УДК 519.876.5 Вестник УрФО № 2(56) / 2025, с. 58–64

Васильев А. А., Сергин Д. А., Щерба Е. В. DOI: 10.14529/secur250206

МОДЕЛЬ АТАКИ ИСТОЩЕНИЯ ЭНЕРГОРЕСУРСОВ МОБИЛЬНЫХ УСТРОЙСТВ В САМООРГАНИЗУЮЩИХСЯ СЕТЯХ

В статье представлена модель атаки истощения энергоресурсов мобильных устройств на базе протокола маршрутизации OLSR, реализованная в сетевом симуляторе ns-3. Успешная реализация указанной атаки на мобильные сетевые устройства с аккумулятором приводит к нарушению их доступности. Проведены экспериментальные исследования показателей работы сети и последствий атаки истощения энергоресурсов с использованием различных режимов реализации подобной атаки. В заключении предложены перспективные подходы к противодействию указанным сетевым атакам.

Ключевые слова: *самоорганизующиеся сети, Интернет вещей, модель нарушителя, атаки истощения энергоресурсов, OLSR, ns-3.*

Vasiliev A. A., Sergin D. A., Shcherba E. V.

MODELING AN ENERGY DEPLETION ATTACK IN MOBILE AD-HOC NETWORKS

The article is devoted to modeling an energy depletion attack in mobile ad-hoc networks (MANET). The attack model is implemented based on the OLSR routing protocol in the ns-3 network simulator. Successful execution of the specified attack on mobile network devices with a battery leads to a violation of their availability. Experimental studies of network performance indicators and the consequences of the energy depletion attack are conducted. In conclusion, promising approaches to counteracting the specified network attacks are proposed.

Keywords: *ad-hoc networks, Internet of Things, attack model, energy depletion attacks, OLSR, ns-3.*

Введение

Атаки, направленные на истощение энергоресурсов (АИЭ, в зарубежной литературе известны под названием Energy Depletion Attack, EDA), являются одной из наиболее критичных угроз для беспроводных сетей устройств, работающих от аккумуляторных батарей, таких как беспроводные сенсорные сети (БСС) или сети устройств Интернета вещей. Основная особенность таких атак заключается в трудности их обнаружения, поскольку, как правило, такая атака воздействует на устройство или сеть опосредованно, путем отправки по коммуникационной сети ложных либо избыточных запросов, которые выглядят на первый взгляд легитимно и не всегда могут быть идентифицированы как атака. При этом процесс разряда аккумулятора в ходе атаки трудно отличим от нормальной работы устройства, и для обнаружения таких атак зачастую требуются специальные средства анализа.

Сложность защиты от атак в динамически организуемых сетях, прежде всего, лежит в самой форме реализации сети, когда её топология и структура связей между узлами способна меняться динамически в зависимости от различных факторов, таких как количество узлов, их производительность, уровень помех в канале связи, заряд аккумуляторов и т.д. Таким образом, задача моделирования подобных атак в беспроводных сетях мобильных устройств представляет особый интерес, с целью разработки эффективных механизмов защиты.

Анализ существующих атак истощения энергоресурсов

В настоящее время проблематике атак на истощение энергоресурсов уделяется всё большее внимание. В частности, в работе [1] приводится детальное описание принципов и классификация АИЭ, выполняемых на различных уровнях сетевого взаимодействия (физический, канальный, сетевой, прикладной), а также теоретический анализ существующих методик защиты от АИЭ. В [2] анализируются существующие разновидности атак истощения энергоресурсов на беспилотные летательные аппараты с выделением их ключевых характеристик.

Значительный интерес представляют конкретные реализации атак истощения энергоресурсов. В работе [3] производится моделирование АИЭ в сетях на основе протокола маршрутизации RPL, а также демонстрация и анализ эффективности защитного механизма на основе сравнения числа переданных пакетов в течение промежутка времени с пороговым значением. В свою очередь, задача организации защиты от подобных атак в работе [4] решается путем использования предложенного протокола маршрутизации для беспроводных сенсорных сетей, учитывающего энергоэффективность узлов сети для расчета оптимального маршрута.

