УДК 004.089 + 004.056 Вестник УрФО № 4(30) / 2018, с. 43–49

Минаев В. А., Королев И. Д., Сабанов А. Г.

DOI: 10.14529/secur180407

ОЦЕНКА РИСКОВ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ СУБЪЕКТОВ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

В статье рассматриваются факторы снижения наблюдающегося сегодня резкого обострения информационного противоборства и ослабления информационной безопасности. В качестве основного фактора определяется эффективное управление доступом в информационные системы, включающее идентификацию и аутентификацию пользователей. Обращается внимание на снижение рисков и формирование доверия взаимодействующих субъектов и объектов доступа за счет научно обоснованных в нормативно-правовой базе и методических рекомендациях методах, механизмах и средствах идентификации и аутентификации. Показана необходимость создания многоуровневой методики аутентификации. Описываются её основные принципы, основанные на формировании концепции информационной безопасности, моделях угроз и нарушителя, применении организационных и технических мер защиты. Особое внимание при этом уделяется управлению рисками в облачных сервисах. Приводится наглядный графический пример оценки рисков.

Ключевые слова: *Оценка, риск, идентификация, аутентификация, электронное взаимодействие, информационная безопасность, управление рисками.*

Minaev V. A., Korolev I. D., Sabanov A. G.

RISK ASSESSMENT IDENTIFICATION AND AUTHENTICATION OF ELECTRONIC INTERACTION SUBJECTS

The article considers the factors of reducing the sharp aggravation of information confrontation and weakening of information security observed today. The main factor is the effective management of access to information systems, including the identification and authentication of users. Attention is drawn to the reduction of risks and the formation of subjects and objects interacting trust access due to the methods, mechanisms and means of identification and authentication scientifically grounded in the legal framework and methodological recommenda-

tions. The necessity of creating a multi-level authentication method is shown. Its basic principles based on the formation of the information security concept, threat and intruder models, application of organizational and technical protection measures are described. Particular attention is paid to risk management in cloud services. An illustrative graphical example of a risk assessment is considered.

Keywords: *Assessment, risk, identification, authentication, electronic interaction, information security, risk management.*

Введение

В условиях резкого обострения информационного противоборства (ИП) в государственной, социально-экономической и гражданской сферах, непрерывного роста кибератак на информационные системы (ИС) различного назначения, практически любая среда информационного обмена априори может быть рассмотрена в качестве потенциально подверженной возможным нападениям. Значительное влияние на снижение факторов такого обострения имеет эффективное управление доступом пользователей в ИС, в качестве основных этапов включающее идентификацию (ИД) и аутентификацию (АУ) субъектов и объектов доступа.

Процессы аутентификации особенно востребованы в случае недоверия к подлинности предъявленных идентификаторов взаимодействующих сторон, например, при удалённом доступе и/или использовании недоверенной среды информационного обмена.

Существуют и риски того, что в среде современных многозадачных информационных систем вычислительный процесс, реализующийся в интересах злоумышленника, может имитировать функционирование легальных субъектов и объектов доступа, как параллельно с ними, так и автономно.

Для снижения указанных рисков и формирования определённого уровня доверия в подлинности взаимодействующих сторон (субъектов и объектов доступа) необходимо применять научно обоснованные, закреплённые в нормативно-правовой базе и методических рекомендациях методы, механизмы и средства ИД и АУ в составе систем управления доступом к ИС.

Еще одна актуальная задача связана с быстро увеличивающимся числом зарегистрированных субъектов доступа, насчитывающих сотни тысяч, а нередко – десятки миллионов пользователей. Это вызывает необходимость научного поиска достаточного числа надежных идентификаторов для достижения заданного уровня достоверности ИД и разработки шкалы доверия к результатам АУ для ИС. Многообразие реализаций схем информационного обмена, методов АУ в отсутствии чётких требований нормативной базы также нуждается во введении определённых уровней доверия к результатам аутентификации сторон электронного взаимодействия.

Значительный вклад в решение проблем идентификации и аутентификации содержится в работах [1-5], в которых разработаны концептуальные основы защиты информации (ЗИ), обоснованы принципы обеспечения информационной безопасности (ИБ) и построения систем защиты информации (СЗИ), рассмотрены теоретические аспекты и методология организации ЗИ, развита теория функциональной надежности (ФН), основы теории функциональной устойчивости, а также сформулированы направления построения моделей угроз и нарушителей безопасности информации.

