УДК 004.056 Вестник УрФО № 3(45) / 2022, с. 83–91

Шевяков И.А., Соколов А.Н.

DOI: 10.14529/secur220310

МЕТОД ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ КРИТИЧЕСКИХ УЗЛОВ ИНФОРМАЦИОННОЙ СЕТИ ТРАНСПОРТНОГО СРЕДСТВА[1]

В статье предложен метод определения уровня защищённости к кибератакам узлов информационной сети транспортного средства, функционирование которых важно для безопасности дорожного движения. Метод основан на применении математического аппарата И/ИЛИ графов для моделирования операционных зависимостей в узлах информационной сети. Приведен перечень угроз, актуальных для информационной сети транспортного средства, и средств защиты информации, применяемых в сетях такого типа. Оценка уровня защищённости проводится для типовой сети транспортного средства, содержащей несколько электронных блоков управления. Сделан вывод об эффективности разработанного метода.

Ключевые слова: *информационная безопасность, защита информации, информационная сеть транспортного средства, подключенное транспортное средство, электронный блок управления (ЭБУ), И/ИЛИ граф, гиперграф, средство защиты информации (СЗИ), кибератака, кибербезопасность.*

Sheviakov I.A., Sokolov A.N.

METHOD FOR DETERMINING THE LEVEL OF SECURITY OF CRITICAL NODES OF THE INFORMATION NETWORK OF A VEHICLE

The article proposes a method for determining the levels of protection against cyberattacks of vehicle information network nodes, the functioning of which is important for road safety. The method based on the use of the mathematical apparatus of AND/OR graphs for modeling operational dependencies in the nodes of the information network. A list of threats relevant to the

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ МТУСИ) в рамках научного проекта № 40469-25/2021-К.

information network of the vehicle, and information protection tools used in networks of this type is given. The security level assessed for a typical vehicle network containing several electronic control units. A conclusion made about the effectiveness of the developed method.

Keywords: *Information security, information security, vehicle information network, connected vehicle, electronic control unit (ECU), AND/OR graphs, hypergraphs, information security tools, cyberattack, cybersecurity.*

Введение

Большинство современных моделей транспортных средств (ТС) в значительной степени компьютеризированы и имеют возможность подключения через внешние беспроводные сети к другим ТС, придорожным приборам, мобильным устройствам и сервисным центрам производителей оригинального оборудования (OEM производителей) [1]. Ввиду наличия большого количества угроз информационной безопасности (ИБ) в этих сетях, компьютерная и сетевая безопасность требует защиты всех компонентов инфраструктуры на нескольких уровнях [2]. Внутренние и внешние информационные сети всех ТС, а также дорожная информационная инфраструктура («умные светофоры», «умные знаки», системы управления дорожным движением и т.д.) являются частью критической информационной инфраструктуры (КИИ) системы дорожного движения города, следовательно, должны приниматься соответствующие меры по защите информации. Обеспечение большей части этих мер должно закладываться в информационные системы ещё на этапе проектирования.

На информационных ресурсах имеется много публикаций о кибератаках на автомобильные системы, некоторые из которых попали под пристальное внимание средств массовой информации [3], что привело к ущербу репутации производителей автомобилей.

Помимо ущерба репутации, стоимость обеспечения кибербезопасности стала значительной проблемой для производителей автомобилей. Обнаружение уязвимостей узлов информационных сетей транспортных средств (ИСТС) привело к постоянному увеличению количества отзывов автомобилей для устранения неисправностей. Так, в 2010 году Чарли Миллер и Крис Валасек [4] продемонстрировали концепцию удаленных атак, взяв под контроль джип и отправив его в бездорожье, что вызвало отзыв 1,4 миллиона автомобилей. Исследователи безопасности взломали электронную систему BMW Connected Drive и смогли удаленно разблокировать автомобили, что оказало еще большее влияние на промышленность – было отозвано 2,2 миллиона автомобилей [5]. Подобные угрозы информационной безопасности оказывают значительное влияние на безопасность дорожного движения и конфиденциальность персональных данных пассажиров и других граждан.

