DOI 10.36622/VSTU.2023.26.1.009
УДК 004.732

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ РЕАЛИЗАЦИИ АТАК, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ ПРИКЛАДНОГО И СЕТЕВОГО УРОВНЕЙ, НА СЕНСОРНЫЕ УСТРОЙСТВА ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, Д.Р. Серых, А.А. Болгов, И.Л. Батаронов, А.С. Кривошеин

В статье предлагается методика оценки и регулирования рисков для повышения защищенности сенсорных устройств промышленного Интернета вещей от атак, использующих уязвимости прикладного и сетевого уровней, направленных на нарушение конфиденциальности, целостности и доступности информации. Методика позволяет проводить оценку риска с учетом основных технических характеристик программных, аппаратных и прошивочных уязвимостей. Процесс регулирования риска включает в себя переоценку риска реализации атаки на конкретное устройство с учётом использования мер противодействия. Представлен программный инструментарий, для оценки и регулирования рисков, позволяющий сравнивать значения риска при использовании различных мер противодействия ему. Полученные результаты в виде количественной оценки позволяют провести анализ рисков реализации возможных атак на каждое из устройств сети, выявлять наиболее уязвимые элементы сети, а также подобрать меры для снижения уровня риска до необходимого значения.

Ключевые слова: промышленный Интернет вещей, риск, атака, конфиденциальность, целостность, доступность.

Введение

Быстрое развитие Интернета вещей (IoT) [1] и его способность предлагать различные виды услуг сделали его самой быстро растущей технологией, оказывающей огромное влияние на социальную жизнь и бизнес-среду. Интернет вещей постепенно проник во все аспекты современной человеческой жизни, такие как образование здравоохранение, включая хранение конфиденциальной информации о людях и компаниях, транзакции с финансовыми данными, разработку продуктов и маркетинг.

Широкое распространение устройств, подключенных в Интернете вещей создало огромный спрос на формирование дополнительных механизмов обеспечения безопасности в ответ на растущий спрос миллионов или, возможно, миллиардов подключенных устройств и услуг по всему миру [2].

С каждым днем количество угроз, масштабность и сложность атак продолжают увеличиваться. Мало того, число потенциальных злоумышленников вместе с размером сетей растет, а и инструменты, доступные потенциальным злоумышленникам, становятся все более изощренными и действенными [3]. Поэтому для того, чтобы Интернет вещей достиг максимально полного потенциала, ему необходима эффективная защита от угроз и уязвимостей [4].

Актуальность настоящего исследования обусловлена следующими факторами:

– быстрым ростом количества и доступности устройств Интернета вещей;

– отсутствием необходимых и достаточных статистических данных о причиненном ущербе, что снижает достоверность оценки рисков и ставит под угрозу безопасность систем Интернета вещей на этапе проектирования;

– слабой защищенностью устройств Интернета вещей, что вызывает большой интерес со стороны злоумышленника;

– отсутствием стандартов безопасности Интернета вещей;

– необходимостью разработки методических и алгоритмических обеспечений оценки и регулирования риска для сетей Интернета вещей;

– необходимостью разработки инструментария автоматизированной оценки риска и его регулирования.

Однако, несмотря на существующие работы [5, 6], связанные с повышением защищенности сетей Интернета вещей, проблема получения количественной оценки риска и его регулирования при реализации атак на устройства Интернета вещей остается недостаточно исследованной. При анализе существующих методик, связанных с темой исследования, были выявлены следующие противоречия:

– между потребностью в количественных оценках рисков защищенности сенсорных устройств промышленного Интернета вещей в условиях атаки на прикладной или сетевой уровни и несовместимостью подобных инструментов в имеющихся методиках для решения этого класса задач.

– между необходимостью регулирования рисков необходимых для повышения защищенности сенсорных устройств промышленного Интернета вещей в условиях атаки на прикладной или сетевой уровни и недостаточными возможностями существующих методик.

– между необходимостью повышения степени защищенности сенсорных устройств промышленного Интернета вещей и недостаточной эффективностью инструментария, позволяющего провести своевременный риск-анализ объекта исследования.

Цель данного исследования заключается в разработке алгоритмического и методического обеспечений для оценки и регулирования рисков, необходимых для повышения защищенности сенсорных устройств промышленного Интернета вещей в условиях атаки на прикладной или сетевой уровень.

