Транспорт

УДК 004.056.53
DOI: 10.30987/1999-8775-2021-9-36-42

Н.М. Кузнецова, Т.В. Карлова, А.Ю. Бекмешов

ПОСТРОЕНИЕ МОДУЛЬНОЙ СТРУКТУРЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СТРАТЕГИЧЕСКИ ВАЖНЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ ТРАНСПОРТА

Построена модульная структура автоматизированной системы комплексного обеспечения защиты ресурсов предприятия (АСКОЗРП), в частности – предприятия транспортного комплекса. Решена задача распределения основных функций защиты ресурсов предприятия между модулями единой автоматизированной системы. Предложены рекомендации к распределению функций защиты между модулями АСКОЗРП и их взаимодействию, исследованы основные трудности реализации функций. Новизной работы является предложенная модульная структура автоматизированной системы комплексной защиты, а также механизм изоляции «пораженных» ресурсов основных автоматизированных систем предприятия.

Ключевые слова: автоматизация, информационная безопасность, защита информации, ресурсы.

N. M. Kuznetsova, T. V. Karlova, A. Y. Bekmeshov

CONSTRUCTION OF A MODULAR STRUCTURE OF AN AUTOMATED SYSTEM FOR INTEGRATING SUPPORT FOR THE PROTECTION OF STRATEGICALLY IMPORTANT RESOURCES OF A TRANSPORT ENTERPRISE

The purpose of the scientific work is to build a scheme for the interaction of modules of an automated system for integrated protection of strategically important resources of an enterprise, in particular, a transportation industry enterprise. To ensure a high efficiency of the presented system, efficient allocation between the modules is necessary for the protection functions. Within the framework of this task, the article presents sets of functions for each security module.

The outstanding feature of the work is the proposed scheme of optimal interaction of the modules of the automated system of integrated protection of strategically important resources of the enterprise.

The article considers the mechanism of isolation of "affected" resources (and modules) of the main automated control systems of a transportation enterprise, consisting of the sequential execution of the functions of forming "affected zones and quarantine", the function of redirecting datastream. The paper presents a structural diagram of the interaction of modules of an automated system for integrated protection of strategically important enterprise resources, sets of functions for each module are formed, a scheme for ensuring isolation of "affected" resources is presented, the main difficulties of implementing an automated system are described, in particular, the features of its implementation at the transportation industry enterprise connected with the client-server architecture of the main AS, a number of additional organizational and technical measures for protecting strategically important enterprise resources are proposed.

Key words: automation, information security, information protection, resources.

Введение

Большинство современных промышленных предприятий используют автоматизированные системы защиты ресурсов. Наиболее важными ресурсами при этом являются информационные, программные и аппаратные. Однако в связи со сложностью связей между ресурсами предприятия, а также с увеличением интеллектуального потенциала злоумышленников (увеличение частоты реализации наиболее сложных целенаправленных атак – *Advanced Persistent Attack – APT* [1, 2]), необходимо построение такой автоматизированной системы защиты, которая обеспечивала бы максимальный уровень информационной безопасности за счёт примене-

ния комплексного подхода [3, 4]. Применение таких автоматизированных систем комплексного обеспечения защиты ресурсов предприятия особенно актуально на предприятиях, относящихся к стратегически важным объектам, а также к объектам критической информационной инфраструктуры (КИИ) [5, 6].

Модульный состав автоматизированной системы комплексного обеспечения защиты ресурсов предприятия транспорта

Для повышения уровня информационной безопасности стратегически важных ресурсов предприятия АСКОЗРП должна включать максимально возможное количество рационально взаимодействующих функций защиты, распределенных между модулями.

Согласно рис. 1, в состав основных модулей АСКОЗРП должны входить:

– модуль аутентификации (МА);

–

– модуль интеллектуального детектирования угроз безопасности (МИДУБ);

– модуль мониторинга (ММ);

– модуль оповещения (МО);

– модуль временной изоляции «пораженных» ресурсов (МВИПР) (информационных, программных, аппаратных и т.д.);

– модуль управления и визуализации (МУиВ).