В исследовании [5] рассматриваются сетевые атаки, приводящие к истощению заряда аккумуляторов беспилотных летательных аппаратов, и предложена комплексная математическая модель процесса истощения энергоресурсов устройств Интернета вещей, которая учитывает чередование циклов активного потребления энергии и спящего режима, а также предусматривает пороговое значение заряда аккумулятора, необходимое для корректной работы устройства.

Моделирование АИЭ в сетях на базе проактивного протокола маршрутизации OLSR

В настоящее время подавляющее большинство устройств с автономным питанием использует источники питания на базе литий-ионных (Li-Ion) либо литий-полимерных аккумуляторов. Характеристики данных источников питания, а также преимущества их применения в устройствах достаточно широко изучены в соответствующих работах [6]. В сетевом симуляторе ns-3 реализована модель источника питания на базе Li-Ion аккумулятора, предложенная в работе [7]. Указанная модель использована в настоящей работе для подготовки имитационной модели атаки истощения энергоресурсов.

Основная идея предложенной модели атаки истощения энергоресурсов базируется на динамическом изменении потребления энергии в процессе работы симулируемого протокола маршрутизации OLSR. Протокол маршрутизации OLSR является одним из наиболее широко используемых протоколов маршрутизации в беспроводных сетях мобильных устройств. Симулятор ns-3 позволяет устанавливать обработчики событий, связанных с симуляцией протокола OLSR, включая приём/передачу сообщений протокола или изменение таблицы маршрутизации. Используя обработчики указанных событий, можно учесть потребление энергии каждым сетевым узлом при их наступлении, что обе-

спечивает корректное функционирование предложенной модели.

Пусть I – величина тока потребления узлом сети в некоторый момент времени t. Для упрощения модели положим, что потребление энергии компонентами узла, не связанными с функционированием протокола маршрутизации, описывается величиной среднего тока потребления аккумулятора в рабочем режиме I_0. Тогда, при функционировании узла сети в нормальном режиме без протокола маршрутизации, ток потребления описывается формулой (1):

$$I = I_0 . \quad (1)$$

В свою очередь, ток потребления на время функционирования процесса протокола маршрутизации OLSR (например, при наступлении события перестройки таблицы маршрутизации), можно описать формулой (2):

$$I = I_0 + I_{OLSR}, \quad (2)$$

где I_{OLSR} – ток потребления процессом протокола маршрутизации OLSR.

При этом временной интервал активности процесса протокола маршрутизации зависит от параметров самого события. Введем величину t_{OLSR}, которая определяет время, в течение которого ток потребления I описывается формулой (2).

Временной интервал $t_{OLSR(table)}$ события перестройки таблицы маршрутизации OLSR можно описать как:

$$t_{OLSR(table)} = \alpha_{table} + \beta_{table} * N_{table}, \quad (3)$$

где α_{table} – постоянная составляющая временного интервала перестройки таблицы маршрутизации в миллисекундах (мс), β_{table} – время обработки одного элемента таблицы маршрутизации в мс, N_{table} – количество записей в таблице маршрутизации.

В свою очередь, временной интервал $t_{OLSR(RX/TX)}$ события приёма/передачи пакетов протокола OLSR можно описать как:

$$t_{OLSR(RX/TX)} = \alpha_{RX/TX} + \beta_{RX/TX} * N_{msg}, \quad (4)$$

где $\alpha_{RX/TX}$ – постоянная составляющая временного интервала приема-передачи пакета в мс, $\beta_{RX/TX}$ – время приема-передачи одного OLSR сообщения в мс, N_{msg} – число сообщений в одном пакете протокола OLSR.

