УДК 004.056.5:519.876.5 Вестник УрФО № 3(45) / 2022, с. 69–75

Литвинов Г.А.

DOI: 10.14529/secur220308

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ РЕПУТАЦИОННОЙ МОДЕЛИ ДЛЯ ПОИСКА МАРШРУТА В САМООРГАНИЗУЮЩИХСЯ СЕТЯХ [1]

Для решения проблемы обеспечения безопасности передачи данных в самоорганизующихся сетях можно использовать подход, основанный на применении моделей доверия. Использование модели доверия для определения репутации узлов позволяет изолировать узлы с низкой репутацией из сетевого взаимодействия и тем самым гарантировать безопасность передачи данных. В статье исследуется разработанная ранее репутационная модель и её имплементация для обеспечения безопасности маршрутизации на основе протокола OLSR. С целью исследования эффективности предложенного комплекса решений проведено имитационное моделирование на базе сетевого симулятора NS-3. Сценарий экспериментального исследования представлен в виде транзитной сети с некоторым количеством узлов нарушителей. В результате исследования получена экспериментальная оценка эффективности нового протокола и проведен сравнительный анализ полученных результатов.

Ключевые слова: *самоорганизующиеся сети, безопасность маршрутизации, репутационные модели, сетевые атаки, имитационное моделирование.*

Litvinov G. A.

EXPERIMENTAL ANALYSIS OF THE REPUTATIONAL MODEL FOR ROUTING IN SELF-ORGANIZING NETWORKS

To solve the problem of ensuring the security of data transmission in ad hoc networks, an approach based on the use of trust models can be used. Using the trust model to determine the reputation of nodes allows you to isolate nodes with a low reputation from network interaction and thereby guarantee the security of data transmission. The article examines the previously

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90100.

developed reputation model and its implementation to ensure routing security based on the OLSR protocol. In order to research the effectiveness of the proposed set of solutions, simulation modeling was carried out on the basis of the NS-3 network simulator. The scenario of the experimental research is presented in the form of a transit network with a certain number of intruder nodes. As a result of the research, an experimental assessment of the effectiveness of the new protocol was obtained and a comparative analysis of the results obtained was carried out. *Acknowledgments: The reported study was funded by RFBR, project number 20-37-90100.*

Keywords: *ad-hoc networks, MANET, routing security, reputation model, network attacks, network simulation.*

Введение

Различные модели и способы вычисления репутации широко применяются для самых разных задач, включая системы электронной торговли и социальные сети [1-3]. Применение репутационной модели в рамках самоорганизующейся сети позволяет избегать ненадёжные узлы с низкой репутацией при доставке пакетов и тем самым повысить безопасность процесса маршрутизации [4, 5]. Установление отношений доверия между узлами сети позволяет определять узлы нарушителей и исключать их из процесса сетевого взаимодействия. Узлы, препятствующие пересылке пакетов, не должны иметь доверия у других узлов сети. Определение доверия к узлам сети производится на основе вычисления значения репутации этих узлов другими узлами сети.

Для определения доверия в рамках процесса сетевого взаимодействия была разработана новая модель, основанная на вычислении репутации каналов связи и маршрутов доставки пакетов с использованием операций булевой алгебры [6]. В рамках разработанной модели был предложен способ определения локального значения репутации каждого канала связи путём отправки тестовых пакетов. Предложенный способ позволяет узлу определить репутацию каналов связи, входящих в маршрут между узлом, который отправил тестовое сообщение и узлом, к которому оно направлено. Производя проверку каналов связи с помощью тестовых пакетов, каждый узел формирует свою локальную базу значений репутации каналов связи в сети, а также производит широковещательную рассылку этих значений другим узлам сети.

Полученные значения репутации являются локальными, поскольку определяются в пределах конкретного узла сети. Значения локальной репутации не отражают объективную оценку репутации на основе наблюдений всех узлов сети. Нередко оценка одного узла может оказаться ошибочной и расходиться с оценками других узлов. Поэтому для получения более достоверной оценки необходимо использовать значения локальной репутации, полученные от всех узлов сети. Таким образом, значение глобальной репутации некоторого канала связи формируется в результате объединения значений локальной репутации от всех узлов сети. При этом конкретный способ определения глобальной репутации зависит от используемой репутационной модели.

