хранить семантику экспертных оценок. Такой подход повышает интерпретируемость интеллектуальных систем и облегчает их дальнейшее развитие и модификацию.

ЛИТЕРАТУРА

1. Dubois D., Prade H. Fuzzy sets and probability: misunderstandings, bridges and gaps // Proceedings of the 2nd IEEE International Conference on Fuzzy Systems (FUZZY'93). – San Francisco, CA, USA: IEEE, 1993. – P. 1059-1068.

2. Zadeh L. A. Fuzzy sets // Information and Control. – 1965. – Vol. 8. – P. 338-353.

3. Klir G. J., Yuan B. Fuzzy Sets and Fuzzy Logic: Theory and Applications. – Englewood Cliffs, NJ: Prentice Hall, 1995. – 592 p.

4. Zadeh L. A. The concept of a linguistic variable // Information Sciences. – 1975. – Vol. 8, No. 3. – P. 199-249.

5. Kosko B. Fuzzy Engineering. – Englewood Cliffs, NJ: Prentice Hall, 1997. – 400 p.

6. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – Upper Saddle River, NJ: Pearson, 2010. – 1132 p.

7. Аверкин А. Н., Батыршин И. З., Блишун А. Ф., Силов В. Б., Тарасов В. Б. Нечеткие множества в моделях управления и искусственного интеллекта. – М.: Наука, 1986. – 312 с.

УДК 004.056

С.А. Евдокимова, доц., канд. техн. наук,
В.С. Моисеев, асп.,
А.В. Скрыпников, зав. кафедрой ИБ, проф., д-р техн. наук
(ВГУИТ, г. Воронеж)

РАЗРАБОТКА ПРОГРАММНОГО ПРИЛОЖЕНИЯ ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИНТЕРНЕТА ВЕЩЕЙ

Современные корпоративные и промышленные сети всё чаще включают в себя устройства Интернета вещей (IoT), которые играют ключевую роль в автоматизации процессов, мониторинге окружающей среды, управлении доступом и повышении общей эффективности бизнеса. Однако массовое внедрение IoT сопровождается ростом угроз информационной безопасности: использование стандартных паролей, наличие уязвимых прошивок, открытые порты, нешифрованный трафик, отсутствие централизованного контроля и мониторинга [1-3].

Поэтому разработка программного приложения, предназначенного для комплексного управления информационной безопасностью IoT-устройств в локальных сетях, является актуальной.

Программное приложение реализовано на Python и позволяет:

– автоматически обнаруживать IoT-устройства в локальной сети;

– анализировать их безопасность (наличие открытых портов, дефолтных учётных записей, тип устройства);

– проводить проверку на наличие известных уязвимостей (на основе CVE по MAC-адресу и типу устройства);

– формировать отчёты о рисках и степени соответствия требованиям информационной безопасности;

– визуализировать сетевую карту с IoT-устройствами и их статусами безопасности.

Приложение разработано с учётом требований практического применения в корпоративной среде: его можно использовать в локальной сети без выхода в интернет, оно не требует установки агентов на устройства и не нуждается в Root-доступе, обеспечивая при этом интеграцию с существующей архитектурой.

Архитектура предлагаемого продукта построена по модульному принципу и включает следующие основные компоненты:

– модуль сканирования – отвечает за сетевое обнаружение устройств в заданном диапазоне IP-адресов. Он выполняет ARP- или Nmap-сканирование с последующим анализом MAC-адресов и активных портов. Модуль работает без необходимости root-доступа и адаптирован под условия локальной корпоративной сети. При сканировании определяются MAC-адреса, открытые TCP-порты, стандартные IoT-сигнатуры;

– модуль идентификации и классификации устройств. На основании MAC-префиксов и открытых портов производится предварительное определение типа устройства: IP-камера, маршрутизатор, датчик, медиаплеер и т.д. Дальнейшая классификация позволяет задать риск-профиль для конкретного класса оборудования;

– модуль проверки дефолтных учётных записей – осуществляет автоматизированный перебор популярных логинов и паролей по Telnet и HTTP Basic Auth. В случае удачного входа устройство помечается как уязвимое и подлежит приоритизации в отчётах;

– модуль CVE-проверки – для каждого устройства по определённому типу, модели или MAC-префиксу осуществляет поиск в открытых базах уязвимостей (например, NVD, CVE Details) [4, 5].