Из описанных выше примеров следует, что при проектировании ТС особое внимание должно уделяться безопасности информации как на уровне всей информационной сети в целом, так и на уровне отдельных узлов и подсистем. Для этого необходимо на этапе проектирования обладать информацией о необходимых мерах защиты, которые требуется применить в информационной сети каждого конкретного разрабатываемого транспортного средства, чтобы обеспечить требуемый уровень безопасности информации, передающейся по внутренней сети ТС.

Вопросы, связанные с исследованием и классификацией угроз безопасности информации в сети ТС, рассмотрены в работах Juan Deng [2] и Florian Sommer, Jürgen Dürrwang [6]. Авторами представлена классификация для описания атак на информационные системы ТС, а также предложены методы защиты от таких вредоносных воздействий, как в рамках отдельного узла, так и в рамках системы в составе информационной сети ТС.

Применению математических методов и алгоритмов анализа защищённости информации в сетях технических объектов и идентификации критических узлов в сложных сетях посвящено множество работ, среди которых необходимо отметить труды Martín Barrère, Chris Hankin [7]. Авторы представили методику оценки уровня информационной безопасности, направленную на определение критических киберфизических компонентов и измерение общей безопасности сетей АСУ ТП. В основе подхода к созданию методики лежит использование моделей на основе графов И/ИЛИ, позволяющее исследовать зависимости между компонентами промышленных сетей.

Используя подходы, предложенные в [2, 6, 7, 8], разработан метод определения уровня защищённости критических узлов ИСТС. При разработке метода определен перечень актуальных угроз безопасности информации в сети ТС и типовой состав узлов и подсистем сети ТС.

Типовая архитектура информационной сети транспортного средства

Большинство архитектур ИСТС включают нескольких систем, связанных между собой центральным шлюзом (рис. 1). Системы отвечают за различные функциональные характеристики компонентов ТС. При компрометации этих компонентов могут появиться риски нарушения ИБ. Влияние этих рисков на безопасное, для дорожного движения, функционирование ТС может варьироваться. По этой причине, критичные для безопасности дорожного движения, компоненты ТС требуют соответствующей защиты.