При детальном изучении выбранной темы исследования были поставлены и решены следующие задачи:

– предложить методическое и алгоритмическое обеспечения для оценки рисков необходимых для повышения защищенности сенсорных устройств промышленного Интернета вещей в условиях атаки на прикладной или сетевой уровни;

– создать необходимые и достаточные методическое и алгоритмическое обеспечения для регулирования рисков успешной реализации атак, использующих уязвимости прикладного и сетевого уровней, на сенсорные устройства промышленного Интернета вещей;

– реализовать программно-технический комплекс автоматизированной оценки и регулирования рисков успешности атак, использующих уязвимости прикладного и сетевого уровней, на сенсорные устройства промышленного Интернета вещей.

Методика оценки риска

В настоящее время существует множество способов оценки риска [7]. В данной работе производить оценку риска предлагается на основе метода EBIOS RM. Предлагаемый подход позволяет проводить оценку риска с учетом основных технических характеристик программных, аппаратных и прошивочных уязвимостей, определять меры безопасности. Методика позволяет проводить оценку как уязвимости сенсорных устройств промышленного Интернета вещей, так и эффективности атак по каждой уязвимости, что повышает точность и объективность оценки рисков. Метод можно использовать, для:

– создания или улучшения процесса управления риском;

– оценки и анализа рисков;

– определения уровня безопасности, который должен быть достигнут для продукта или сети в соответствии с угрозами, которым необходимо противодействовать.

Для оценки рисков реализации атак, использующих уязвимости прикладного и сетевого уровня, на сенсорные устройства промышленного Интернета вещей необходимо:

– определить устройства, в отношении которых могут быть совершены попытки несанкционированного доступа;

– сформировать перечень возможных атак;

– оценить масштаб атаки, с учетом метрики способа получения доступа нарушителем, метрики сложности получения доступа нарушителем, метрики требуемых привилегий, метрики взаимодействия с пользователем;

– оценить ущерб, нарушения конфиденциальности, целостности и\или доступности информации;

– осуществить оценку риска.

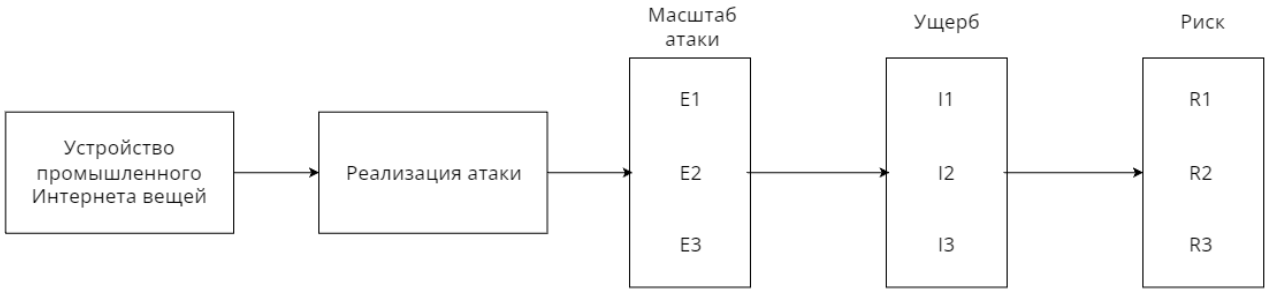

Рис. 1. Схема оценки риска реализации атаки

Масштаб атаки может оцениваться в соответствии с формулой (1):

$$E = k \times AV \times AC \times PR \times UI, \qquad (1)$$

где k – весовой коэффициент;

AV – метрика способа получения доступа нарушителем (attack vector);

AC – метрика сложности получения доступа нарушителем (attack complexity);

PR – метрика требуемых привилегий (privileges required);

UI – метрика взаимодействия с пользователем (user interaction).

Величина ущерба вычисляется в соответствии с формулой (2):

$$I = k \times [1 - \{(1 - C) \times (1 - I) \times (1 - A)\}], \qquad (2)$$

где k – весовой коэффициент;

C – метрика влияния на конфиденциальность (Confidentiality impact);

I – метрика влияния на целостность (Integrity impact);

A – метрика влияния на доступность (Availability impact).