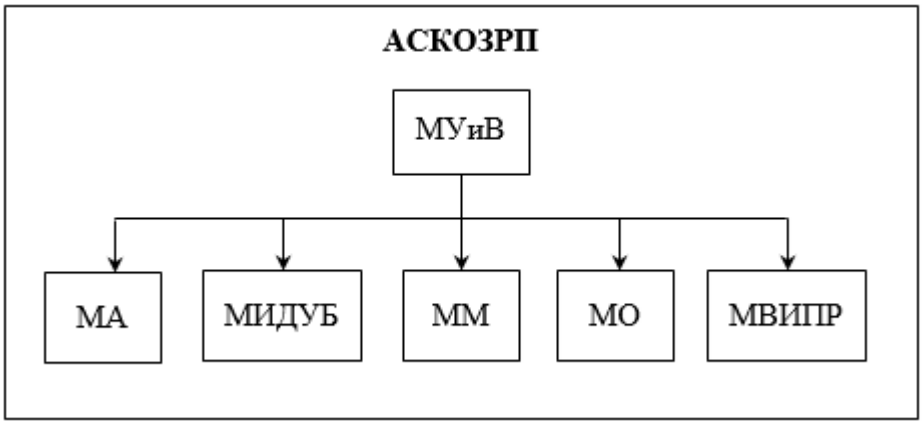

Рис. 1. Структурная схема взаимодействия модулей АСКОЗРП

Основными функциями МА являются идентификация и аутентификация сотрудников предприятия.

Основными функциями МИДУБ являются:

– применение комплекса технических мер противодействия социальной инженерии;

– анализ основных внутренних информационных потоков (ИП) в локальной вычислительной сети (ЛВС) предприятия;

– применение методов детектирования утечек информации (аналог систем класса *Data Leak Prevention – DLP*).

Применение систем класса *DLP* особенно актуально на «точках входа» в ЛВС предприятия. К основным «точкам входа» относятся:

– диски;

– флэш-накопители *USB*, брелоки;

– порты выхода в сеть Интернет;

– принтеры;

– факсы и т.д.

Основными функциями ММ являются: отслеживание параметров технических средств основных автоматизированных систем (АС) предприятия (аналог систем класса *Supervisory Control And Data Acquisition – SCADA*).

Примерами таких параметров являются: скорость передачи данных; состояние оборудования; температура воздуха помещения; температура элементов конструкций; давление; влажность воздуха; зашумленность и т.д.

– превентивная функция «предсказания» критических состояний основных АС предприятия при анализе параметров мониторинга – выход значений нескольких параметров за границы допустимых значе-

ний может свидетельствовать о системном сбое;

– аудит действий сотрудников (данная функция связана функцией анализа основных внутренних информационных потоков МИДУБ). Важно отметить, что анализ данных, собранных во время аудита действий сотрудников позволит проводить расследования, в том числе по выявлению реализации методов социальной инженерии.

Часто именно методы социальной инженерии используются как часть подготовки атаки класса *APT* [7 – 9].

Основными функциями МО являются:

– оповещение сотрудников службы безопасности о инцидентах информационной безопасности (ИИБ);

– оповещение лиц, принимающих решения (ЛПР) – руководство предприятия, руководителей подразделений, в которых произошел ИИБ.

Основными функциями МВИПР являются:

– формирование границ «зоны поражения» – определение «пораженных» модулей и ресурсов основных АС предприятия (связана с функцией анализа основных внутренних ИП МИДУБ);

– формирование границ «зоны карантина» – модулей основных АС предприятия, взаимодействующих с ресурсами и модулями из «зоны поражения». Важно отметить, что модули основных АС предприятия также относятся к стратегически важным аппаратно-программным ресурсам предприятия;

– перенаправление ИП (связана с функцией анализа основных внутренних ИП МИДУБ).

Важно отметить, что перечисленные функции МВИПР должны выполняться последовательно. Главной задачей является изоляция «пораженных» ресурсов основных АС предприятия. При этом необходимо перенаправить основные ИП таким образом, чтобы максимально сохранить эффективность работы основных АС предприятия.