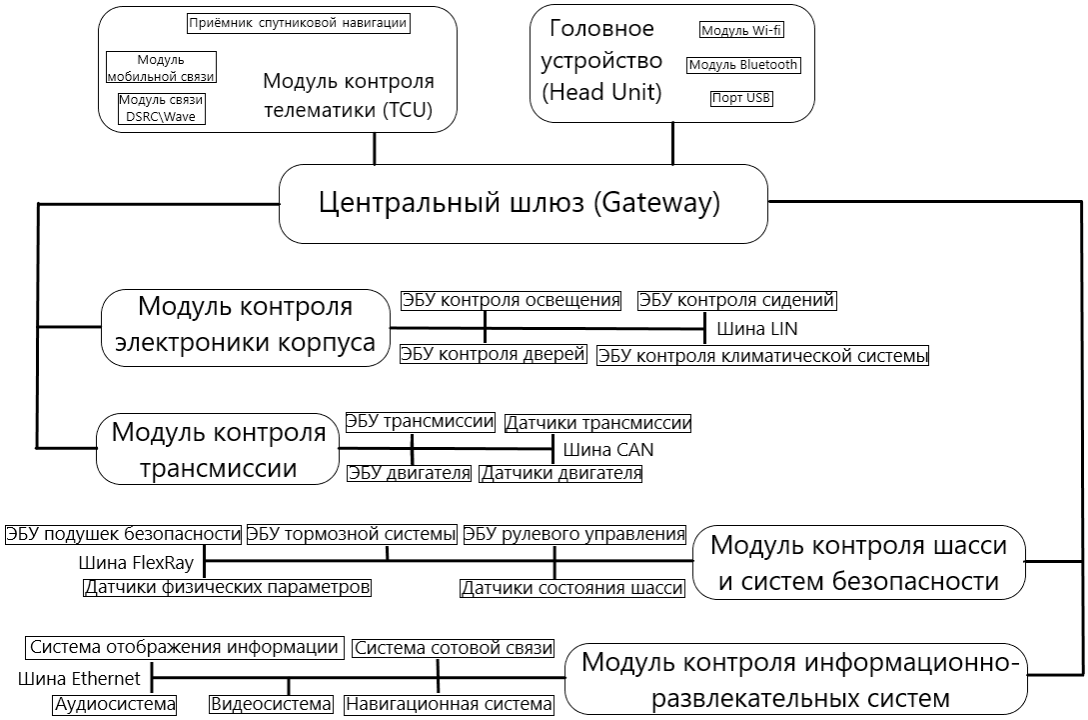

Рис. 1. Структура информационной сети транспортного средства

Компоненты разделяются по следующим категориям:

– управление трансмиссией;

– управление шасси;

– контроль корпуса;

– управление информационно-развлекательной системой;

– контроль коммуникаций;

– системы диагностики и обслуживания.

Угрозы, актуальные для информационной сети транспортного средства

Для представления основных задач информационной безопасности, актуальных для информационной сети транспортного средства, рассмотрены угрозы, которые могут возникнуть при эксплуатации и обслуживании транспортных средств. Большая часть угроз безопасности информации в ИСТС описана в базе данных Automotive Attack Database (AAD) [6], разработанной в университете Карлсруэ. База данных предлагает схему классификации для описания автомобильных атак безопасности в виде единой таксономии. Чтобы иметь возможность использовать описания атак на нескольких этапах разработки в качестве источника информации, атаки представлены с различным уровнем детализации.

Все угрозы, актуальные для ИСТС, можно объединить в несколько групп.

Угрозы потери информации:

– угроза потери информации в облаке;

– угроза потери целостности конфиденциальной информации;

– угрозы потери информации от конфликтов DRM.

Угрозы возникновения сбоев и неисправностей:

– угроза сбоя или перебоев в электроснабжении;

– угроза наличия критических программных ошибок;

– угроза сбоя или нарушения работы каналов связи.

Угрозы перехвата и подделки сообщений сети:

– угроза перехвата информации через побочные электромагнитные излучения;

– угроза подделки сообщений сети;

– угроза «человек посередине» (MitM).

Угрозы вредоносного воздействия на информационную сеть:

– угроза отказа в обслуживании;

– угроза манипуляции с аппаратным и программным обеспечением, манипулирования информацией;

– угроза несанкционированного доступа к информационной системе/сети;

– угроза компрометации конфиденциальной информации;

– угроза действия вредоносного программного обеспечения;

– угроза удаленного исполнения кода.

Для противодействия угрозам информационной безопасности в сети транспортного средства используются меры обеспечения ИБ, которые применяются и к компьютерным информационным сетям, но модифицируются с учётом специфики используемых протоколов и алгоритмов работы устройств, а также требований надёжности и быстродействия. Все меры защиты условно можно поделить на две категории – программные и аппаратные.

Программные меры защиты информации в сети ТС:

– обфускацию кода;

– использование криптографических методов;

– ловушки руткитов.

Аппаратные меры защиты информации в сети ТС:

– использование системы обнаружения вторжений;

– применение межсетевого экрана на центральном шлюзе и других критически важных узлах.