Методические подходы к оценке рисков идентификации и аутентификации

Сравнительный анализ международных и российских стандартов, зарубежной и отечественной нормативной базы по вопросам регулирования процессов аутентификации, научных исследований по вопросам анализа рисков, надежности и безопасности применительно к процессам АУ показал, что за рубежом нормативная и научно-методическая база по вопросам их регулирования существенно опережает отечественную. Терминология в данной области также нуждается в существенном совершенствовании. Так, из 66 международных стандартов по идентификации и аутентификации в нашей стране имеется только один аналог – стандарт 1998 года (ГОСТ 9594-8 [6]).

Таким образом, вопросы идентификации и аутентификации и особенно разработки их математических моделей нуждаются в расширении исследований, системном изложении функций основных участников, процессов, а также способов построения систем ИД и АУ с учетом требований функциональной

надёжности и безопасности передаваемой и обрабатываемой в них информации. Также нуждаются в развитии требования ИБ к проектированию и построению систем удалённой аутентификации, к безопасности и надёжности выполнения идентификации и аутентификации в корпоративных (закрытых) ИС и современных ИС общего пользования, особенно при переходе к облачным вычислениям.

Исследования [7, 8] показали, что анализ рисков аутентификации в конкретно взятой ИС может проводиться в соответствии с традиционным подходом, основанном на оценке вероятности реализации угроз и величины ущерба (тяжести последствий от их реализации). Однако при этом можно получить лишь грубые оценки, а для более глубокого и точного анализа существует необходимость разработки многоуровневой методики оценки рисков, учитывающей специфику последовательно организованных процессов, составляющих процедуру аутентификации.

чительными. На рис. 1 представлена схема оценки рисков, учитывающая специфику процессов ИД и АУ.

При разработке требований к аутентификации в качестве основного метода анализа взята оценка рисков. За основу критериев оценки выбрано обеспечение трех взаимосвязанных компонент – конфиденциальности, доступности и целостности персональной информации при организации доступа с применением аутентификации.

Основными задачами являлись описание рассматриваемой системы, выработка целей и критериев идентификации и анализа рисков.

Затем был выбран перечень известных методов исследования рисков для рассматриваемой системы. Учитывая, что аутентификация является сложным процессом, в который включены персонал, аппаратное и программное обеспечение нескольких систем, сначала оценены высокоуровневые риски с помощью качественных методов.