Риск оценивается в соответствии с формулой (3):

$$R = E + I. \qquad (3)$$

Алгоритм оценки риска можно представить в следующем виде:

1. Формирование баз данных (таблиц) устройств подверженных атакам. В базе указывается какая информация циркулирует в устройстве.

2. Формирование таблицы возможных атак. В таблице указываются: атака, уровень на котором осуществляется атака, метрика способа получения доступа нарушителем, метрика сложности получения доступа, метрика требуемых привилегий, метрика конфиденциальности, метрика целостности, метрика доступности, устройства подверженные данной атаке.

3. Проведение оценки масштаба атаки на каждое устройство в сети, в соответствии с формулой (1).

4. Проведение оценки возможного ущерба от реализации атак на каждое из устройств подверженное ей, в соответствии с выражением (2).

5. Оценка риска реализации атак на каждое из устройств, в соответствии с формулой (3).

6. Принятие решения о приемлемости риска на основе полученных значений риска для каждого устройства.

Алгоритм оценки риска представлен на рис. 2.

Рис. 2. Алгоритм оценки риска

Алгоритм регулирование риска

Управление риском реализации атак, использующих уязвимости прикладного и сетевого уровней на сенсорные устройства промышленного Интернета вещей, будет осуществляться за счет регулирования значений метрик конфиденциальности, целостности и доступности, путем внедрения предложенных мер противодействия.

Алгоритм регулирования риска реализации атак можно формализовать в следующем виде:

1. Формирование необходимых баз данных, в соответствии с методикой, изложенной выше.

2. Формирование перечня мер противодействия выявленным атакам, с целью повышения защищенности устройств промышленного Интернета вещей.

3. Осуществление оценки масштаба каждой атаки на каждое устройство в сети, в соответствии с формулой (1).

4. Проведение оценки возможного ущерба от реализации каждой атаки на каждое из устройств, в соответствии с выражением (2).

5. Оценка риска реализации атак на каждое из устройств, в соответствии с формулой (3).

6. Проведение оценки возможного ущерба от реализации атаки, с внедрением

мер противодействия, на каждое из устройств.

7. Оценка риска реализации атак (с внедрением мер противодействия) на каждое из устройств.

8. Сравнение полученных оценок риска с использованием мер противодействия и без них.

9. Принятие решения о приемлемости полученных значений и выбор оптимальной меры противодействия.

Результаты проведенной оценки для различных атак с использованием различных контрмер сведены в табл 1.

Для наглядности полученные результаты представлены на рис. 3. Результаты представлены в нормированном виде. Нормирование проводилось методом минимаксной нормализации в соответствии с формулой (4):

$$X = \frac{x - x_{\min}}{x_{\max} - x_{\min}}, \quad (4)$$

где X – полученная нормированная величина;

x – нормируемая величина;

x_{min} – наименьшая величина;

x_{max} – наибольшая величина.

Таблица 1

Оценка риска и ущерба с применением мер противодействия

Атака	Мера противодействия	Ущерб	Риск
Прослушивание сети	Взаимная аутентификация	0.437	0.599
Спуфинг	Обновление протоколов	0.495	0.657
Анализ трафика сети	Сквозное шифрование	0.452	0.614
Атака «маскарад»	Многоканальная архитектура	0.553	0.715
Атака «человек посередине»	Шифрование WPA3	0.199	0.343
Отказ в обслуживании	Распределение данных	0.379	0.601
Атака «олицетворение»	Система аутентификации пользователей	0.125	0.269
Подделка/модификация/повторное воспроизведение	Структурированный план восстановления	0.487	0.649