Методика оценки уровня уязвимости узлов ИСТС

Автомобильную информационную сеть W можно представить как ориентированный И/ИЛИ граф G = (V, E), который представляет взаимодействия между узлами в W (рис. 2). Граф включает три типа базовых вершин, называемых атомарными узлами (V_{AT}), которые моделируют различные компоненты сети: S представляет набор узлов датчиков, C представляет набор узлов исполнительных механизмов, а A представляет набор программных агентов (работающих, например, в ЭБУ и TCU). V_{AT} определяется как: $V_{AT} = S \cup C \cup A$. Кроме того, граф также включает два типа искусственных узлов, которые моделируют логические зависимости между компонентами сети: Δ представляет собой набор логических узлов И, а Θ представляет собой набор узлов логического ИЛИ. Набор всех узлов графа определяется как $V(G) = VAT \cup \Delta \cup \Theta$. E(G) является набором ребер между узлами, и их семантика зависит от типа узлов, которые они соединяют.

Меры защиты, применяемые в информационных сетях транспортного средства, могут применяться сразу к нескольким узлам сети, поэтому могут быть представлены как дополнительный уровень над графом логических зависимостей информационной сети транспортного средства. Множество задействованных мер безопасности Mi определяется как $S = \{s_1, s_2, ...\}$.

Гиперребра объединяют каждый сетевой узел с мерами безопасности, которые используются для их защиты. Таким образом, можно следовать той же логической структуре, что и в исходном графе, и объединять эти суперузлы с помощью связок И/ИЛИ, как показано на рис. 3.

Рассмотрим проблему с логической точки зрения, следовательно, с точки зрения выполнимости.

Решение задачи максимальной выполнимости для описанного логического представления информационной сети транспортного средства, где веса задаются функциями $\phi(n)$ для каждого узла $n \in Vr$ и q(s) для каждой меры безопасности $s \in S$, состоит из нескольких этапов:

1. Операционные зависимости представляются в подсистеме в виде логических зависимостей типа И/ИЛИ графа G.

2. Зависимости графа G преобразуются в эквивалентное логическое представление g(x).

3. Зависимость g(t) преобразуется в новую форму k(t), где каждый не виртуальный узел сети $n \in Vr$ в g(x) заменяется на $(n \vee s_i \vee ... \vee s_j)$, где $s_i \vee ... \vee s_j$ — это дизъюнкция мер безопасности, которые защищают узел n.

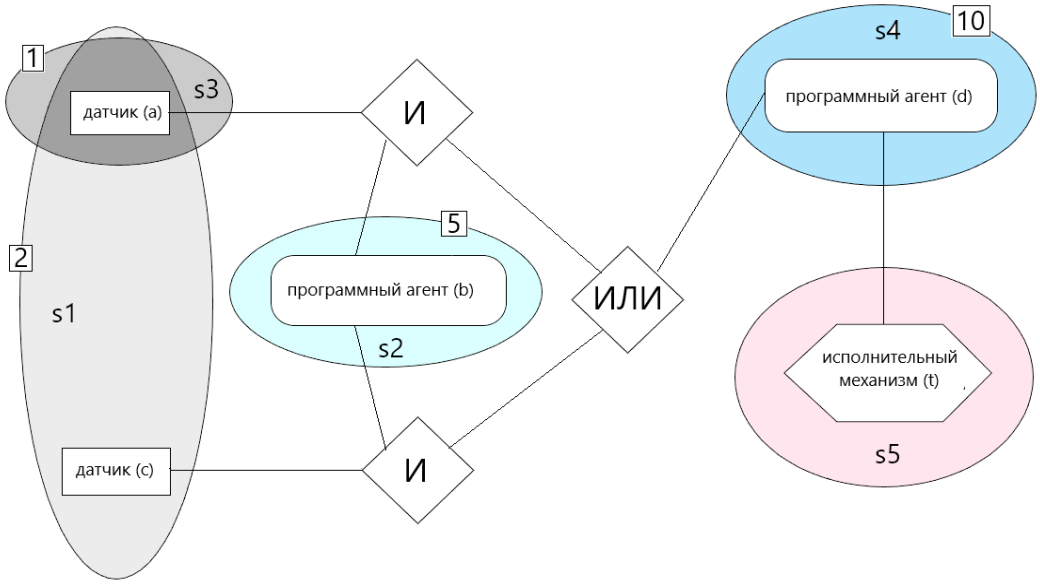

Рис. 2. Участок информационной сети в виде И/ИЛИ графа с перекрывающимися мерами безопасности