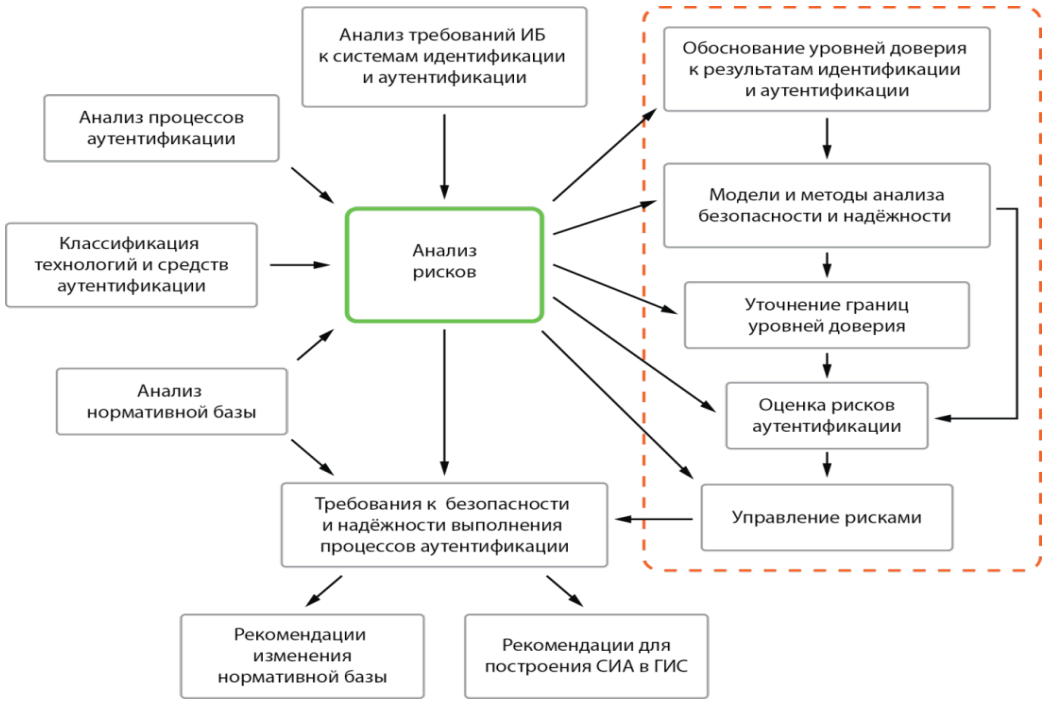

Рис. 1. Блок-схема методики оценки рисков ИД и АУ

Методика связана с исследованием рисков на различных уровнях детализации: сначала рассматриваются риски всей системы ИД и АУ, затем отдельные процедуры, составляющие процесс АУ, следующими уровнями детализации являются отдельные её элементы, для которых значения рисков и тяжести последствий их реализации могут быть зна-

Потом для проведения детализированного анализа рисков применительно к развитым ИС при наличии ценных информационных активов применены количественные оценки рисков. Кроме того, при необходимости осуществлялся дополнительный анализ процесса аутентификации с помощью построения дерева событий, дерева неисправностей и вида отка-

зов. Далее выявленные уязвимости соотнесены с соответствующими угрозами и имеющимися статистическими данными по инцидентам и механизмам контроля для оценки потенциального ущерба от реализации рисков.

Пример расчета рисков удаленной аутентификации

Результаты предложенной методики проиллюстрированы на конкретном примере, представленном в таблице 1. При этом учитывалось, что процедуры первого блока процесса (с 1.1 по 1.6 в таблице 1) являются разовыми, а процедуры 2.1 – 4.1 – многократными. Уязвимости с высокой вероятностью реализации (p = 0,9 ÷ 1) обозначены буквой В, со средней вероятностью (p ≈ 0,5) – буквой С, с низкой вероятностью (p ≤ 0,1) – буквой Н. Аналогично для оценки наиболее вероятных угроз принято обозначение В, для средней вероятности реализации угроз – С, для низкой – Н.

Выявлено, что наиболее уязвимыми являются процедуры проверки идентификаторов, предъявленных центру регистрации (ЦР), процедуры хранения и предъявления аутентификатора.

$$R = \sum_{i=1}^{M} R_i = \sum_{i=1}^{M} p(U_i) \cdot L(U_i), \quad (1)$$

где U_i – i-ое опасное событие; $p(U_i)$ – вероятность наступления i-го опасного события; $L(U_i)$ – ущерб от наступления i-го опасного события; M – количество опасных событий.

Проранжируем вероятные опасные события (ВОС), используя значение вероятности появления опасного события в год – p_i и относительного значения риска R_i (таблица 2). Условием нормировки является

$$\overline{R} = \frac{\sum_{i=1}^{M} R_i}{\sum_{i=1}^{M} L(U_i)} = 1 \quad (2)$$

Результаты ранжирования представлены на рисунке 2 в виде пронумерованных кружков, обозначающих номер события в таблице 2 в плоскости переменных $\{R_i,\ lgp_i\}$.

Из анализа рисунка 2 следует, что, например, для снижения ВОС 2 (фишинг – подмена сайта, на который пользователю необходимо предоставить доступ) достаточно перейти с парольной аутентификации на технологию защищенного доступа с использованием TLS (Transport Secure Socket Layer) с двусторонней взаимной аутентификацией на основе применения цифровых

Таблица 1

Оценки уязвимостей и угроз процедур удаленной аутентификации

Блоки	Процесс	Уязвимости	Угрозы
1	**Регистрация**	С	С
1.1	Субъект ***предъявляет*** свои идентификаторы	Н	С
1.2	ЦР ***проверяет*** предъявленные субъектом идентификаторы	С	В
1.3	ЦР ***создает*** учетную запись субъекта	Н	Н
1.4	ЦР ***регистрирует/создает*** секрет (аутентификатор) и ***издает*** ЭУ	Н	С
1.5	ЦР ***делегирует*** права доступа субъекта к другим ИС	Н	Н
1.6	ЦР ***выдает*** секрет и ЭУ на руки субъекту	Н	Н
2	**Подтверждение подлинности**	С	С
2.1	Субъект ***хранит*** секрет и ЭУ	С	В
2.2	Субъект ***предъявляет*** секрет и ЭУ доверяющей стороне (ДС)	С	С
3	**Валидация**	Н	Н
3.1	ДС ***проверяет*** цепочку сертификатов, срок и область действия ЭУ	Н	С
4	**Принятие решения**	Н	Н
4.1	ДС ***принимает решение*** о результате аутентификации	Н	Н