Информация используется для расчёта риска и генерации рекомендаций;

– модуль веб-интерфейса (frontend/backend). Пользовательский интерфейс реализован с использованием Flask. Он предоставляет доступ к результатам сканирования, позволяет запускать процедуры анализа, просматривать отчёты и выгружать данные в формате CSV;

– модуль оценки риска и соответствия стандартам – на основе полученной информации рассчитывает уровень риска для каждого устройства и сопоставляет его с требованиями стандартов ГОСТ 57580, ГОСТ Р 56939 и ISO/IEC 27001. Это позволяет оценить уровень соответствия устройств требованиям информационной безопасности в организации. Применяется балльная шкала по категориям (открытые порты, CVE, пароли), маркировка: низкий / средний / высокий риск.

Пример работы программы показан на рис. 1. Для оценки используется простая бальная система, за каждый критичный фактор начисляются баллы (например, 3 за дефолтный пароль, 2 за Telnet, 2 за CVE).

В зависимости от суммы выставляется уровень риска: 0-2 балла – низкий риск, 3-5 баллов – средний риск, 6 и выше – высокий риск. На основе этого уровня приложение формирует рекомендации: изоляция, обновление, смена пароля и т.д. Оценка запускается автоматически после сканирования и проверки устройства. Результат сохраняется в таблице и используется в отчётах и визуализации, пользователь может вручную задать весовые коэффициенты для каждого фактора риска.

Для удобства взаимодействия с результатами анализа безопасности IoT-устройств в разработанном приложении реализована система визуализации и генерации отчётов. Пользовательский интерфейс предоставляет сводную таблицу с результатами сканирования всех устройств, выявленных в локальной сети. Таблица содержит ключевую информацию (рис. 1): IP-адрес, MAC-адрес, открытые порты, тип устройства, наличие дефолтных учётных данных, уровень риска и количество обнаруженных уязвимостей. Каждое устройство можно выбрать для более детального анализа. При переходе к устройству отображается информация об идентифицированных уязвимостях (CVE), включая их идентификаторы, описания и базовые оценки риска (CVSS).

Также реализована возможность оценки соответствия каждого устройства требованиям стандартов информационной безопасности (ГОСТ Р 56939, ГОСТ 57580, ISO/IEC 27001). Нарушения отображаются в виде списка, формируемого автоматически. Дополнительно

предусмотрена функция генерации отчёта в формате CSV, который включает всю информацию по каждому устройству и может быть использован для хранения, анализа или передачи в системы централизованного аудита и SIEM-платформы.

Сканер сетевых устройств

Информация о вашей системе:

IPv4: 192.168.0.172

MAC-адрес: B4:2E:99:1A:16:04

Интерфейс: enp7s0

Платформа: Linux

Обнаруженные устройства:

IP	MAC	Порты	Тип	Дефолтные креды	Уровень риска
192.168.0.172	не найден	—	ПК	Нет	Низкий
192.168.0.1	78:8C:B5:ED:ED:5B	53, 80, 443	IoT-устройство	admin / admin	Высокий
192.168.0.162	B4:C9:B9:59:F2:39	—	Телефон Android	Нет	Низкий
192.168.0.195	62:74:28:A4:5A:49	—	Неизвестное устройство	Нет	Низкий
192.168.0.45	78:8B:2A:D5:BA:81	—	Телефон Iphone	Нет	Низкий
192.168.0.120	B8:87:6E:F6:32:30	443, 22	IoT-устройство	root / root	Низкий
192.168.0.219	78:8B:2A:DF:16:06	—	Телевизор	Нет	Низкий
192.168.0.103	92:9A:4A:07:B0:15	80, 443, 515	IoT-устройство	admin / admin	Средний
192.168.0.80	92:9A:4A:07:B0:15	80, 515	IoT-устройство	admin / admin	Средний
192.168.0.101	92:9A:4A:07:B0:15	—	Ноутбук	Нет	Низкий
192.168.0.188	D4:D2:D6:F7:28:C3	—	Телевизор	Нет	Низкий
192.168.0.192	74:56:3C:9D:06:55	21, 80, 443	IoT-устройство	user / 1234	Высокий
192.168.0.60	64:1C:AE:E9:8E:2A	—	Неизвестное устройство	Нет	Низкий