Таким образом, при функционировании узла сети в нормальном режиме, когда процесс протокола маршрутизации остается неактивным, ток потребления вычисляется по формуле (1). Как только в процессе симуляции наступает событие протокола OLSR, по формулам (3) или (4) вычисляется временной интервал данного события, что в свою очередь позволяет вычислить ток потребления по формуле (2).

В процессе симуляции производится регулярное отслеживание текущего напряжения аккумулятора V сетевых устройств. Если текущее напряжение аккумулятора устройства снижается до порогового значения разряда V_{off}, аккумулятор считается разряженным, и устройство выводится из работы.

Предложенная модель атаки истощения энергоресурсов сетевых узлов реализуется посредством уменьшения интервалов отправки служебных сообщений протокола маршрутизации. Стандарт RFC 7181 описывает интервалы отправки служебных сообщений OLSR: в частности, для сообщений HELLO он составляет 2с, для сообщений TC – 5с [8]. В результате уменьшения данных интервалов увеличивается частота отправки указанных сообщений, и, как следствие, частота их приема смежными узлами. Поскольку обработка каждого сообщения влечет за собой потребление энергии, путем увеличения частоты отправки таких сообщений узел нарушителя может добиться ускоренного разряда источников питания целевых устройств.

На рисунке 1 представлена диаграмма сетевой топологии, использованная для процесса имитационного моделирования сетевого взаимодействия. Для экспериментальной оценки предложенной модели атаки было произведено несколько испытаний. В ходе первого испытания все узлы сети функционировали со стандартными значениями временных таймеров протокола OLSR. Для второго испытания таймер отправки сообщений HELLO узлом 2 был уменьшен до 1с. Для третьего испытания таймер отправки сообщений HELLO узлом 2 был уменьшен до 0,1с. В рамках четвертого испытания таймер отправки сообщений TC узлом 2 был уменьшен до 1 с.

Остальные параметры моделирования были определены следующим образом:

- Количество узлов в сети: 8.
- Ёмкость аккумулятора целевых узлов (кроме узла 2): 1000 мА/ч.

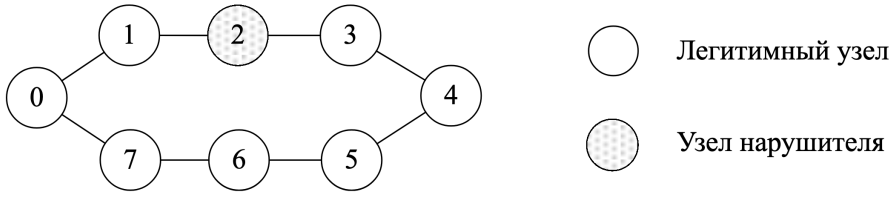


Рис. 1. Диаграмма сетевой топологии для имитационного моделирования

- Ток потребления аккумулятора в рабочем режиме I_0 = 20 мА.
- Ток потребления на время отработки процесса OLSR: I_{OLSR} = 200 мА.
- Номинальное напряжение аккумулятора в полностью заряженном состоянии: V_0 = 4,2 В.
- Пороговое напряжение разряда аккумулятора: V_{off} = 3.3 В.
- Номинальный интервал отправки сообщений протокола OLSR:
  - для сообщений типа HELLO – 2 с.
  - для сообщений типа ТС – 5 с.
- Временные интервалы обработки сообщений OLSR:

α_{table} = 10 мс, β_{table} = 0,5 мс.

$\alpha_{RX/TX}$ = 10 мс, $\beta_{RX/TX}$ = 1 мс.

- Время моделирования: 24 часа.

На рисунке 2 представлены графики зависимости напряжения аккумуляторов сетевых узлов от времени их работы в сети, полученные в результате имитационного моделирования.