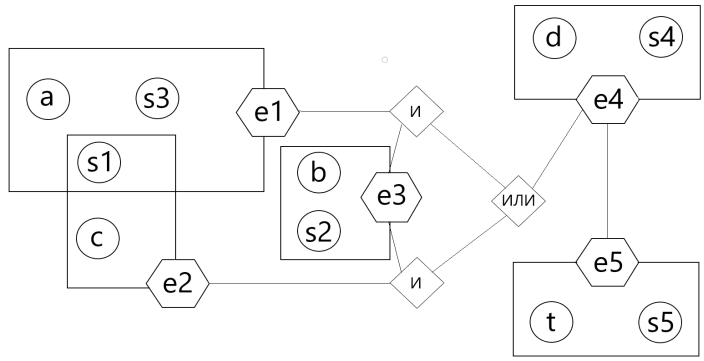

Рис. 3. Представление узлов сети (a, b, c, d, c1) и мер безопасности (s1, s2, s3, s4, s5) в виде рёбер гиперграфа И/ИЛИ (e1, e2, e4, e5)

4. Цель атакующего ¬k(t) преобразуется в конъюнктивную нормальную форму (КНФ) с помощью преобразования Цейтина, т. е. G(x) = КНФ (¬g(x)), где $g(x) = (v_{1i} \vee ... \vee v_{1j}) \wedge ... \wedge (v_{hi} \vee ... \vee v_{hj})$.

5. Определяется мягкое предложение для каждого невиртуального узла $n \in V_r$ и каждой меры безопасности $s \in S$ и присваиваем им веса (n, w(n)) и (s, q(s)) соответственно.

Оценка защищённости узлов

Для реализации метода разработано программное обеспечение (ПО), в основу которого положен обобщённый алгоритм решения задачи максимальной выполнимости. Функционально ПО состоит из трёх вычислительных модулей, модуля отображения результата, модуля чтения исходных данных и модуля формирования результата. Модуль расчёта показателей основан на решателе META4ICS [9], используемом для анализа защищённости сетей АСУ ТП.

Результаты, представленные в табл. 1, представляют собой список узлов и экземпляров мер защиты (М1 – М6) для информационной сети ТС, представленной на рис. 1, каждая система которой представлена в виде И/ИЛИ графа (рис. 4), которые необходимо применить к этим узлам, чтобы затраты злоумышленника на преодоления данного узла были максимальны. Затраты злоумышленника, необходимые для преодоления системы защиты в расчитанной конфигурации, приведены в третьем столбце табл. 1.

Полученные данные о количестве и виде защитных мер можно использовать в системах автоматизированного проектирования, а также вносить в спецификации выпускаемых изделий.