В рамках разработанной репутационной модели значение глобальной репутации для каждого канала связи определяется как булевозначный вектор. Формирование значения глобальной репутации r(u, v) канала связи (u, v) между узлами u и v производится, используя значения локальной репутации $r_{vi}(u, v)$ этого канала связи, определяемые всеми соответствующими узлами сети v_i:

$$r(u, v) = (r_{v1}(u, v), r_{v2}(u, v), ..., r_{vn}(u, v))$$

Применение указанной репутационной модели позволяет найти наиболее безопасные маршруты от источника до каждого узла назначения. Для этого топология сети рассматривается как булевозначная сеть [7]. При этом стоимость дуги булевозначной сети определяется значением глобальной репутацией соответствующего канала связи. Для оценки безопасности маршрутов в сети была определена соответствующая вогнутая метрика безопасности маршрутов или глобальная репутация пути. Таким образом, метрика безопасности некоторого маршрута в самоорганизующейся сети определяется как мощность соответствующего пути в булевозначной сети. То есть, наиболее безопасным является путь, все дуги которого одновременно рекомендованы максимальным количеством узлов.

Для поиска наиболее безопасных маршрутов до узлов сети был разработан соответ-

ствующий эффективный алгоритм, основанный на булевозначном представлении сети передачи данных. Учитывая вогнутую метрику безопасности маршрутов, определенную в рамках репутационной модели, указанный алгоритм позволяет находить маршруты с наилучшей репутацией, что позволяет избегать узлы с низкой репутацией при доставке пакетов и тем самым повысить безопасность процесса маршрутизации.

Для имплементации, разработанной репутационной модели и алгоритма поиска наиболее безопасных маршрутов был выбран протокол маршрутизации OLSR, который является базовым проактивным протоколом маршрутизации для самоорганизующихся сетей [8]. Стандартная версия протокола не содержит механизмов защиты от внутренних нарушителей и скомпрометированных узлов сети. В результате имплементации была подготовлена имитационная модель протокола маршрутизации BOLSR [9].

Предложенная имплементация предлагает расширение существующих таблиц хранения данных о состояниях каналов связи, для хранения значений репутации. Оценка каналов связи сохраняется в виде вектора, содержащего адреса устройств, рекомендующих рассматриваемый канал связи. Также были предложены два дополнительных типа сообщений. Каждый узел периодически выполняет рассылку другим узлам сети скрытых проверочных сообщений запроса ECHO, маскируемых под полезный трафик. При получении запроса ECHO, узел должен направить ECHO ответ отправителю запроса. При получении ответа, узел определяет локальную репутацию всех каналов связи, образующих маршрут до получателя, как 1. В противном случае, если ответ не был получен в течение заданного временного интервала, локальная репутация всех каналов связи, образующих маршрут до получателя, устанавливается как 0. Широковещательная рассылка значений локальной репутации выполняется посредством сообщений RM.

Предложенная модель была реализована на базе распространенного сетевого симулятора с открытым исходным кодом NS-3 [10]. В ходе программной реализации разработанного протокола маршрутизации BOLSR была поставлена задача экспериментального исследования эффективности предложенного комплекса решений посредством имитационного моделирования.

Описание эксперимента

Для указанного экспериментального исследования был предложен сценарий взаимодействия удаленных узлов с использованием транзитной самоорганизующейся сети с некоторым количеством узлов нарушителей в этой сети. В данном сценарии узел нарушителя выполняет атаку «блэкхол», действия которой вызывают отброс всех передаваемых пакетов полезных данных, в то время как передача сообщений вспомогательных сетевых протоколов, включая протоколы маршрутизации, продолжается без изменений. Оценка эффективности была выполнена на основе сравнительного анализа результатов взаимодействия узлов при использовании протоколов OLSR и BOLSR.

На рис. 1 в качестве примера представлена одна из случайных сетевых топологий, использованных в рамках эксперимента, и обозначены маршруты доставки пакетов от отправителя до получателя, выбранные при помощи протоколов OLSR и BOLSR. Пунктирной линией ограничена область расположения транзитных узлов. Следует обратить внимание, что в предложенном примере при использовании протокола OLSR был выбран маршрут доставки пакетов через узел нарушителя. При этом, при использовании BOLSR был найден альтернативный маршрут доставки пакетов. Несмотря на то, что данный маршрут может не являться кратчайшим, маршрут исключает узлы нарушителей при доставке пакетов до получателя.