В результате последующих испытаний была получена оценка зависимости времени работы сетевых узлов от значений таймеров

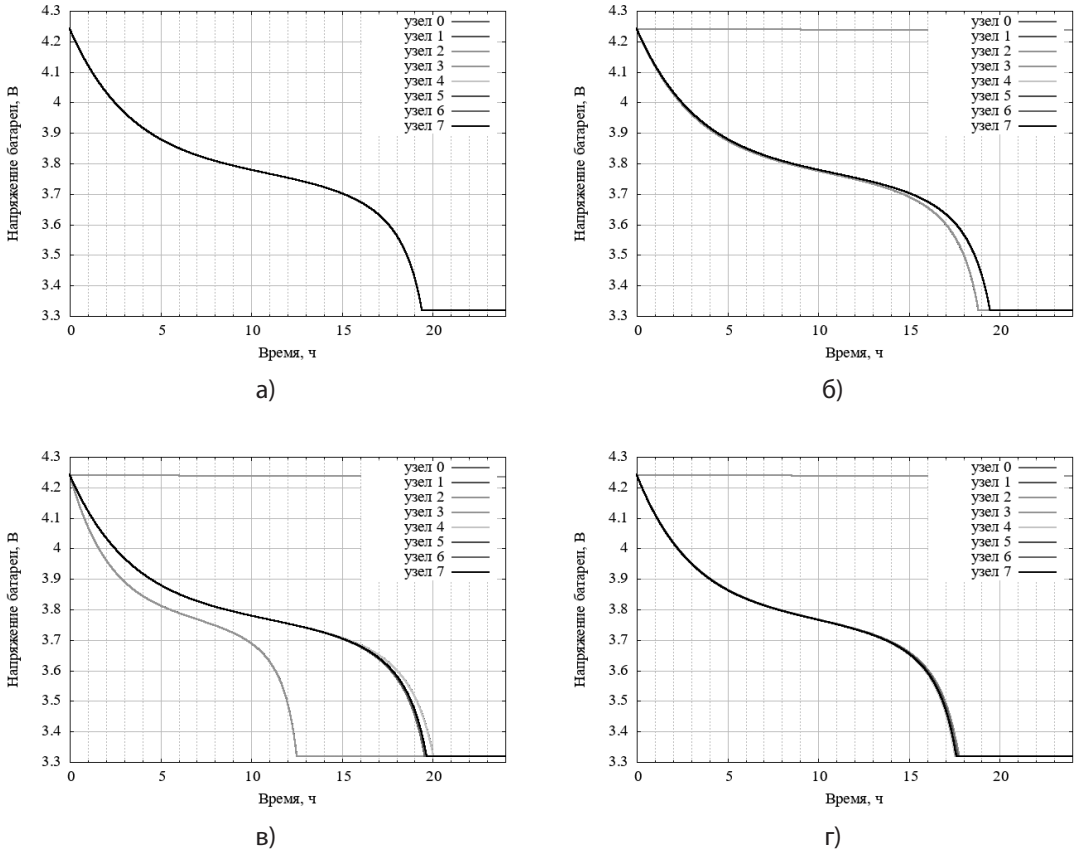
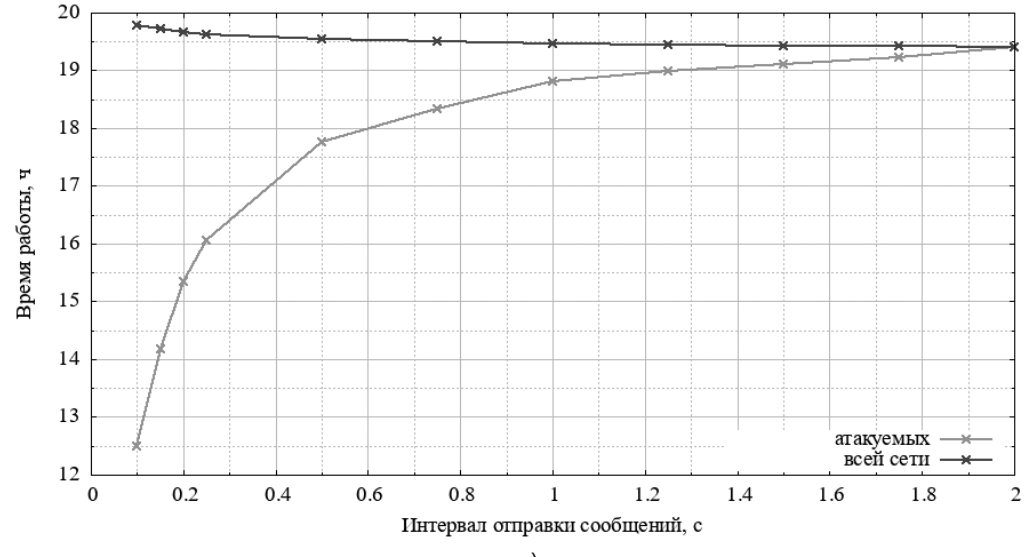
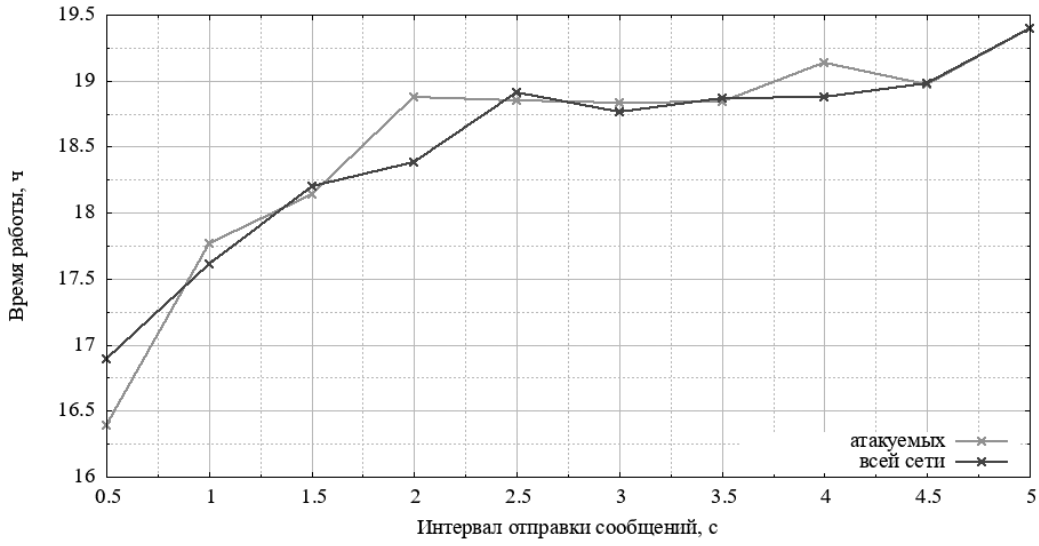