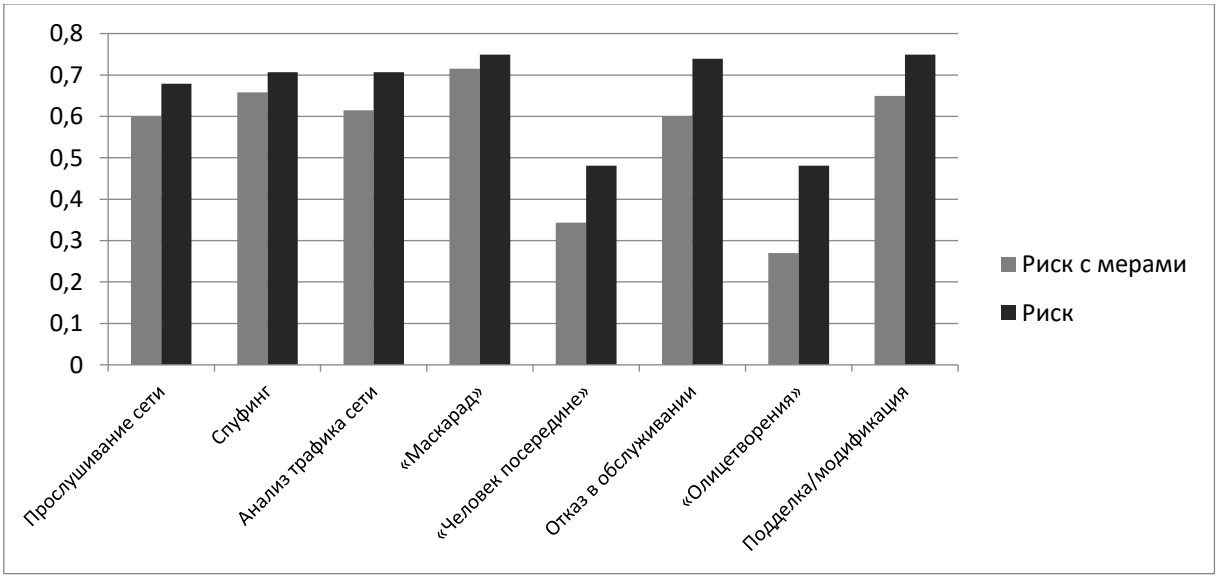

Рис. 3. Результаты оценки риска различных атак

Результаты оценки риска и ущерба с применением различных мер противодействия к атаке прослушивание сети сведены в табл. 2.

Для наглядности полученные результаты представлены на рис. 4 и рис. 5.

Таблица 2

Оценка риска и ущерба с применением различных мер противодействия к атаке прослушивание сети

Мера	Ущерб	Риск
Взаимная аутентификация	0.437	0.599
Обновление протоколов	0.454	0.616
Сквозное шифрование	0.399	0.561
Многоканальная архитектура	0.44	0.602
Шифрование WPA3	0.41	0.554
Без применения мер	0.517	0.679