Оценка быстродействия и эффективности метода

Для оценки быстродействия предложенного подхода проведён набор эксперимен-

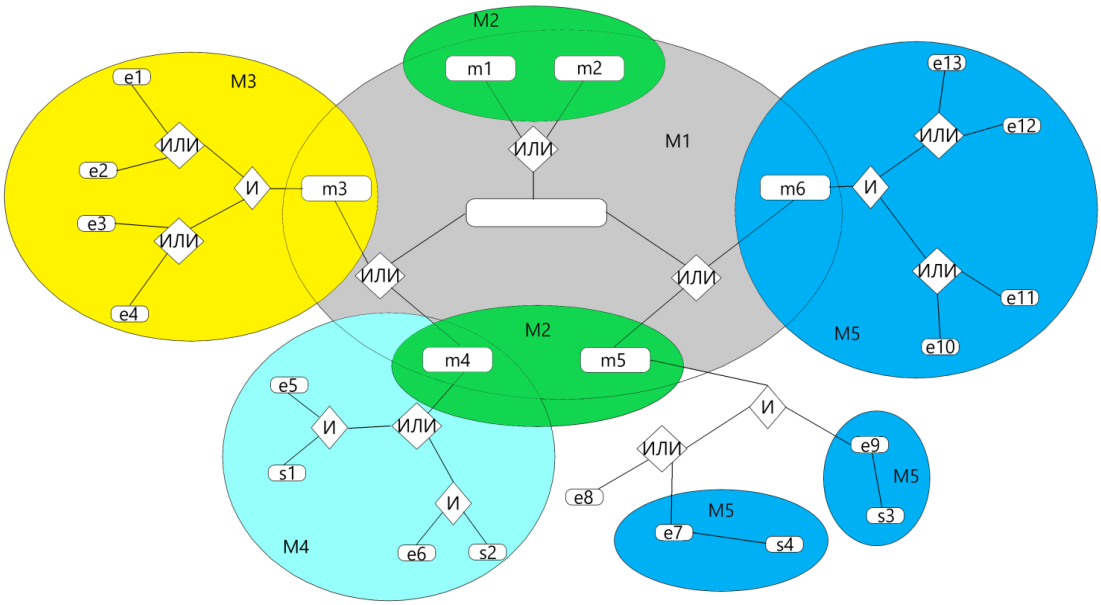

Рис. 4. Модель распределения средств защиты в типовой информационной сети ТС (e1…e13 – ЭБУ, s1… s4 – датчики, m1 … m6 – модули)

Таблица 1

Список мер защиты для каждого из компонент подсистемы

Мера защиты	Тип меры защиты	Затраты на преодоление	Защищаемые узлы
M1	M1	1	m1, m2, m3, m4, m5, m6
M2-1	M2	1	m1, m2
M2-2	M2	2	m4, m5
M3	M3	4	e1, e2, e3, e4, m3
M4	M4	4	e5, e6, s1, s2, m4
M5-1	M5	3	e7, s4
M5-2	M5	3	e9, s3
M5-3	M5	2	e10, e11 e12, e13, m6

тов, основанных на синтетических псевдослучайных графах И/ИЛИ разного размера и состава.

Эти эксперименты проводились на системе с процессором AMD Ryzen 5 5600 3,7 ГГц, 32 ГБ памяти DDR4 2400 МГц. Процедура построения графа И/ИЛИ размера n выглядит следующим образом.

На рис. 5 показано поведение методологии на взвешенных графах И/ИЛИ, когда размер входного графа увеличивается. В этом эксперименте создаются псевдослучайные графы И/ИЛИ размера n и композиционной конфигурации (60, 20, 20). Размер n изменяется как $n \in [0, 500, 1000, 1500, \ldots, 20000]$, и процесс оценки повторяется 10 раз для каждого значения n.

Для графов с 10 000 узлов среднее время разрешения составляет около 3 секунд, а для графов с 20 000 узлов среднее время составляет около 15 секунд. В целом время преобразования Цейтина стабильно на всех итерациях, процесс разрешения MAX-SAT требует больше времени для решения проблемы на одних графах, чем на других. Это происходит из-за того, что некоторые графы дают формулы с более длинными последовательностями операторов И или ИЛИ, соединяющих различные комбинации узлов графа, что требует переменного времени вычислений. Получен-