Рис. 2. Графики напряжения аккумуляторов сетевых узлов при различном поведении узла 2: нормальный режим (а), с уменьшенным до 1с таймером отправки сообщений HELLO (б), с уменьшенным до 0,1с таймером отправки сообщений HELLO (в), с уменьшенным до 1с таймером отправки сообщений ТС (г)



а)



б)

Рис. 3. Графики зависимости времени работы сетевых узлов
от значений таймеров отправки сообщений HELLO (а) и TC (б) узлом 2.

отправки служебных сообщений протокола OLSR узлом нарушителем (рисунок 3).

Анализируя полученные результаты, можно отметить, что уменьшение таймера отправки сообщений HELLO узлом нарушителем приводит к снижению времени работы соседних узлов, в то время как уменьшение таймера отправки сообщений TC вызывает заметное снижение времени работы узлов всей сети в целом. Это связано с тем, что сообщения TC, в отличие от сообщений HELLO, распространяются по всем узлам сети, охватываемой протоколом OLSR. В целом, зафиксированные результаты подчеркивают необходимость реализации мер по противодействию атакам на истощение энергоресурсов на всех узлах сети.

Заключение

По результатам моделирования атаки на истощение энергоресурсов в сетевом симуляторе ns-3 можно составить определенные рекомендации по противодействию данному классу атак.

Для противодействия атаке истощения энергоресурсов на базе протокола маршру-

тизации OLSR, каждый узел, во-первых, должен отбрасывать служебные сообщения протокола, для которых интервалы отправки, указанные в заголовке сообщения, не соответствуют интервалам отправки, определенным в конфигурации рассматриваемого узла. Для более эффективного противодействия, каждое сетевое устройство должно выполнять анализ количества отправленных и полученных служебных сообщений. При отклонении указанных показателей от нормальных значений (в частности, в случае аномально короткого интервала между сообщениями), устройство должно принимать меры по противодействию узлу нарушителя. Например, легитимные узлы могут просто игнорировать избыточные сообщения, если это не оказывает серьезного влияния на работоспособность сети. В некоторых случаях, легитимные узлы могут полностью изолировать узел нарушителя, полностью игнорируя все сообщения указанного узла.

Для корректной идентификации узла нарушителя могут применяться репутационные модели [9, 10]. В рамках подобной модели, отправка избыточных служебных сообщений протокола OLSR узлами сети будет приводить к снижению их репутации, что в конечном счете может быть использовано для изоляции узлов нарушителей с низкой репутацией.

Литература

1. Nguyen V.L., Lin P.C., Hwang R.H. Energy Depletion Attacks in Low Power Wireless Networks, IEEE Access, 2019, Vol. 7, pp. 51915-51932, DOI: 10.1109/ACCESS.2019.2911424.

2. Десницкий В.А., Рудавин Н.Н. Моделирование и оценка атак истощения энергоресурсов на беспилотные летательные аппараты в системах антикризисного управления / В.А. Десницкий, Н.Н. Рудавин // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России, 2019. № 4. С. 69-74.

3. Pu C. Energy Depletion Attack Against Routing Protocol in the Internet of Things, 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), January 2019, pp. 1-4, DOI: 10.1109/CCNC.2019.8651771.

4. Gong P., Chen T.M., Xu P. Resource-Conserving Protection against Energy Draining (RCPED) Routing Protocol for Wireless Sensor Networks, Network, 2022, Vol. 2(1), pp. 83-105, DOI: 10.3390/NETWORK2010007.

5. Kuaban G.S., Gelenbe E., Czachórski T., Czekalski P., Tangka J.K. Modelling of the Energy Depletion Process and Battery Depletion Attacks for Battery-Powered Internet of Things (IoT) Devices, Sensors (Basel), 2023, Vol. 23(13):6183, DOI: 10.3390/s23136183.

6. Sajja K.S., Bhowmik B. IoT Systems and Battery-Based Energy Sources, International Conference on Artificial Intelligence and Smart Communication (AISC), January 2023, pp. 212-219, DOI: 10.1109/AISC56616.2023.10085426.

7. Tremblay O., Dessaint L.A., Dekkiche A.I. A Generic Battery Model for the Dynamic Simulation of Hybrid Electric Vehicles, 2007 IEEE Vehicle Power and Propulsion Conference, September 2007, pp. 284-289, DOI: 10.1109/VPPC.2007.4544139.

8. RFC7181: The Optimized Link State Routing Protocol Version 2 / T. Clausen, C. Dearlove, P. Jacquet, U. Herberg. – 2014. – URL: https://tools.ietf.org/html/rfc7181 (дата обращения: 21.05.2025).

9. Литвинов Г.А., Щерба Е.В. Применение моделей доверия и репутации для обеспечения для обеспечения безопасности маршрутизации в динамически организуемых сетях / Г.А. Литвинов, Е.В. Щерба // Вестник УрФО. Безопасность в информационной сфере, 2021. № 3(41). С. 12-23.

