УДК 004 DOI:10.31854/1813-324X-2020-6-1-94-98

Методика обнаружения аномального взаимодействия пользователей с информационными активами для выявления инсайдерской деятельности

М.А. Поляничко[1]

[1]Санкт-Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург, 190031, Российская Федерация
*Адрес для переписки: polyanichko@pgups.ru

Информация о статье
Поступила в редакцию 05.11.2019
Принята к публикации 03.03.2020

Ссылка для цитирования: Поляничко М.А. Методика обнаружения аномального взаимодействия пользователей с информационными активами для выявления инсайдерской деятельности // Труды учебных заведений связи. 2020. Т. 6. № 1. С. 94–98. DOI:10.31854/1813-324X-2020-6-1-94-98

Аннотация: *Выявление инсайдеров и инсайдерской деятельности в организации – актуальное направление обеспечения информационной безопасности, так как высокий уровень развития программных и аппаратных средств защиты информации выводит на первый план злоумышленные действия легитимных пользователей. В данной статье рассматривается методика, позволяющая выявлять аномалии во взаимодействии работников организации с информационными активами, и оценивается ее применимость в условиях проведения работ по обнаружению злонамеренной деятельности инсайдеров.*

Ключевые слова: *инсайдер, аномальное взаимодействие, инсайдерские угрозы, косинусное сходство, статистическая мера IDF, информационная безопасность.*

Введение

Любая современная организация представляет собой взаимосвязанное информационное пространство, обеспечивающее возможности доступа к информации и ее совместной обработке. В этих условиях многие из наиболее опасных потенциально возможных инцидентов информационной безопасности связаны с злоумышленными действиями легитимных пользователей – инсайдеров [1]. Выявление инсайдеров – направление, которое с каждым годом становится все более актуальным [12]. Совершенствование программных и аппаратных средств защиты информации, развитие криптографических алгоритмов, популяризация портативных устройств и облачных хранилищ выводят инсайдерские угрозы на первый план [3, 4]. Существуют различные способы выявления инсайдерских угроз [5]. Большинство из них базируется на анализе различных технических и инструментальных показателей, таких как сетевая активность, использование периферийных устройств, загруженность системы, интенсивность взаимодействия с информационными системами и т. п. Это связано с тем, что многие методы противодействия инсайдерам развиваются под влиянием подходов, которые используются для обнаружения внешних угроз [6], в частности, для мониторинга сети и обнаружения вторжений. Современные системы обнаружения вторжений (IDS, *от англ.* Intrusion Detection System) внедряются для выявления атак в реальном времени, используют базу данных шаблонов (сигнатур) атак, методы машинного обучения, могут регистрировать множество данных, характеризующих взаимодействие работников с информационными активами организации, и хорошо зарекомендовали себя при решении задачи обнаружения внешних угроз [7, 8]. В статье предлагается рассмотреть возможность использования информации о взаимодействии работников с информационными активами для определения инсайдерских угроз и выявления инсайдеров.

Выявление аномалий при взаимодействии работников с информационными активами организации

Существуют различные подходы к анализу действий пользователей и выявлению отклонений от нормального поведения [6, 9, 10]. В данной работе

рассматривается методика, которая базируется на использовании двудольного графа [11, 12] для отражения взаимодействия субъектов (пользователей/работников организации) с объектами (информационными системами и активами) на основании данных сети, собираемых IDS [13]. Множество субъектов обозначим $S = \{s_1, s_2, \dots, s_n\}$, объекты определим множеством $O = \{o_1, o_2, \dots, o_n\}$, а набор пользователей, которые обращались к объектам o_i за какой-то определенный период времени, множеством S_{O_i}. Обозначением Gr_{O_i} определим полный граф S_{O_i}, где значением веса между парами вершин выступает величина сходства.