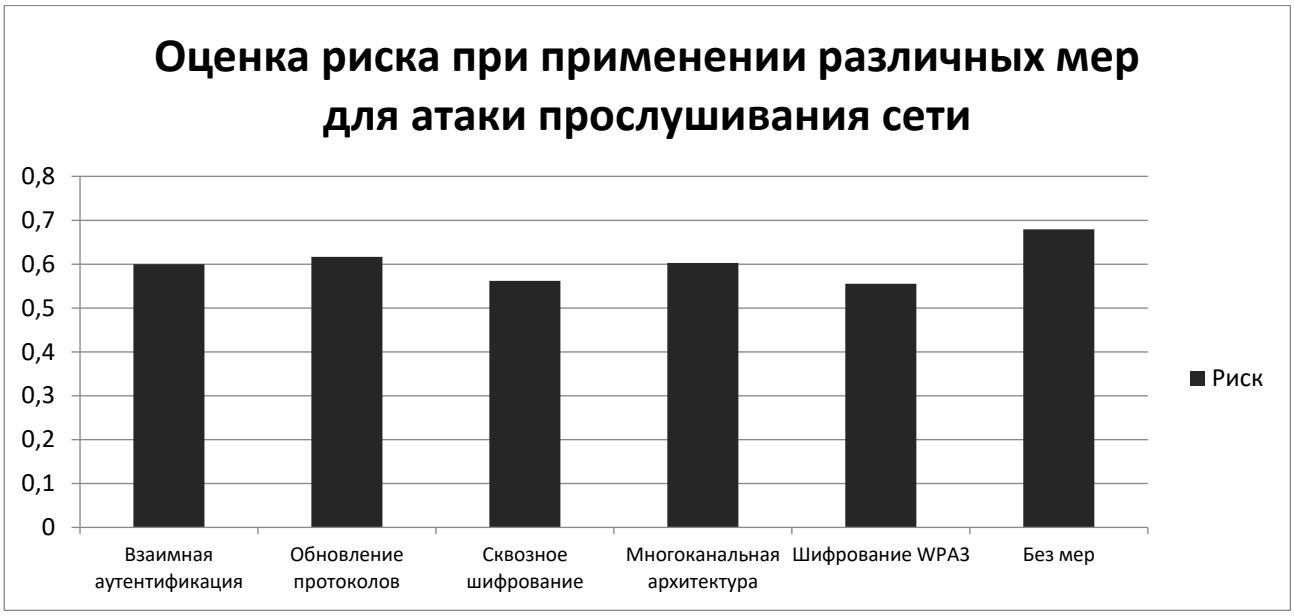

Рис. 4. Оценка риска при применении различных мер для атаки прослушивания сети

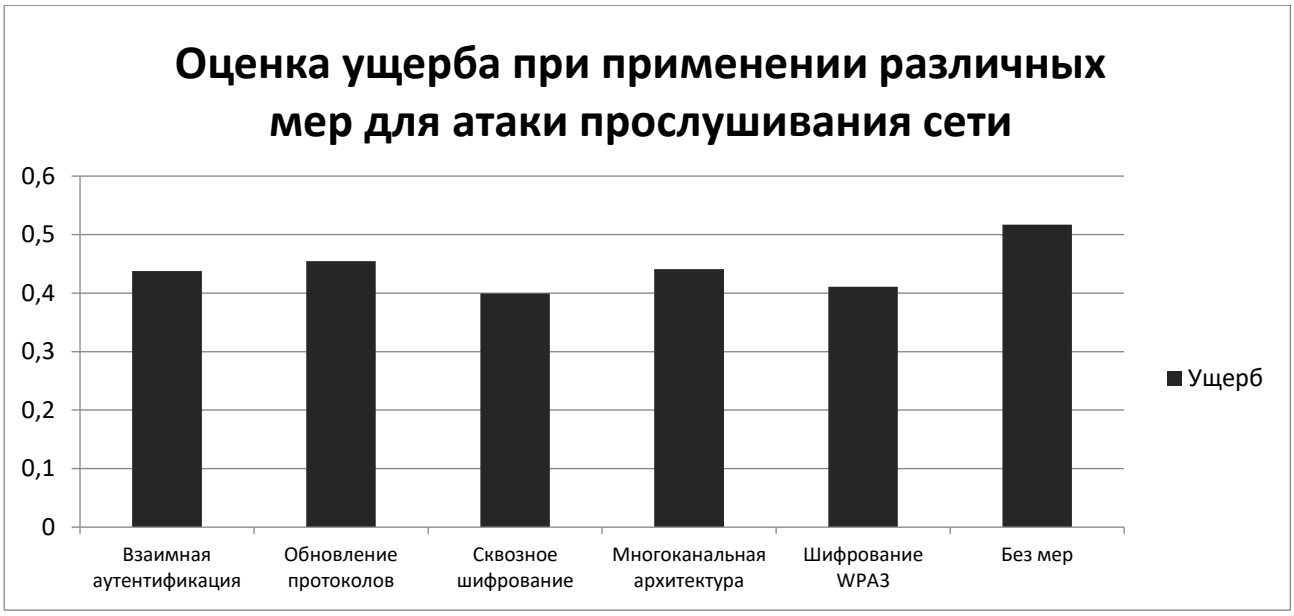

Рис. 5. Оценка ущерба при применении различных мер для атаки прослушивания сети

Заключение

Исходя из полученных результатов можно сделать вывод о том, какие методическое и алгоритмическое обеспечения позволят своевременно выявлять наиболее уязвимые устройства в сети промышленного Интернета вещей.

Предложенные методическое и алгоритмическое обеспечения оценки и регулирования риска реализации атак, использующих уязвимости прикладного и сетевого уровней, направленных на нарушение конфиденциальности целостности и доступности информации сенсорных устройств промышленного Интернета вещей, могут быть использованы для оценки состояния защищенности устройств в сети промышленного Интернета вещей.

Разработанные методическое и алгоритмическое обеспечения могут быть адаптированы для других сетей, таких как «Умный дом», медицинский Интернет вещей (IoMT).