Рисунок 1 – Результат работы программного приложения

Таким образом, разработанное программное обеспечение позволяет сканировать корпоративную сеть, выявлять IoT-устройства, проверять их на наличие открытых портов и уязвимых сервисов, анализировать наличие дефолтных учетных записей, проводить оценку уязвимостей на основе актуальных данных и формировать профиль рисков для каждого устройства.

Среди преимуществ разработанного решения можно выделить его универсальность, модульную архитектуру, кроссплатформенность, а также возможность автономной работы в изолированных сетях без постоянного подключения к внешним источникам. Проведённое тестирование на реальных и виртуальных устройствах подтвердило работоспособность и эффективность предложенного решения.

ЛИТЕРАТУРА

1. Винявский, А.А. Industrial Internet of Things: риски и защита в цифровую эпоху / А.А. Винявский // Автоматизация в промышленности. – 2024. – № 9. – С. 57-60.

2. Евдокимова, С.А. Проблемы безопасности промышленного интернета вещей / С.А. Евдокимова // Актуальные проблемы автоматизации, роботизации и управления в технических, организационных, экономических системах : сборник материалов Всероссийской научно-практической конференции преподавателей и специалистов и Всероссийской научно-практической конференции студентов и молодых ученых. – Воронеж, 2025. – С. 62-68.

3. Cindrić, I. Mapping of Industrial IoT to IEC 62443 Standards / I. Cindrić, M. Jurčević, T. Hadjina // Sensors. – 2025. – Vol. 25(3). – S. 728. – DOI: 10.3390/s25030728.

4. NVD – Home. National Vulnerability Database. – URL: https://nvd.nist.gov/(дата обращения: 18.01.2026).

5. CVE: Common Vulnerabilities and Exposures. – URL: https://cve.mitre.org/ (дата обращения: 18.01.2026).

УДК 517.925

Р. Пренов;
Р. Мамедсалиев
(Туркменский государственный университет имени Магтымгулы, г. Ашхабад);
(Туркменский инженерно-технологический университет имени Огуз Хана, г. Ашхабад, Туркменистан)

ОБ ОДНОЙ НАЧАЛЬНО-КРАЕВОЙ ЗАДАЧЕ ДЛЯ СИСТЕМЫ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ ПЕРВОГО ПОРЯДКА

В настоящей работе рассматривается нелокальная начально-краевая задача для системы гиперболических уравнений первого порядка.

$$\begin{cases} \dfrac{\partial u(t,x)}{\partial t} = a(x)\dfrac{\partial u(t,x)}{\partial x} - \delta u(t,x) + b(t,x)v(t,x) + f_1(t,x),\ 0 < t \le T,\ 0 < x < l, \\ \dfrac{\partial v(t,x)}{\partial t} = -a(x)\dfrac{\partial v(t,x)}{\partial x} - \delta v(t,x) + f_2(t,x),\ 0 < t \le T,\ 0 < x < l, \\ u(t,0) = u(t,l), \qquad v(t,0) = v(t,l), \qquad 0 \le t \le T, \\ u(0,x) = u_0(x), \qquad v(0,x) = v_0(x), \qquad 0 \le x \le l. \end{cases} \tag{1}$$

Здесь

$a(x) \ge a > 0,\ f_1(t,x), f_2(t,x),\ u_0(x), v_0(x),\ b(t,x),\ \delta > 0,\ ((t,x) \in [0,T] \times [0,l])$