Двудольный граф, отражающий факт обращения субъектов к объектам, обозначим двоичной матрицей OS. При этом $OS(i,j) = 1$, если пользователь s_i осуществляет доступ к объекту o_i, и $OS(i,j) = 0$, если – нет. Для оценки связности субъектов с объектами предлагается использовать статистическую меру IDF (*от англ.,* Inverse Document Frequency). Мера IDF – обратная частота документа, представляет собой инверсию частоты, с которой некоторое слово встречается в документах коллекции и обозначается формулой:

$$IDF(S_i) = \log \frac{|O|}{1 + E \cdot S_i}, \quad (1)$$

где $E = \{1, 1, \dots, 1\}$ – единичный вектор n-ой размерности; $|O|$ – мощность множества O; S_i – столбец субъекта матрицы OS (вектор доступа).

Полученную после трансформации матрицу обозначим IDF_OS. Сходство между парами субъектов может быть получено на основе их векторов доступа. Для измерения схожести двух векторных объектов предлагается использовать косинусное сходство [14]:

$$Sim(s_i, s_j) = \frac{IDF_{S_i} \times IDF_{S_j}}{\|IDF_{S_i}\| \times \|IDF_{S_j}\|} = \frac{\sum_{k=1}^{m} IDF_{S_{i,k}} \times IDF_{S_{j,k}}}{\sqrt{\sum_{k=1}^{m} \left(IDF_{S_{i,k}}\right)^2} \times \sqrt{\sum_{k=1}^{m} \left(IDF_{S_{j,k}}\right)^2}}. \quad (2)$$

Если даны два вектора признаков: A и B, то косинусное сходство может быть представлено, используя скалярное произведение и норму. В случае информационного поиска косинусное сходство двух документов изменяется в диапазоне от 0 до 1, поскольку частота терма не может быть отрицательной. Угол между двумя векторами частоты терма не может быть больше, чем 90 °. Одна из причин популярности косинусного сходства состоит в том, что оно эффективно в качестве оценочной меры, особенно для разреженных векторов, так как необходимо учитывать только ненулевые измерения [15].

В результате вычислений будет получена матрица сходства взаимодействия пользователей с информационными активами (субъектов с объектами). Предполагается, что в случае, если один из пользователей является инсайдером, то его действия отразятся на матрице сходства. Вокруг каждого объекта образуется индивидуальная группа субъектов, которые с ним работают и к нему обращаются. Для вычисления сходства между группами пользователей необходимо вычислить среднее сходство между всеми парами пользователей (общее сходство пользователей):

$$Sim(Gr_{O_k}) = \frac{\forall s_i \neq s_j \in S_{O_k} \forall s_j \sum Sim(s_i, s_j)}{\frac{|S_{O_k}| \times (|S_{O_k}| - 1)}{2}}, \quad (3)$$

где $|S_{O_k}|$ – количество субъектов в группе пользователей.

Если $Sim(Gr_{O_k})$ имеет высокое значение, то это означает, что субъекты имеют сильное взаимодействие относительно объекта o_k. Для выявления аномальных действий субъекта необходимо исключить его из группы и посчитать среднее сходство для получившейся подгруппы:

$$Rate(s_j, o_i) = Sim\left(Gr_{O_{ij}}\right) - Sim(Gr_{O_i}), \quad (4)$$

где $Gr_{O_{ij}}$ – подгруппа субъектов без пользователя o_j.

Чем выше значение $Rate(s_j, o_i)$, тем вероятнее, что доступ субъекта s_j к объекту o_i является аномальным.

Предлагаемая методика выявления аномальных действий пользователей на основе анализа сетевых данных может быть представлена в виде последовательности шагов.

Шаг 1. Построение множества субъектов и объектов.

Шаг 2. Построение двудольного графа взаимодействия.

Шаг 3. Вычисление статистической меры IDF.

Шаг 4. Вычисление матрицы сходства действий пользователей.

Шаг 5. Вычисление общего сходства действий пользователя.

Шаг 6. Выявление аномальных действий.