Предложенный подход использован авторами для оценки риска в системах управления доступом в различных ИС, начиная от локальных корпоративных систем и завершая доступом к сервисам публичного облака.

Интегральная оценка рисков проведена на основе экспертного метода, используя соотношение:

SSL-сертификатов на стороне сервера и клиента.

Это приведет к снижению вероятности подмены сайта приблизительно на два порядка (с 10^{-4} до 10^{-6}). Еще примерно на два порядка можно снизить вероятность фишинговой атаки за счет применения технологии хранения закрытого ключа и клиентского

Таблица 2

Пример ранжирования рисков аутентификации

ВОС	Описание опасного события	p_i	R_i
1	Воздействие вредоносного ПО	10^{-3}	0,122
2	Фишинг	10^{-4}	0,141
3	Риск добровольной передачи носителя (ключа и АУ)	10^{-4}	0,110
4	Ошибки или целенаправленные действия при смене АУ	10^{-4}	0,096
5	Использование уязвимостей системы АУ	10^{-4}	0,088
6	Ошибки валидации	10^{-5}	0,120
7	Spoofing (подмена) доверенной стороны	10^{-5}	0,089
8	Помощь инсайдера	10^{-5}	0,084
9	Регистрация злоумышленника под видом легального пользователя	10^{-6}	0,137

сертификата в устройстве класса SSCD (Secure Signature Creation Design – устройство генерации ключей электронной подписи). Итоговое снижение ВОС в год за счет указанных мер может снизиться до 10^{-6} и даже ниже.

информационной безопасности, моделях угроз и нарушителя, применении организационных и технических мер защиты. При этом риски будут снижаться в вертикальном направлении до определенного уровня.

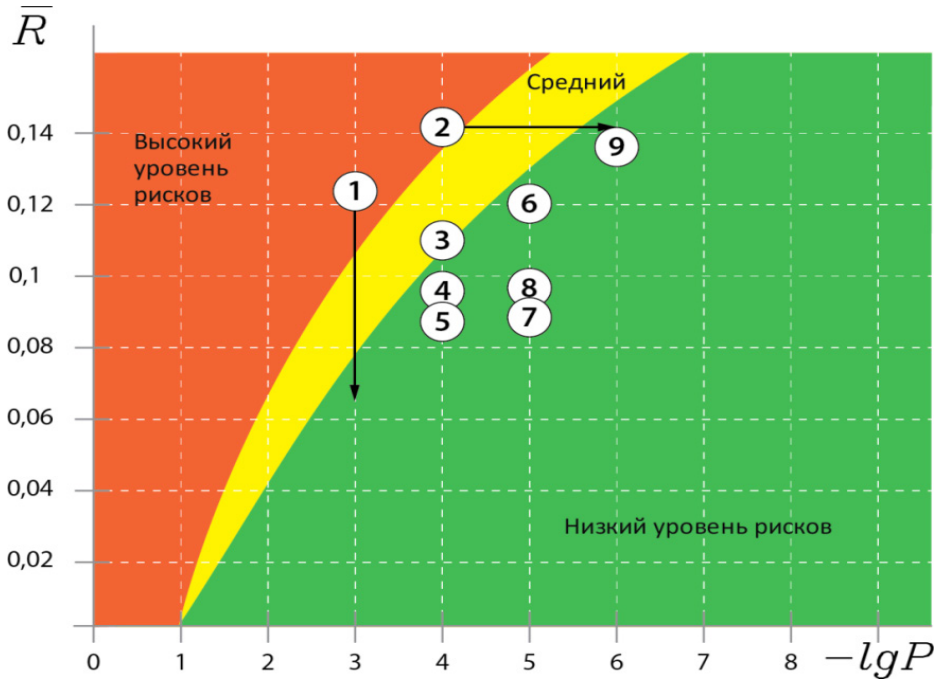

Рис. 2. Поле управления рисками для системы ИД и АУ

В то же время снижение рисков в рассмотренных примерах может проводиться в отношении не только частоты реализации ВОС, но и размера риска, используя в качестве механизмов снижения рисков традиционные способы обеспечения доступности, целостности и конфиденциальности информации, основанные на формировании концепции

Соответствующими способами можно снизить риски за счет внедрения СЗИ (ВОС 1 – установка антивирусного программного обеспечения; ВОС 3 – переход на смарт-карты с технологией Match-on-Card; ВОС 8 – внедрение СЗИ в систему АУ).