Разработанный программный комплекс автоматизированной оценки и регулирования рисков реализации атак, использующих уязвимости прикладного и сетевого уровней, на сенсорные устройства промышленного Интернета вещей, может быть использован для оценки и регулирования рисков как в функционирующих сетях, так и на этапе проектирования новых.

Перспектива развития данного исследования видится в оценке влияния мер противодействия угрозам на эффективность работы устройств и сети Интернета вещей.

Список литературы

1. Atzori L. The internet of things: A survey / L. Atzori, A. Iera, G. Morabito // Computer networks. 2010. V. 54. No. 15. P. 2787-2805.

2. Taneja M. An analytics framework to detect compromised iot devices using mobility behavior / ICT Convergence (ICTC), 2013 International Conference on. IEEE. 2013. P. 38-43.

3. Jiang D. A study of information security for m2m of IoT / D. Jiang, C. ShiWe // Advanced Computer Theory and Engineering (ICACTE). 2010. 3rd International Conference on IEEE. 2010. V. 3. P. 573-576.

4. Kizza J. M. Guide to Computer Network Security. Springer, 2013.

5. Болгов А.А. Оценка риска безопасности в сетях интернета вещей / А.А. Болгов, С.А. Ермаков, Л.В. Паринова, Н.И. Баранников // Информация и безопасность. 2020. Т. 23. Вып. 4. С. 561-566.

6. Татарникова Т.М. Модель оценки временных характеристик при взаимодействии в сети интернета вещей / Т.М. Татарникова, М.А. Елизаров// Информационно-управляющие системы. – 2017. № 2.С. 44-50.

7. Ермаков С.А. Оценка и регулирование рисков сетей промышленного интернета вещей на разных этапах жизненного цикла систем в условиях отсутствия статистики ущерба / С.А. Ермаков, С.Ю. Громовиков, А.А. Болгов, Е.А. Москалева // Информация и безопасность. 2021. Т. 24. Вып. 1. С. 127-134.

Концерн «Созвездие»
Concern «Sozvezdie»

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 21.01.2023

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, начальник отдела, Концерн «Созвездие», e-mail: mnac@comch.ru

Серых Дмитрий Романович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Болгов Андрей Александрович – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Батаронов Игорь Леонидович – д-р физ.-мат. наук, заведующий кафедрой, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Кривошеин Александр Сергеевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

ASSESSMENT AND REGULATION OF THE RISKS OF ATTACKS USING VULNERABILITIES OF THE APPLIED AND NETWORK LEVEL ON SENSOR DEVICES OF THE INDUSTRIAL INTERNET OF THINGS

S.A. Ermakov, D.R. Seryh, A.A. Bolgov, I.L. Bataronov, A.S. Krivoshein

The article proposes a methodology for assessing and managing risks to increase the security of industrial Internet of Things sensor devices from attacks that use vulnerabilities in the application and network layers aimed at violating the confidentiality, integrity and availability of information. The technique allows to carry out a risk assessment taking into account the main technical characteristics of software, hardware and firmware vulnerabilities. The risk management process involves reassessing the risk of an attack on a particular device, taking into account the use of countermeasures. A software toolkit is presented for assessing and managing risks, which makes it possible to compare risk values when using various measures to counteract it. The obtained results in the form of a quantitative assessment make it possible to analyze the risks of implementing possible attacks on each of the network devices, identify the most vulnerable elements of the network, and select measures to reduce the risk level to the required value.

Keywords: Industrial Internet of Things, risk, attack, confidentiality, integrity, availability.

Submitted 21.01.2023

Information about the authors

Sergey A. Ermakov – Cand. Sc. (Technical), Concern "Sozvezdie", e-mail: mnac@comch.ru

Dmitry R. Seryh – student, Voronezh State Technical University, e-mail: mnac@comch.ru

Andrey A. Bolgov – graduate student, Voronezh State Technical University, e-mail: mnac@comch.ru

Igor L. Bataronov – Dr. Sc. (Phisical and Mathimatical), Head of Department, Voronezh State Technical University, e-mail: mnac@comch.ru

Alexander S. Krivoshein – student, Voronezh State Technical University, e-mail: mnac@comch.ru