Рассмотрим действие методики на абстрактном примере. Предположим, что в организации имеется шесть субъектов $S = \{s_1, s_2, s_3, s_4, s_5, s_6\}$ и семь информационных активов $O = \{o_1, o_2, o_3, o_4, o_5, o_6, o_7\}$. Тогда двудольный граф взаимодействий пользователей с информационными активами можно описать бинарной матрицей OS размерностью 6×7 [6]:

$$OS = \begin{Bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{Bmatrix}.$$

На следующем шаге необходимо вычислить статистическую меру инверсии частоты IDF:

$$IDF(S_1) = \log\frac{|O|}{1 + E \cdot S_1} = \log\frac{7}{1+4} \approx 0{,}15$$

.....

$$IDF(S_6) = \log\frac{|O|}{1 + E \cdot S_1} = \log\frac{7}{1+2} \approx 0{,}37$$

Полученные значения IDF необходимо подставить в матрицу инверсий частот IDF_OS по правилу $IDF\_OS_{i,j} = \begin{cases} IDF(S_i), & \text{если } OS_{i,j} = 1 \\ 0, & \text{если } OS_{i,j} = 0 \end{cases}$:

$$IDF\_OS = \begin{Bmatrix} 0{,}15 & 0 & 0{,}15 & 0 & 0 & 0 \\ 0{,}15 & 0{,}15 & 0{,}15 & 0{,}15 & 0{,}15 & 0 \\ 0{,}15 & 0{,}15 & 0 & 0{,}15 & 0{,}15 & 0{,}37 \\ 0{,}15 & 0 & 0 & 0 & 0 & 0{,}37 \\ 0 & 0{,}15 & 0 & 0{,}15 & 0{,}15 & 0 \\ 0 & 0 & 0{,}15 & 0 & 0 & 0 \\ 0 & 0{,}15 & 0{,}15 & 0{,}15 & 0{,}15 & 0 \end{Bmatrix}.$$

Далее вычисляется матрица сходства действий пользователей [14]:

$$Sim(s_1, s_2) = \frac{IDF_{S_1} \cdot IDF_{S_2}}{\|IDF_{S_1}\| \times \|IDF_{S_2}\|} =$$

$$= \frac{\sum_{k=1}^{m} IDF_{S_{1,k}} \times IDF_{S_{2,k}}}{\sqrt{\sum_{k=1}^{m}\left(IDF_{S_{1,k}}\right)^2} \times \sqrt{\sum_{k=1}^{m}\left(IDF_{S_{2,k}}\right)^2}} =$$

$$= \frac{2 * (0{,}15)^2}{\sqrt{4 * (0{,}15)^2} \times \sqrt{4 * (0{,}15)^2}} = 0{,}5$$

.....

$$Sim(s_1, s_6) = \frac{IDF_{S_1} \cdot IDF_{S_6}}{\|IDF_{S_1}\| \times \|IDF_{S_6}\|} =$$

$$= \frac{\sum_{k=1}^{m} IDF_{S_{1,k}} \times IDF_{S_{6,k}}}{\sqrt{\sum_{k=1}^{m}\left(IDF_{S_{1,k}}\right)^2} \times \sqrt{\sum_{k=1}^{m}\left(IDF_{S_{6,k}}\right)^2}} =$$

$$= \frac{2 * 0{,}15 * 0{,}37}{\sqrt{4 * (0{,}15)^2} \times \sqrt{2 * (0{,}37)^2}} = 0{,}71$$

.....

$$im(s_5, s_6) = \frac{IDF_{S_5} \cdot IDF_{S_6}}{\|IDF_{S_5}\| \times \|IDF_{S_6}\|} =$$

$$= \frac{\sum_{k=1}^{m} IDF_{S_{5,k}} \times IDF_{S_{6,k}}}{\sqrt{\sum_{k=1}^{m}\left(IDF_{S_{5,k}}\right)^2} \times \sqrt{\sum_{k=1}^{m}\left(IDF_{S_{6,k}}\right)^2}} =$$

$$= \frac{0{,}15 * 0{,}37}{\sqrt{4 * (0{,}15)^2} \times \sqrt{2 * (0{,}37)^2}} = 0{,}58,$$

$$Sim(IDF_{OS}) = \begin{Bmatrix} 1 & & & & \\ 0{,}50 & 1 & & & \\ 0{,}50 & 1 & 1 & & \\ 0{,}50 & 1 & 1 & 1 & \\ 0{,}71 & 0{,}58 & 0{,}58 & 0{,}58 & 1 \end{Bmatrix}.$$