Основные параметры проведенной серии экспериментов в сетевом симуляторе NS-3 представлены в табл. 1. Каждая топология транзитной сети включает 50 устройств, положение которых определяется случайным образом согласно модели симулятора «Random Rectangle Position Allocator». Проверка связности между отправителем и получателем производилась с помощью отправки сетевого трафика с постоянной скоростью передачи (Constant Bit Rate, CBR).

Результатом каждого испытания является файл трассировки, включающий информацию о всех отправленных и полученных пакетах. Анализ файла трассировки позволяет определить коэффициент доставки пакетов (Packet Delivery Ratio, PDR).

Кроме того, в ходе каждого испытания фиксировалась расширенная таблица маршрутизации узла, выполняющего отправку пакетов. Расширенная версия таблицы маршру-

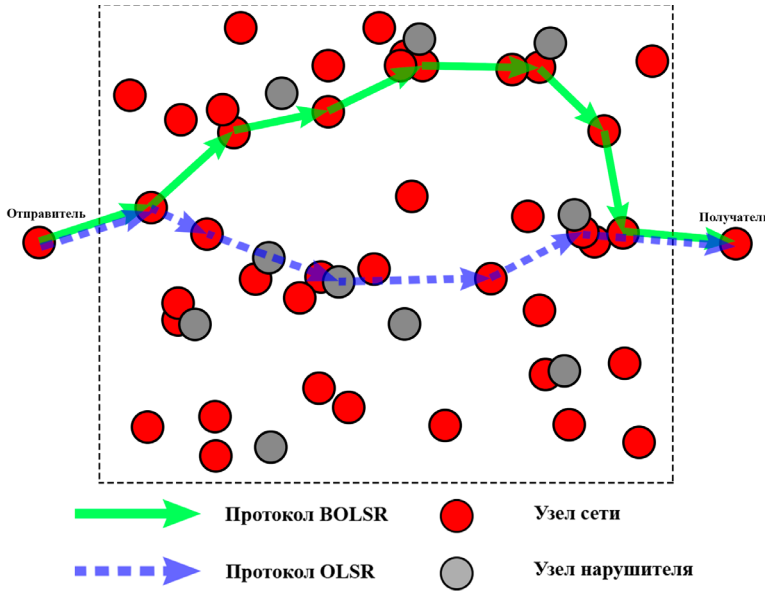

Рис. 1. Пример различного выбора маршрутов при использовании OLSR и BOLSR

Таблица 1

Предлагаемые параметры сценария эксперимента

Параметры эксперимента	Значение
Количество повторений	100
Время симуляции	180 с
Площадь расположения узлов	600м х 900м
Количество устройств в сети	52
Мобильность устройств	Статическая
Радиус взаимодействия	200 м
Протоколы маршрутизации	[OLSR, BOLSR]
Передаваемые данные	UDP
Частота отправки пакетов	1 с
Количество нарушителей	[0 - 6]
Наблюдаемые характеристики	Коэффициент доставки пакетов (Packet Delivery Ratio, PDR), Количество маршрутов через узлы нарушителей, Средняя длина маршрута

тизации, помимо адреса следующего перехода, включает также весь предполагаемый маршрут доставки пакетов до узла назначения. Полученная информация позволяет сравнить среднюю длину маршрутов до всех узлов сети, а также определить процентное отношение маршрутов, включающих узлы нарушителей. Указанные наблюдаемые характеристики позволили оценить эффективность предложенной репутационной модели поиска маршрутов и её программной реализации для имитационной модели протокола маршрутизации BOLSR.

Анализ результатов эксперимента

В результате проведения экспериментальных исследований, согласно описанному выше сценарию, была получена оценка эффективности предложенной репутационной модели для поиска маршрутов и ее программной реализации в рамках протокола BOLSR.