10. Литвинов Г.А. Экспериментальное исследование репутационной модели для поиска маршрута в самоорганизующихся сетях / Г.А. Литвинов // Вестник УрФО. Безопасность в информационной сфере, 2022. № 3. С. 69-75.

References

1. Nguyen V.L., Lin P.C., Hwang R.H. Energy Depletion Attacks in Low Power Wireless Networks, IEEE Access, 2019, Vol. 7, pp. 51915-51932, DOI: 10.1109/ACCESS.2019.2911424.

2. Desnickij V.A., Rudavin N.N. Modelirovanie i ocenka atak istoshhenija jenergoresursov na bespilotnye letatel'nye apparaty v sistemah antikrizisnogo upravlenija / V.A. Desnickij, N.N. Rudavin // Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MChS Rossii, 2019. № 4. S. 69-74.

3. Pu C. Energy Depletion Attack Against Routing Protocol in the Internet of Things, 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), January 2019, pp. 1-4, DOI: 10.1109/CCNC.2019.8651771.

4. Gong P., Chen T.M., Xu P. Resource-Conserving Protection against Energy Draining (RCPED) Routing Protocol for Wireless Sensor Networks, Network, 2022, Vol. 2(1), pp. 83-105, DOI: 10.3390/NETWORK2010007.

5. Kuaban G.S., Gelenbe E., Czachórski T., Czekalski P., Tangka J.K. Modelling of the Energy Depletion Process and Battery Depletion Attacks for Battery-Powered Internet of Things (IoT) Devices, Sensors (Basel), 2023, Vol. 23(13):6183, DOI: 10.3390/s23136183.

6. Sajja K.S., Bhowmik B. IoT Systems and Battery-Based Energy Sources, International Conference on Artificial Intelligence and Smart Communication (AISC), January 2023, pp. 212-219, DOI: 10.1109/AISC56616.2023.10085426.

7. Tremblay O., Dessaint L.A., Dekkiche A.I. A Generic Battery Model for the Dynamic Simulation of Hybrid Electric Vehicles, 2007 IEEE Vehicle Power and Propulsion Conference, September 2007, pp. 284-289, DOI: 10.1109/VPPC.2007.4544139.

8. RFC7181: The Optimized Link State Routing Protocol Version 2 / T. Clausen, C. Dearlove, P. Jacquet, U. Herberg. – 2014. – URL: https://tools.ietf.org/html/rfc7181 (дата обращения: 21.05.2025).

9. Litvinov G.A., Shcherba E.V. Primenenie modelej doverija i reputacii dlja obespechenija dlja obespechenija bezopasnosti marshrutizacii v dinamicheski organizuemyh setjah / G.A. Litvinov, E.V. Shcherba // Vestnik UrFO. Bezopasnost' v informacionnoj sfere, 2021. № 3(41). S. 12-23.

10. Litvinov G.A. Jeksperimental'noe issledovanie reputacionnoj modeli dlja poiska marshruta v samoorganizujushhihsja setjah / G.A. Litvinov // Vestnik UrFO. Bezopasnost' v informacionnoj sfere, 2022. № 3. S. 69-75.

ВАСИЛЬЕВ Артем Андреевич, аспирант федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». 644050, г. Омск, пр. Мира, 11. E-mail: dedaav55@gmail.com

СЕРГИН Даниил Альбертович, аспирант федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». 644050, г. Омск, пр. Мира, 11. E-mail: daniil0808_98@mail.ru

ЩЕРБА Евгений Викторович, кандидат технических наук, доцент, доцент кафедры «Комплексная защита информации» федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». 644050, г. Омск, пр. Мира, 11. E-mail: evscherba@gmail.com

VASILIEV Artem Andreevich, post-graduate student of the Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: dedaav55@gmail.com

SERGIN Daniil Albertovich, post-graduate student of the Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: daniil0808_98@mail.ru

SHCHERBA Evgeny Victorovich, Candidate of Engineering, Associate Professor, Department of Complex Information Protection, Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: evscherba@gmail.com