Вычисляется общее сходство действий пользователя:

$$Sim(s_1, s_2, s_4, s_5, s_6) = \frac{\forall s_i \neq s_j \in S_{O_k} \forall s_j \sum Sim(s_i, s_j)}{\frac{|s_{O_k}| \times (|s_{O_k}| - 1)}{2}} =$$

$$= 6{,}95/10 = 0{,}69,$$

$$Sim(s_2, s_4, s_5, s_6) = 4{,}74/6 = 0{,}79,$$

$$Sim(s_1, s_4, s_5, s_6) = 4{,}37/6 = 0{,}73,$$

$$Sim(s_1, s_2, s_5, s_6) = 5{,}37/6 = 0{,}89,$$

$$Sim(s_1, s_2, s_4, s_6) = 5{,}37/6 = 0{,}89,$$

$$Sim(s_1, s_2, s_4, s_5) = 6{,}95/6 = 1{,}16.$$

Выявляются аномальные действия по отношению к объекту o_3:

$$Rate(s_1, o_3) = Sim\left(Gr_{O_{ij}}\right) - Sim(Gr_{O_i}) =$$

$$= 0{,}79 - 0{,}69 = 0{,}10,$$

$$Rate(s_2, o_3) = 0{,}73 - 0{,}69 = 0{,}04,$$

$$Rate(s_4, o_3) = 0{,}89 - 0{,}69 = 0{,}20,$$

$$Rate(s_5, o_3) = 0{,}89 - 0{,}69 = 0{,}20,$$

$$Rate(s_6, o_3) = 1{,}16 - 0{,}69 = 0{,}47.$$

По результатам моделирования выявлено, что s_6, o_3 является аномальным, так как имеет самое большое отклонение от нормального поведения. Аномальное поведение может быть вызвано множеством факторов, в том числе и инсайдерской деятельностью [16]. При этом надо отметить, что в качестве меры сходства действий пользователя также рассматривалось евклидово расстояние. Но его применение оказалось менее эффективным, так как евклидово расстояние более чувствительно к порядку следования значений в векторе и дает более низкие оценки сходства, например, сходства $d(s_1, s_2) = 0{,}25$.

Заключение

Таким образом, можно сделать вывод, что приведенная методика позволяет определить, что взаимодействие пользователя с каким-то информационным активом организации носит аномальный характер. Данные могут быть переданы администратору информационной безопасности для дальнейшего анализа.

Тем не менее, этот подход не позволяет достоверно определить, является ли данная активность инсайдерской деятельностью, так как такой анализ не учитывает контекст взаимодействия и причину его возникновения. Например, возможно, что подобное взаимодействие происходит в рамках выполнения поручения руководства, которое необходимо оперативно выполнить: например, deadline. Применение данной методики целесообразно в совокупности с анализом других показателей, позволяющих определить наличие у работника склонности к инсайдерской деятельности, например, с использованием метода оценивания актуальности инсайдерских угроз на основе нечеткого анализа иерархий [17].