На рис. 2 представлены полученные графики зависимости коэффициентов доставки пакетов (Packet Delivery Ratio, PDR) от количества узлов нарушителей в транзитной сети для базового протокола маршрутизации OLSR и протокола BOLSR. Появление в транзитной сети хотя бы одного узла нарушителя приводит к тому, что некоторые из пакетов полезных данных не могут быть доставлены до получателя. Очевидно, что при увеличении количества нарушителей в транзитной сети, значение показателя PDR снижается в

любом случае. Важно, что при использовании протокола BOLSR это снижение происходит значительно медленнее по сравнению с базовым протоколом OLSR. Таким образом, по результатам экспериментальной оценки протокол BOLSR позволил повысить коэффициент доставки пакетов (на значение от 10% до 70%, в зависимости от количества нарушителей) по сравнению с базовым протоколом OLSR.

На рис. 3 представлен график зависимо-

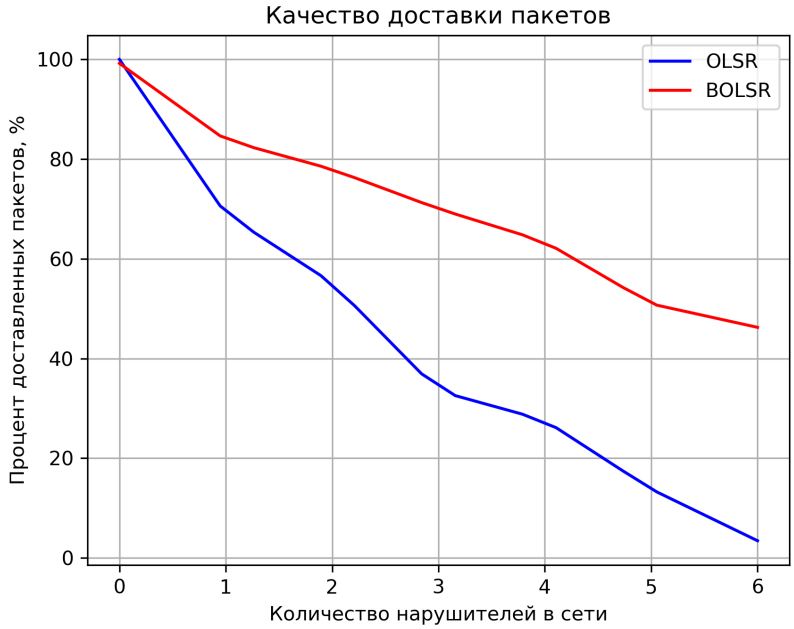

Рис. 2. Сравнение коэффициентов доставки пакетов при использовании OLSR и BOLSR

сти относительного количества маршрутов, проходящих через узлы нарушителей, от числа нарушителей. Можно отметить, что при увеличении числа узлов нарушителей в транзитной сети, относительное количество маршрутов через узлы нарушителей при использовании протокола BOLSR растёт медленнее по сравнению с базовым протоколом OLSR.

В то время как для протокола маршрутизации OLSR в качестве основной маршрутной

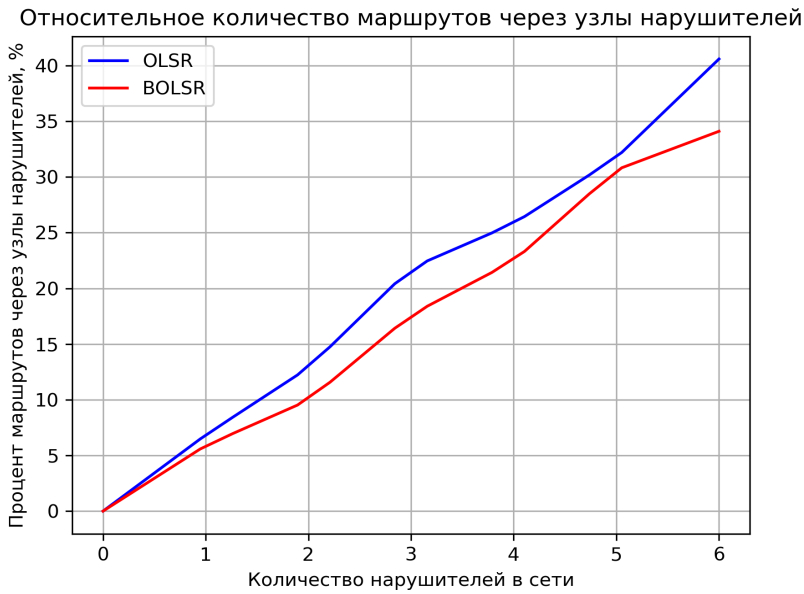

Рис. 3. Сравнение относительного количества маршрутов через узлы нарушителей при использовании OLSR и BOLSR