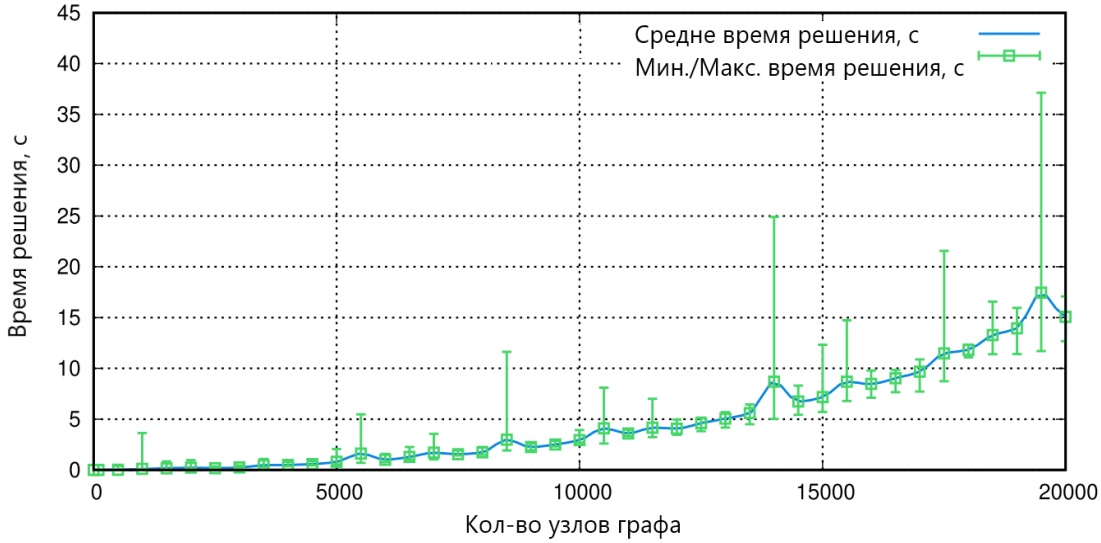

Рис. 5. Результаты измерения производительности при масштабируемости размера графа до 20000 узлов

ные результаты показывают, что представленный подход может эффективно масштабироваться до больших графов И/ИЛИ, включающих тысячи узлов, защищенных несколькими мерами безопасности.

Для оценки эффективности разработанного метода, сравним эффективность определения уязвимостей критических узлов системы защиты информации информационной сети ТС (СЗ ИСТС) при использовании предложенного программного средства и при выполнении этой работы традиционными методами. Для сравнения применён метод многокритериального анализа альтернатив Беллмана-Заде. Полученное отношение множеств $P_2 / P_1 = 1{,}47$ позволяет сделать вывод, что применение разработанного ПО делает процесс оценки уязвимостей СЗ ИСТС в полтора раза более эффективным.

Заключение

В работе приведён обобщённый метод определения защищённости узлов, состоящий из пяти этапов, позволяющий применять его для сети любого размера. Однако необходимо учитывать, что для большого количества узлов возможно существенное снижение производительности вычислений.

Разработано программное средство расчёта конфигурации мер защиты информации в ИСТС. Проведён анализ производительности программного комплекса на различных конфигурациях модельных сетей с разным количеством, атомарных и виртуальных узлов.

Полученные в ходе работы результаты могут быть использованы при проектировании СЗИ ИСТС и при моделировании инцидентов ИБ на специализированных стендах [10].

Литература

1. What Is an OEM? [Электронный ресурс]. – Режим доступа: https://www.cars.com/articles/what-is-an-oem-1420696948647/, свободный (дата обращения: 01.09.2022 г.).

2. Juan Deng, Lu Yu, Yu Fu, Oluwakemi Hambolu, Richard R. Brooks, Chapter 6 – Security and Data Privacy of Modern Automobiles // Data Analytics for Intelligent Transportation Systems, Elsevier, 2017, P. 131–163.

3.WIRED: Car Hacking. [Электронный ресурс]. – Режим доступа: https://www.wired.com/tag/car-hacking/, свободный (дата обращения: 01.09.2022 г.).

4. Charlie Miller, Chris Valasek. Adventures in Automotive Networks and Control Units. [Электронный ресурс]. – Режим доступа: https://illmatics.com/car_hacking.pdf, свободный (дата обращения: 01.09.2022 г.).

5. Beemer, Open Thyself! – Security vulnerabilities in BMW's Connected Drive [Электронный ресурс]. – Режим доступа: https://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html, свободный (дата обращения: 01.09.2022 г.).