При достижении приемлемых уровней рисков по частоте (в горизонтальном направ-

лении) и размеру (в вертикальном направлении) процесс управления рисками можно считать выполненным.

Если приемлемых уровней для остаточных рисков достичь не удается, необходимо подключать такие механизмы управления рисками, как уклонение от риска (ликвидация причин и/или последствий риска), ограничение (нейтрализация) риска (например, путем реализации контрмер, уменьшающих воздействие угроз безопасности), перенос риска на стороннюю организацию (страхование рисков).

К достоинствам данного метода анализа рисков аутентификации можно отнести его наглядность. Недостатком же его является необходимость в большом объеме предварительной работы по выявлению ВОС, зачастую в условиях отсутствия фактического материала в виде статистических данных или результатов мониторинга за достаточно продолжительный период времени. В таких случаях, согласно ГОСТ Р ИСО/МЭК 13335-1-2006, рекомендуется воспользоваться методом экспертных оценок.

Выводы

1. В условиях резкого обострения информационного противоборства и ослабления информационной безопасности вследствие роста кибератак различного характера, значительное влияние на снижение факторов такого обострения имеет эффективное управление доступом в информационные системы, в качестве основных этапов включающее идентификацию и аутентификацию пользователей.

2. Для снижения рисков и формирования определённого уровня доверия в подлинности взаимодействующих сторон (субъектов и объектов доступа) необходимо применять научно обоснованные, закреплённые в нормативно-правовой базе и методических рекомендациях методы, механизмы и средства ИД и АУ в составе систем управления доступом к ИС.

3. Для глубокого и точного анализа рисков аутентификации необходима разработка многоуровневой методики их оценки, учитывающей специфику последовательно организованных процессов, составляющих процедуру аутентификации. За основу критериев оценки следует выбирать обеспечение трех взаимосвязанных компонент – конфиденциальности, доступности и целостности информации при организации доступа с применением аутентификации.

4. Снижение рисков должно проводиться не только в отношении частоты реализации опасных событий, но и размера риска, используя в качестве механизмов снижения рисков традиционные способы, основанные на формировании концепции информационной безопасности, моделях угроз и нарушителя, применении организационных и технических мер защиты [9]. Особое внимание при этом должно уделяться управлению рисками в облачных сервисах [10].

Литература

1. Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие. / Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. М.: Горячая линия-Телеком, 2012. – 552 С.

2. Баушев С. В., Аристархов И. В., Кузьмин А. С., Сабанов А. Г. и др. Удостоверяющие автоматизированные информационные системы и средства. Введение в теорию и практику. СПб.: "БХВ-Петербург", 2016. – 304 С.

3. Сабанов А.Г. Основные процессы аутентификации // Вопросы защиты информации. 2012. №3. – С. 54-57.

4. Сабанов А.Г. Об оценке рисков удаленной аутентификации // Электросвязь. 2013. №4. – С. 27-32.

5. Смит Р. Э. Аутентификация: от паролей до открытых ключей. М.: «Вильямс», 2002. – 432 С.

6. "Информационная технология. Взаимосвязь открытых систем. Основы аутентификации". Справочник. Часть 8. Государственный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 9594-8-98.

7. Сабанов А.Г. Аутентификация как часть единого пространства доверия // Электросвязь. 2012. №8. С. 40-44.

8. Сабанов А.Г. Об оценке рисков удаленной аутентификации // Электросвязь. 2013. №4. – С. 27-32.

9. Фисун А.П., Касилов А.Г., Фисенко В. Е., Минаев В.А., Афанасьев В.В., Митяев В.В., Фисун Р. А., Джевага К.А., Кожухов С. А. Развитие методологических основ информатики и информационной безопасности систем. Депонированная рукопись. Орловский государственный университет. Номер 1165-В2004. ВИНИТИ. Дата депонирования 07.07.2004. – 253 С.