Список используемых источников

1. Insider Threat Report: Out of sight should never be out of mind // Verizon Threat Research Advisory Center. URL: https://enterprise.verizon.com/resources/reports/verizon-threat-research-advisory-center (дата обращения: 12.01.2020)
2. Информационная безопасность на практике // Код Безопасности. URL: https://www.securitycode.ru/documents/analytics/informatsionnaya-bezopasnost-na-praktike (дата обращения: 12.08.2019)
3. Insider Threat Report: 2018 – CA Technologies // CA Technologies. URL: https://www.ca.com/content/dam/ca/us/files/ ebook/insider-threat-report.pdf (дата обращения: 18.07.2018)
4. Буйневич М.В., Васильева И.Н., Воробьев Т.М., Гниденко И.Г., Егорова И.В., Еникеева Л.А. и др. Защита информации в компьютерных системах. СПб.: Изд-во Санкт-Петербургский государственный экономический университет, 2017. 163 с.
5. Homoliak I., Toffalini F., Guarnizo J., Elovici Y., Ochoa M. Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures // ACM Computing Surveys. 2019. Vol. 52. Iss. 2. DOI:10.1145/3303771
6. Chen Y., Steve Nyemba, Zhang W., Malin B. Specializing network analysis to detect anomalous insider actions // Security Informatics. 2012. Vol. 1. Iss. 5. DOI:10.1186/2190-8532-1-5
7. Kumar S. Classification and detection of computer intrusions. PhD Thesis. West Lafayette: Purdue University Publ., 1995.
8. Zeadally S., Yu B., Jeong D.H., Liang L. Detecting Insider Threats Solutions and Trends // Information Security Journal: A Global Perspective. 2012. Vol. 4. Iss. 21. PP. 183–192. DOI:10.1080/19393555.2011.654318
9. Eberle W., Holder L. Insider Threat Detection Using Graph-Based Approaches // Proceedings of Conference for Homeland Security. Cybersecurity Applications & Technology (CATCH' 09). 2009. PP. 237–241. DOI:10.1109/CATCH.2009.7
10. Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86–97. DOI:10.31854/1813-324X-2019-5-3-86-97
11. Chen Y, Malin B: Detection of anomalous insiders in collaborative environments via relational analysis of access logs // Proceedings of the 1th ACM Conference on Data and Application Security and Privacy (CODASPY'11, San Antonio, USA, February 2011). New York: Association for Computing Machinery Publ., 2011. PP. 63–74. DOI:10.1145/1943513.1943524
12. Белов В.В., Воробьев Е.М., Шаталов В.Е. Теория графов. М.: Высшая школа, 1976. С. 392.
13. Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. М.: Наука, 1990. 384 с.
14. Sarwar B., Karypis G., Konstan J., Riedl J. Item-based collaborative filtering recommendation algorithms // Proceedings of the 10th International Conference on World Wide Web (WWW' 2001, Hong Kong, Chinese, April 2001). New York: ACM Publ., 2001. PP. 285–295. DOI:10.1145/371920.372071
15. Daniel J., James H.M. Speech and Language Processing. An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition. Upper Saddle River, New Jersey: Prentice Hall, 2008. 1024 p.
16. Поляничко М.А. Формирование понятийного аппарата в области противодействия инсайдерской деятельности // Современная наука: Актуальная проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 6-2. С. 94–97.
17. Поляничко М.А., Королев А.И. Подход к выявлению инсайдерских угроз в организации // Естественные и технические науки. 2018. №9(123). 2018. С. 152–154.
18. Поляничко М.А., Пунанова К.В. Оценивание актуальности инсайдерских угроз на основе нечеткого метода анализа иерархий // Вестник Воронежского института МВД России. 2019. № 3. С. 88–98.

* * *

Methodology for Detecting Anomalous Interaction of Users with Information Assets to Identify Insider Activity

M. Polyanichko[1]

[1]Emperor Alexander Ist. Petersburg State Transport University,
St. Petersburg, 190031, Russian Federation

Article info
DOI:10.31854/1813-324X-2020-6-1-94-98
Received 5th November 2019
Accepted 3nd March 2020

For citation: Polyanichko M. Methodology for Detecting Anomalous Interaction of Users with Information Assets to Identify Insider Activity. *Proc. of Telecom. Universities.* 2020;6(1):94–98. (in Russ.) DOI:10.31854/1813-324X-2020-6-1-94-98

Abstract: *The article describe us that the identification of insiders and insider activities in the organization is an actual direction of ensuring information security, since the high level of software development and hardware information protection brings the malicious actions of legitimate users to the fore. This article discusses the methodology which allows to identify anomalies in the organization's employees interaction with information assets and its applicability is assessed in the context of work to detect malicious activities of insiders.*

Keywords: *insider, anomaly detection, insider threats, cosine similarity, IDF statistical measure, intrusion detection system.*

References

1. Verizon Threat Research Advisory Center. *Insider Threat Report: Out of sight should never be out of mind*. Available from: https://enterprise.verizon.com/resources/reports/verizon-threat-research-advisory-center [Accessed 12th January 2020]

2. Security code. *Information Security in Practice.* (in Russ) Available from: https://www.securitycode.ru/documents/analytics/informatsionnaya-bezopasnost-na-praktike [Accessed 12th August 2019]

3. Insider Threat Report: 2018 – CA Technologies // CA Technologies URL: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (дата обращения: 18.07.2018).