метрики используется количество переходов, в рамках протокола BOLSR была определена новая вогнутая метрика безопасности маршрутов, основанная на их репутации. Поскольку

маршруты с наилучшей репутацией не всегда являются кратчайшими относительно количества переходов, использование таких маршрутов может приводить к увеличению средней длины маршрутов в таблицах маршрутизации, что может негативно сказываться на других характеристиках сетевого взаимодействия, включая задержки и пропускную способность.

На рис. 4 представлен график, позволяющий оценить увеличение средней длины маршрутов до всех узлов в сети с увеличением количества нарушителей при использовании протокола BOLSR. Поскольку при использовании протокола OLSR выбор маршрутов доставки не зависит от поведения узлов сети, средняя длина маршрутов не изменяется при появлении узлов нарушителей в транзитной сети. Следует заметить, что применение протокола BOLSR вместо OLSR приводит лишь к незначительному увеличению средней длины маршрутов.

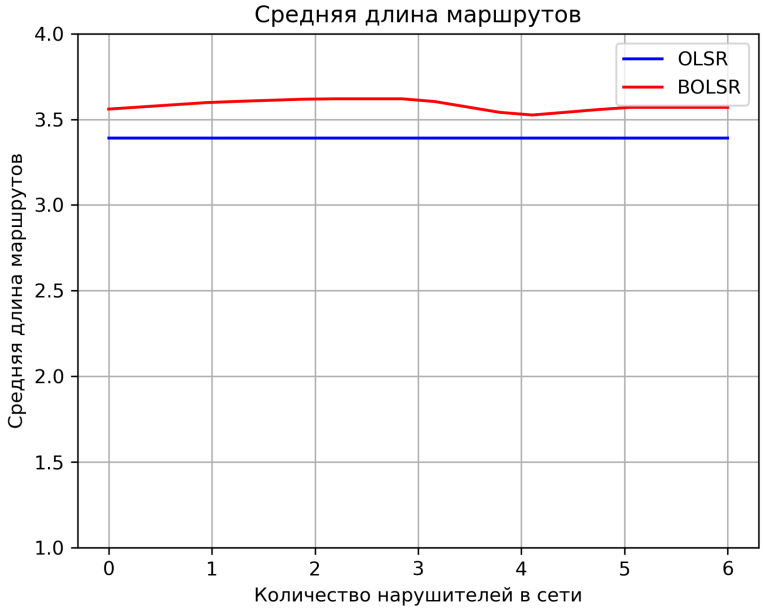

Рис. 4. Сравнение средней длины маршрутов при использовании OLSR и BOLSR

Заключение

Таким образом, в результате исследования была получена экспериментальная оценка эффективности протокола маршрутизации BOLSR для самоорганизующихся сетей, основанного на имплементации разработанной репутационной модели и алгоритма поиска наиболее безопасных маршрутов для существующего протокола маршрутизации OLSR. Указанная оценка позволила провести сравнительный анализ протоколов BOLSR и OLSR на основе объективных количественных характеристик, включая коэффициент доставки пакетов, относительное количество маршрутов через узлы нарушителей и среднюю длину маршрутов.

В частности, было зафиксировано, что при увеличении числа узлов нарушителей в сети, относительное количество маршрутов через узлы нарушителей для протокола BOLSR растёт медленнее по сравнению с исходным протоколом OLSR. Кроме того, по результатам экспериментальной оценки протокол BOLSR позволил повысить коэффициент доставки пакетов по сравнению с исходным протоколом OLSR. При этом, средняя длина маршрутов при использовании BOLSR по сравнению с оригинальным протоколом OLSR увеличилась незначительно. Указанные результаты свидетельствуют о том, что применение протокола BOLSR в самоорганизующихся сетях вместо протокола OLSR позволяет минимизировать влияние сетевых атак на доступность информации и, как следствие, повысить безопасность передачи данных в этих сетях при незначительном увеличении накладных расходов.

Литература

1. Braga D.D.S., Niemann M., Hellingrath B., Neto F.B.L. Survey on computational trust and reputation models // ACM Computing Surveys. 2018. Vol. 51, №5. P. 1–40.

2. Nosovsyi M.M., Degtiarev K.Yu. Reputation Systems in E-commerce: Comparative Analysis and Perspectives to Model Uncertainty Inherent in Them. Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS). 2019;31(3):99-122.

3. Al-Yazidi S.A., Berri J. and Hassan M.M. Novel hybrid model for organizations' reputation in online social networks. Journal of King Saud University-Computer and Information Sciences, 2022.

4. Овасапян Т.Д., Иванов Д.В. Обеспечение безопасности WSN-сетей на основе модели доверия // Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 64–72.

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

6. Shcherba E. V., Litvinov G. A., Shcherba M. V. A novel reputation model for trusted path selection in the OLSR routing protocol //2019 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2019. – С. 1–5.

7. Салий В.Н. Оптимизация в булевозначных сетях // Дискретная математика. – 2005. – Т. 17, № 1. – С. 141–146.

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

9. Litvinov G., Shcherba E. Implementation of the Reputation Model for Secure Routing Based on the OLSR Protocol //2021 International Conference Engineering and Telecommunication (En&T). – IEEE, 2021. – С. 1–4.

10. Свидетельство о государственной регистрации программы для ЭВМ 2021661846 Российская Федерация. Репутационный модуль поиска наиболее безопасных маршрутов для протокола маршрутизации OLSR: № 2021661027: заявл. 14.07.2021: опубл. (зарег.) 16.07.2021 / Г. А. Литвинов, Е. В. Щерба; заявитель ОмГТУ.

References

1. Braga D.D.S., Niemann M., Hellingrath B., Neto F.B.L. Survey on computational trust and reputation models // ACM Computing Surveys. 2018. Vol. 51, №5. P. 1–40.

2. Nosovsyi M.M., Degtiarev K.Yu. Reputation Systems in E-commerce: Comparative Analysis and Perspectives to Model Uncertainty Inherent in Them. Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS). 2019;31(3):99-122.

3. Al-Yazidi S.A., Berri J. and Hassan M.M. Novel hybrid model for organizations' reputation in online social networks. Journal of King Saud University-Computer and Information Sciences, 2022.

4. 4. Ovasapyan T.D., Ivanov D.V. Obespecheniye bezopasnosti WSN-setey na osnove modeli doveriya // Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy. 2017. № 4. P. 64–72.

5. 5. Litvinov G.A., Shcherba Ye.V. Primeneniye modeley doveriya i reputatsii dlya obespecheniya bezopasnosti marshrutizatsii v dinamicheski organizuyemykh setyakh // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2021. – №. 3 (41). – P. 12–23.

6. Shcherba E. V., Litvinov G. A., Shcherba M. V. A novel reputation model for trusted path selection in the OLSR routing protocol //2019 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2019. – P. 1–5.

7. Saliy V.N. Optimizatsiya v bulevoznachnykh setyakh // Diskretnaya matematika. – 2005. – T. 17, № 1. – P. 141–146.

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

9. Litvinov G., Shcherba E. Implementation of the Reputation Model for Secure Routing Based on the OLSR Protocol //2021 International Conference Engineering and Telecommunication (En&T). – IEEE, 2021. – P. 1–4.

10. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM 2021661846 Rossiyskaya Federatsiya. Reputatsionnyy modul' poiska naiboleye bezopasnykh marshrutov dlya protokola marshrutizatsii OLSR: № 2021661027: zayavl. 14.07.2021: opubl. (zareg.) 16.07.2021 / G. A. Litvinov, Ye. V. Shcherba; zayavitel' OmGTU.

ЛИТВИНОВ Георгий Александрович, аспирант кафедры комплексной защиты информации, Омский государственный технический университет, 644050, г. Омск, пр. Мира, 11. E-mail: georgyfunds@gmail.com

LITVINOV George, Graduate student, Department of Complex Information Protection, Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: georgyfunds@gmail.com