10. Сабанов А.Г. Особенности аутентификации при доступе к облачным сервисам // Вестник Нижегородского университета им. Н.И. Лобачевского. 2013. №2-1. – С. 45-51.

References

1. Afanas'ev A. A., Veden'ev L. T., Voroncov A. A. i dr. Autentifikaciya. Teoriya i praktika obespecheniya bezopasnogo dostupa k informacionnym resursam. Uchebnoe posobie. / Pod red. A. A. SHelupanova, S. L. Gruzdeva, YU. S. Nahaeva. M.: Goryachaya liniya-Telekom, 2012. – 552 S.

2. Baushev S.V., Aristarhov I.V., Kuz'min A. S., Sabanov A. G. i dr. Udostoveryayushchie avtomatizirovannye informacionnye sistemy i sredstva. Vvedenie v teoriyu i praktiku. SPb.: "BHV-Peterburg", 2016. – 304 S.

3. Sabanov A.G. Osnovnye processy autentifikacii // Voprosy zashchity informacii. 2012. №3. – S. 54-57.

4. Sabanov A.G. Ob ocenke riskov udalennoj autentifikacii // EHlektrosvyaz'. 2013. №4. – S. 27-32.

5. Smit R. EH. Autentifikaciya: ot parolej do otkrytyh klyuchej. M.: «Vil'yams», 2002. – 432 S.

6. "Informacionnaya tekhnologiya. Vzaimosvyaz' otkrytyh sistem. Osnovy autentifikacii". Spravochnik. CHast' 8. Gosudarstvennyj standart Rossijskoj Federacii GOST R ISO/MEHK 9594-8-98.

7. Sabanov A.G. Autentifikaciya kak chast' edinogo prostranstva doveriya // EHlektrosvyaz'. 2012. №8. S. 40-44.

8. Sabanov A.G. Ob ocenke riskov udalennoj autentifikacii // EHlektrosvyaz'. 2013. №4. – C. 27-32.

9. Fisun A.P., Kasilov A.G., Fisenko V. E., Minaev V.A., Afanas'ev V.V., Mityaev V.V., Fisun R. A., Dzhevaga K.A., Kozhuhov S. A. Razvitie metodologicheskih osnov informatiki i informacionnoj bezopasnosti sistem. Deponirovannaya rukopis'. Orlovskij gosudarstvennyj universitet. Nomer 1165-B2004. VINITI. Data deponirovaniya 07.07.2004. – 253 S.

10. Sabanov A.G. Osobennosti autentifikacii pri dostupe k oblachnym servisam // Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo. 2013. №2-1. – S. 45-51.

МИНАЕВ Владимир Александрович, доктор технических наук, профессор, профессор Московского государственного технического университета им. Н.Э. Баумана. Россия, 105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1. E-mail: m1va@yandex.ru

КОРОЛЕВ Игорь Дмитриевич, доктор технических наук, профессор, профессор Краснодарского высшего военного училища имени генерала армии С. М. Штеменко. Россия, 350063, г. Краснодар, ул. Красина, 4. E-mail: pi_korolev@mail.ru

САБАНОВ Алексей Геннадьевич, кандидат технических наук, доцент, доцент Московского государственного технического университета им. Н.Э. Баумана. Россия, 105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1. E-mail: aladdin@aladdin-rd.ru

MINAEV Vladimir, Doctor of Technical Sciences, Professor, Professor of Moscow State Technical University. N.E. Bauman. Russia, 105005, Moscow, 2 nd Baumanskaya Str., 5, bld. 1. E-mail: m1va@yandex.ru

KOROLEV Igor, Doctor of Technical Sciences, Professor, Professor of the Krasnodar Higher Military School named after Army General S. M. Shtemenko. Russia, 350063, Krasnodar, ul. Krasin, 4. E-mail: pi_korolev@mail.ru

SABANOV Alexey, Candidate of Technical Sciences, Associate Professor, Associate Professor of Moscow State Technical University. N.E. Bauman. Russia, 105005, Moscow, 2 nd Baumanskaya Str., 5, bld. 1. E-mail: aladdin@aladdin-rd.ru