4. Buynevich M.V., Vasilyeva I.N., Vorobev T.M., Gnidenko I.G., Egorova I.V., Enikeeva L.A. et al. *Information Security in Computer Systems*. St. Petersburg: Saint Petersburg State University of Economics Publ.; 2017. 163 p. (in Russ.)

5. Homoliak I., Toffalini F., Guarnizo J., Elovici Y., Ochoa M. Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Computing Surveys*. 2019;52(2). DOI:10.1145/3303771

6. Chen Y., Steve Nyemba, Zhang W., Malin B. Specializing network analysis to detect anomalous insider actions. *Security Informatics*. 2012;1(5). DOI:10.1186/2190-8532-1-5

7. Kumar S. *Classification and detection of computer intrusions*. PhD Thesis. West Lafayette, IN: Purdue University; 1995.

8. Zeadally S., Yu B., Jeong D.H., Liang L. Detecting Insider Threats Solutions and Trends. *Information Security Journal: A Global Perspective*. 2012;4(21):183–192. DOI:10.1080/19393555.2011.654318

9. Eberle W., Holder L. Insider Threat Detection Using Graph-Based Approaches. *Proceedings of Conference for Homeland Security. Cybersecurity Applications & Technology (CATCH' 09)*. 2009. p.237–241. DOI:10.1109/CATCH.2009.7

10. Krasov A., Petriv R., Sakharov D., Storozhuk N., Ushakov I. Scalable Honeypot Solution for Corporate Networks Security Provision. *Proc. of Telecom. Universities*. 2019;5(3):86–97. (in Russ.) DOI:10.31854/1813-324X-2019-5-3-86-97

11. Chen Y, Malin B: Detection of anomalous insiders in collaborative environments via relational analysis of access logs. *Proceedings of the 1th ACM Conference on Data and Application Security and Privacy, CODASPY'11, February 2011, San Antonio, USA*. New York: Association for Computing Machinery Publ.; 2011. p.63–74. DOI:10.1145/1943513.1943524

12. Belov V.V., Vorobev E.M., Shatalov V.E. *Graph Theory*. Moscow: Vysshaia shkola Publ.; 1976. P. 392. (in Russ)

13. Emelichev V.A., Melnikov O.I., Sarvanov V.I., Tyshkevich R.I. Lectures on Graph Theory. Moscow: Nauka Publ.; 1990. 384 p. (in Russ)

14. Sarwar B., Karypis G., Konstan J., Riedl J. Item-based collaborative filtering recommendation algorithms. *Proceedings of the 10th International Conference on World Wide Web, WWW' 2001, April 2001, Hong Kong, Chinese.* New York: ACM Publ.; 2001. p.285–295. DOI:10.1145/371920.372071

15. Daniel J., James H.M. *Speech and Language Processing. An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition*. Upper Saddle River, New Jersey: Prentice Hall; 2008. 1024 p.

16. Polyanichko M.A. Formation of definition complex for insider counteraction scope. *Modern Science: actual problems of theory and practice. Series of Natural and Technical Sciences*. 2019;6-2:94–97. (in Russ)

17. Polyanichko M.A., Korolev A.I. Organization Insider Identification Approach. *Natural and technical sciences*. 2018;9(123): 152–154. (in Russ)

18. Polyanichko M.A., Punanova K.V. Insider Threats Evaluation Based on the Fuzzy Analytic Hierarchy Process. *The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2019;3:88–98 (in Russ)

Сведения об авторах:

ПОЛЯНИЧКО Марк Александрович кандидат технических наук, доцент кафедры «Информатика и информационная безопасность» Санкт-Петербургского государственного университета путей сообщения Императора Александра I, polyanichko@pgups.ru
https://orcid.org/0000-0002-8817-7921

DOI:10.31854/1813-324X-2020-6-1