6. Sommer F, Dürrwang J, Kriesten R. Survey and Classification of Automotive Security Attacks. Information. 2019; 10 (4):148. https://doi.org/10.3390/info10040148.

7. Martín Barrère, Chris Hankin, Nicolas Nicolaou, Demetrios G. Eliades, Thomas Parisini, Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies // Journal of Information Security and Applications, Volume 52, 2020, 102471, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102471.

8. A. Barinov, N. Davydkin, D. Sharova and S. Skurlaev, "Prioritization methodology of computing assets for connected vehicles in security assessment purpose," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), 2019, pp. 1–6.

9. M. Barrère. META4ICS – metric analyser for industrial control systems. [Электронный ресурс]. – Режим доступа: https://github.com/mbarrere/meta4ics, свободный (дата обращения: 01.09.2022 г.).

10. Шевяков И. А., Соколов А. Н. Концепция стенда для исследования кибербезопасности устройств на шине FlexRay «подключенного» транспортного средства, основанная на использовании интерфейсных плат // Вестник УрФО: Безопасность в информационной сфере. – Челябинск: Изд-во Южно-Уральский юридический вестник. – 2019. – №3(33) – С.73–81.

References

1. What Is an OEM? [Online]. – Rezhim dostupa: https://www.cars.com/articles/what-is-an-oem-1420696948647/, svobodnyj (data obrashhenija: 01.09.2022).

2. Juan Deng, Lu Yu, Yu Fu, Oluwakemi Hambolu, Richard R. Brooks, Chapter 6 - Security and Data Privacy of Modern Automobiles // Data Analytics for Intelligent Transportation Systems, Elsevier, 2017, P. 131–163.

3. WIRED: Car Hacking. [Online]. – Режим доступа: https://illmatics.com/car_hacking.pdf, свободный (дата обращения: 01.08.2022 г.)

4. Charlie Miller, Chris Valasek. Adventures in Automotive Networks and Control Units. [Online]. – Rezhim dostupa: https://illmatics.com/car_hacking.pdf, svobodnyj (data obrashhenija: 01.09.2022).

5. Beemer, Open Thyself! – Security vulnerabilities in BMW's Connected Drive [Online]. – Rezhim dostupa: https://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-Connected Drive-2540957.html, svobodnyj (data obrashhenija: 01.09.2022).

6. Sommer F, Dürrwang J, Kriesten R. Survey and Classification of Automotive Security Attacks. Information. 2019; 10 (4) :148. https://doi.org/10.3390/info10040148.

7. Martín Barrère, Chris Hankin, Nicolas Nicolaou, Demetrios G. Eliades, Thomas Parisini, Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies // Journal of Information Security and Applications, Volume 52, 2020, 102471, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102471.

8. A. Barinov, N. Davydkin, D. Sharova and S. Skurlaev, "Prioritization methodology of computing assets for connected vehicles in security assessment purpose," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), 2019, pp. 1–6.

9. M. Barrère. META4ICS – metric analyser for industrial control systems. [Online]. – Rezhim dostupa: https://github.com/mbarrere/meta4ics, svobodnyj (data obrashhenija: 01.09.2022).

10. Sheviakov I. A., Sokolov A. N. Koncepcija stenda dlja issledovanija kiberbezopasnosti ustrojstv na shine FlexRay «podkljuchennogo» transportnogo sredstva, osnovannaja na ispol'zovanii interfejsnyh plat // Vestnik UrFO: Bezopasnost' v informacionnojsfere. – Chelyabinsk: Izd-vo Juzhno-Ural'skij juridicheskij vestnik. – 2019. – №3(33) – P. 73–81.

ШЕВЯКОВ Игорь Андреевич, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: regnlager@yandex.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

SHEVIAKOV Igor Andreevich, PhD student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: regnlager@yandex.ru

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru