленников, целью которых является получение несанкционированного доступа к данным, что, в свою очередь, приводит к нарушению информационной безопасности систем, в архитектуре которых используются «умные» устройства. Только на 2021 год приходится свыше 20 миллиардов украденных персональных данных, опубликованных на теневых форумах [4].

Уязвимости подсистемы передачи данных в автоматизированной системе «Умный дом» можно классифицировать по источникам: уязвимость каналов передачи данных, незащищенность узлов сети, использование динамической топологии, отсутствие четкой инфраструктуры. Вышеописанные уязвимости, открывают пространство для реализации атак: направленных на нарушение конфиденциальности, целостности и доступности информации. В зависимости от характера воздействия все атаки на АС можно разделить на пассивные и активные.

В данной работе рассматривается потенциальный нарушитель, т.е. субъект АС «Умный дом», со средним или высоким уровнем квалификации, мотивацией которого является получение собственной выгоды. Состав информационной системы включает в себя набор устройств и протоколов, использующихся для функционирования автоматизированной системы.

В условиях недостатка статистики, одним из немногих решений при использовании подхода управления рисками на практике является, применение нечеткой логики как расширение экспертного метода.

Преимущество подхода, основанного на применении нечеткой логики, заключается в более высокой точности и меньшей зависимости от субъективного мнения экспертов. Данный подход позволяет применять объективные данные (например, параметры передаваемых данных, характеристики уязвимостей и т.д.) и получать на выходе нечетких алгоритмов конкретные численные значения [5, 6].

**Методика оценки рисков для АС «Умный дом»**

Анализ рисков информационной безопасности любой информационной системы невозможен без применения математического аппарата оценки и управления рисками.

Риск может быть найден как произведение величины ущерба на вероятность наступления данного ущерба.

$$Risk = Ut \times P(Ut), \quad (1)$$

где $Ut$ – ущерб от реализации атак, $P(Ut)$ – вероятность наступления ущерба $Ut$.

Данная формула является объективной и может служить основой для создания методической базы оценки и управления рисками [7]. Как было сказано ранее, математический аппарат оценки и управления рисками не может быть применен в исходном виде для информационных систем с динамической топологией. Далее представлена модель, учитывающая специфику данного класса систем. В формуле (1) положим $Ut=W$, тогда стандартная формула расчета риска примет следующий вид:

$$Risk = W \times p(W), \quad (2)$$

где $p(W)$ – вероятность наступления ущерба $W$, $W$ – величина ущерба.

Пользователь системы может получить ущерб вследствие успешного перехвата трафика субъектом рассматриваемой информационно-управляющей системы. Ущерб наносится системе посредством атаки.

В связи с этим формула (2) принимает следующий вид:

$$Risk = P \times W,$$

где $P$ – множество вероятностей реализации атак, $W$ – величина ущерба.

Принимается, что в конкретный момент времени злоумышленник осуществляет только одну атаку. Атака направлена на получение конкретного типа данных. В результате вероятности атаки являются независимыми величинами, что позволяет построить следующую формулу вычисления риска:

$$Risk = \frac{n!}{n_0! \times \ldots \times n_k!} \times \prod p_i^{n_j} \times (n_0 + \ldots + n_k)W,$$

где $n_k$ – количество успешных атак на $k$-й объект, через который проходит трафик с защищаемыми данными, $p_i^{n_j}$ – вероятность успешной реализации $i$-й атаки на $j$-м объекте, $W$ – ущерб от получения злоумышленником данных.

Данная модель представляет собой многомерное распределение вероятностей осуществления ряда атак, актуальных для системы. При осуществлении атаки злоумышленник может получить доступ к сразу нескольким типам данных, что увеличит возможный ущерб.

При составлении первичного методического обеспечения предлагается использовать следующие вероятностные величины: $p_0$ – вероятность отсутствия атаки; $p_1$ – вероятность атаки прослушивания и анализа трафика; $p_2$ – вероятность атаки на протокол обмена ключами шифрования; $p_3$ – вероятность атаки на процесс аутентификации устройств в сети; $p_4$ – вероятность атаки с подключением фиктивного устройства; $p_5$ – вероятность иных атак.

Поскольку некоторые атаки, направленные на перехват трафика, предусматривают проведение деаутентификации с зашумлением либо временным отключением каналов связи, разумно включить в модель показатель доступности. Данный показатель будет рассчитываться как для устройств, так и для линий связи.

Динамический характер системы вызывает необходимость вычисления показателей доступности в том числе для потенциальных линий связи - на случай изменения топологии. Объём вычислений возможно сократить путем введения единого показателя доступности для всех потенциальных линий связи.

В целях получения численных значений для оценки вероятности реализации угроз применим аппарат нечеткой логики.

Таким образом, формула расчёта оценки вероятности реализации конкретной угрозы может принять следующий вид (3) для модели без учёта параметра доступности и вид (4) для модернизированной модели учитывающей доступность:

$$p_i = Defuzz(Fuzz(h_i) \times Fuzz(a_i) \times Fuzz(v_i) \times Fuzz(N)), \quad (3)$$

$$p_i = Defuzz(Fuzz(h_i) \times Fuzz(a_i) \times Fuzz(v_i) \times Fuzz(N) \times Fuzz(A)), \quad (4)$$

где $p_i$ – вероятность успешной реализации $i$-й угрозы, *Defuzz* – операция дефаззификации нечеткого значения, *Fuzz* – операция фаззификации оценочного значения, $h_i$ – оценка сложности реализации $i$-й угрозы, $a_i$ – оценка привлекательности информационных активов, на получение доступа к которым направлена $i$-я угроза, $v_i$ – показатель наличия уязвимостей, необходимых для реализации $i$-й угрозы, в том числе уязвимостей реализованных в системе механизмов динамической топологии, $N$ – показатель важности конкретного элемента системы, выраженный в отношении проходящего через элемент трафика к общему трафикусистемы, $V$ – показатель доступности элементов системы.

Специфика информационных систем с динамической топологией учитывается в параметре $vi$. Кроме этого, вычисление значения риска на временном промежутке также позволит более корректно отобразить динамический характер системы.

Результатом вычислений, в том числе посредством нечеткой математики, является двумерная матрица вероятностей (5) реализации угроз информационной безопасности на объектах системы, представляющих собой устройства либо каналы связи.

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{i1} & \cdots & p_{in} \end{pmatrix}, \quad (5)$$

В рамках столбца представляется информация о вероятностях атак на конкретный объект системы, в рамках строк - информация о вероятности осуществления конкретной атаки для каждого объекта системы.

Чтобы из матрицы вероятностей (5) получить матрицу рисков, необходимо каждый элемент матрицы умножить на значение ущерба. Для получения интегрального значения риска можно воспользоваться способами, приведенными в работе [8], с некоторыми изменениями, учитывающими специфику и направленность данной работы в сравнении с исходной. Следует учесть следующие положения:

– исходные способы получения интегрального значения предусматривают наличие однотипных элементов таблицы. В составленной матрице присутствуют не только устройства, но и каналы связи;

– наличие разнотипных элементов таблицы вызывает необходимость вывода интегральных значений риска как минимум для каждого типа объектов;

В таком случае матрица рисков приобретает следующий вид:

$$R = \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{i1} & \cdots & r_{in} \end{pmatrix}$$

**Результаты**

Для проверки актуальности нечеткой переменной, обозначающей доступность каналов связи и элементов системы, проверяются возможности расчета рисков для системы при проведении следующих операций:

– атака длится 30 секунд. В промежуток с 5 по 15 секунду производится зашумление канала связи. После этого доступность восстанавливается, а в 20 секунду злоумышленник получает контроль над одним из устройств в составе системы;

– атака длится 30 секунд. В 20 секунду злоумышленник получает контроль над одним из устройств в составе системы.

На рис. 1 и 2 по оси X определяется время в секундах, по оси Y – значение риска.

Как видно из рис. 1 и 2, нечеткую переменную доступности каналов связи и элементов системы для атаки необходимо учитывать в модели, поскольку, с учетом данного параметра, пользователь системы может получить больше информации о негативном воздействии на систему.

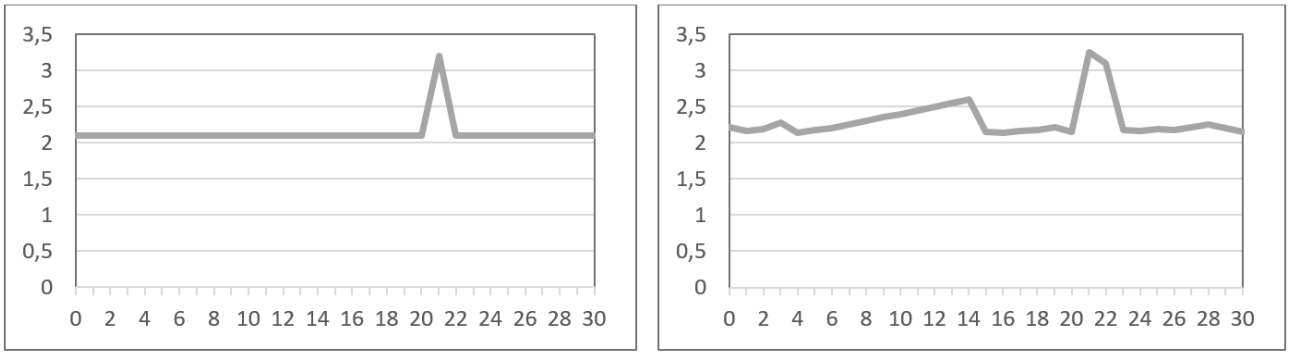


Рис. 1. (a) График значений риска без нечеткой переменной доступности, для атаки, которая влияет на доступность. (b) График значений риска с наличием нечеткой переменной доступности, для атаки, которая влияет на доступность.

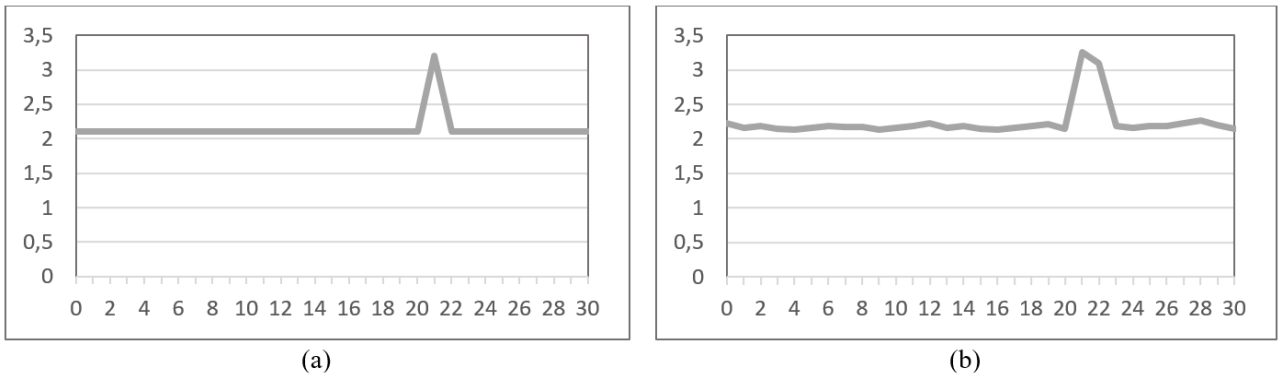


Рис. 2. (a) График значений риска без нечеткой переменной доступности, для атаки, которая не влияет на доступность. (b) График значений риска с наличием нечеткой переменной доступности, для атаки, которая не влияет на доступность.

**Управление рисками**

В процессе исследования эффективности разработанного методического обеспечения произведено сравнение работоспособности вышеуказанного обеспечения с работоспособностью архитектуры безопасности, представляющей собой эшелонированную защиту информационной системы. На основе результатов исследования эффективности разработан набор рекомендаций по построению архитектуры безопасности информационных систем, построенных на базе концепции Интернета вещей:

• Средства защиты информации в системе должны быть встроенными и автоматическими, требующие минимальных усилий по настройке со стороны владельца системы.

• Защита системы обязательно должна включать в себя модули обеспечения безопасности трафика и механизмы защиты информации при обмене криптографическими ключами.

• При обнаружении уязвимостей существующих механизмов обеспечения безопасности либо системного ПО устройств должно производиться обновление системы в

соответствии с рекомендациями производителя.

- При использовании встроенных мер защиты открывается перспектива применения машинного обучения для обнаружения отклонений в работе сети.
- Максимального эффекта от методического обеспечения оценки и управления рисками можно добиться только в комбинации с иными защитными мерами.
- Для предупреждения пассивных атак на трафик, требуется установка специального радиоприемного устройства и настройка его на диапазон работы беспроводной сети с дальнейшим подключением к головному узлу системы в целях оповещения владельца системы.

**Заключение**

В результате разработки методического обеспечения оценки и регулирования рисков информационной безопасности АС «Умный дом» усовершенствован подход к обеспечению безопасности данных, циркулирующих в информационной системе, путём включения нового параметра доступность, который отражает чувствительность элементов АС к атакам, направленным на перехват трафика или отключение каналов и устройств, входящих в состав IoT-сети.

Разработанная модель имеет ряд преимуществ перед моделью с эшелонированной защитой: учитываются каналы связи, динамический характер системы, снижен объем вычислений. Применение аппарата нечетко-множественной логики уменьшило субъективность экспертных оценок. Дальнейшие развитие полученного методического обеспечения заключается в оценки рисков для реальной IoT-сети «Умный дом».

Главным отличием данного исследования является возможность применения методического обеспечения в сетях с динамической топологией, так как для сетей, построенных по концепции Интернета Вещей быстрое подключение и отключение компонентов обеспечивает удобство эксплуатации, а разработанная методика усиливает безопасность таких систем.

**Список литературы**

Mohan A., Cyber security for personal medical devices internet of things in Distributed Computing in Sensor Systems, 2014 IEEE International Conference. 2016. P. 372-374.

Carruthers K., Internet of Things and Beyond: Cyber-Physical Systems IEEE Internet of Things (IEEE Internet of Things, Newsletter, 2016). 2016. P. 62-64.

Алалван А.Р., Беляева Ю.А., Смирнова А.А., Российский рынок интернета вещей // Экономика и бизнес: теория и практика. 2017. Вып. 11. С. 6-10.

Liu X., Qian S., Hatcher G., Xu X., Liao W. IEEE Standard Access. 2019. No. **7.** P. 79523-79544.

Калашников А.О., Бугайский К.А., Аникина Е.В., Модели количественного оценивания компьютерных атак (часть1) // Информация и безопасность. 2019. Т. 22. Вып. 4. С. 517-528.

Sanchez S., Rotondo D., Escobet T., Puig V., Quevedo J., Annual Reviews in Control. 2019. No. 48. P. 103-128.

Остапенко А.Г., Радько Н.М., Калашников А.О., Остапенко О.А., Бабаджанов Р.К. Эпидемии в телекоммуникационных сетях // монография, под ред. Новикова Д.А. 2017. № 1. 282 с.

Ермаков С.А., Кунавин В.Е., Петрухненко К.Н. Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем // Информация и безопасность. 2020. Т. 18. Вып. 1. С. 97-111.

Концерн «Созвездие», г. Воронеж
Concern «Sozvezdie», Voronezh

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 14.11.2022

**Информация об авторах**

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

**Чурсин Андрей Германович –** аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru

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

# FUZZY-SET RISK ASSESSMENT METHODOLOGY OF THE AUTOMATED "SMART HOME" SYSTEM WITH DYNAMIC TOPOLOGY

**S.A. Ermakov, A. G. Chursin, A.A. Bolgov**

The growing number of new devices on the Internet of Things market forces users to configure the topology anew with each connection of a new device to the system, and this problem can be solved by introducing a dynamic topology, however, due to the widespread use of Internet of Things devices, possible security risks of systems are also growing, including those associated with the threat of interception of telecommunications traffic. The purpose of the work is to increase the security of the traffic exchange subsystem of the Smart Home system with a dynamic topology from attacks aimed at intercepting traffic by modernizing the existing methodological support for risk assessment and management. An improved risk assessment methodology for an automated system with a dynamic topology is proposed. A fuzzy multiple availability indicator has been added as an additional parameter for risk assessment. The objectivity of risk assessments has been increased, which made it possible to more accurately assess the security of the system. The risk during an attack on a network with an availability indicator is calculated and the relevance of this parameter is proved. Methodological recommendations for the construction of a secure automated system "Smart Home" have been developed. The use of these recommendations has increased the security of the automated network from attacks.

Keywords: fuzzy logic, risk, dynamic topology, quantitative assessment, security, Internet of Things.

Submitted 14.11.2022

**Information about the authors**

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

**Andrey G. Chursin –** graduate student, Voronezh State Technical University, e-mail: mnac@comch.ru

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