На рис. 2 представлена схема работы МВИПР – схема обеспечения изоляции «пораженных» ресурсов основных АС предприятия.

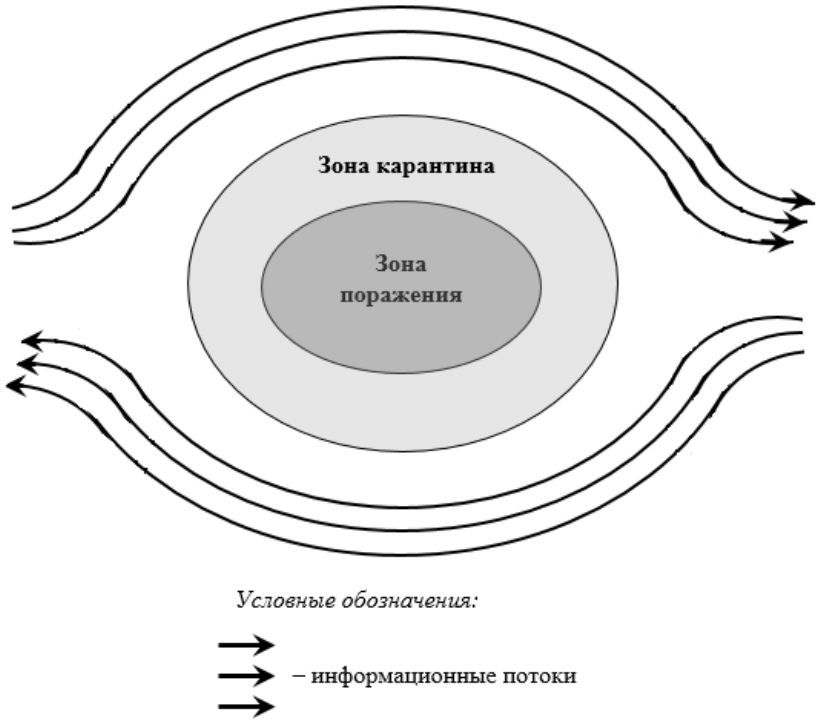

Рис. 2. Схема обеспечения изоляции «пораженных» ресурсов основных АС предприятия

Основными задачами МУиВ являются:

– обеспечение координации работы МА, МИДУБ, ММ, МО, МВИПР;

– визуализация работы модулей (в виде схем, графиков и т.д.).

Основные трудности внедрения автоматизированной системы комплексного обеспечения защиты ресурсов предприятия транспорта

К основным трудностям внедрения АСКОЗРП относятся:

– ограничения вычислительных ресурсов предприятия при реализации АСКОЗРП;

– ограничения экономических ресурсов предприятия;

– человеческий фактор;

– трудности обеспечения модернизации АСКОЗРП;

– трудности обеспечения физической изоляции ресурсов АСКОЗРП;

– влияние АСКОЗРП на эффективность работы основных АС предприятия. АСКОЗРП является «надстройкой» к основным АС предприятия, влияющей на работу АС (замедление основных ИП во время мониторинга и фильтрации, трата времени на принятие решения о доступе и т.д.).

При внедрении АСКОЗРП на предприятии транспортного комплекса необходимо учитывать, что основные АС имеют клиент-серверную архитектуру. При этом клиентская часть может быть территориально удалена. В связи с этим, особое внимание следует уделять:

– обеспечению безопасности пассивного оборудования ЛВС (каналов передачи данных между серверной частью АС и клиентами);

– обеспечение контроля со стороны АСКОЗРП всех взаимодействий клиентов с сервером: проведение процессов аутентификации клиентов (МА), мониторинга запросов (ММ), фильтрации информационного трафика (МИДУБ);

– физическое «экранирование» особо важных стратегических ресурсов на серверной стороне от модулей коммуникации с клиентской частью АС (минимизация обращений клиентской части основных АС к стратегически важным ресурсам).

На рис. 3 представлена схема взаимодействия АСКОЗРП с клиентской и серверной частями основных АС предприятия.

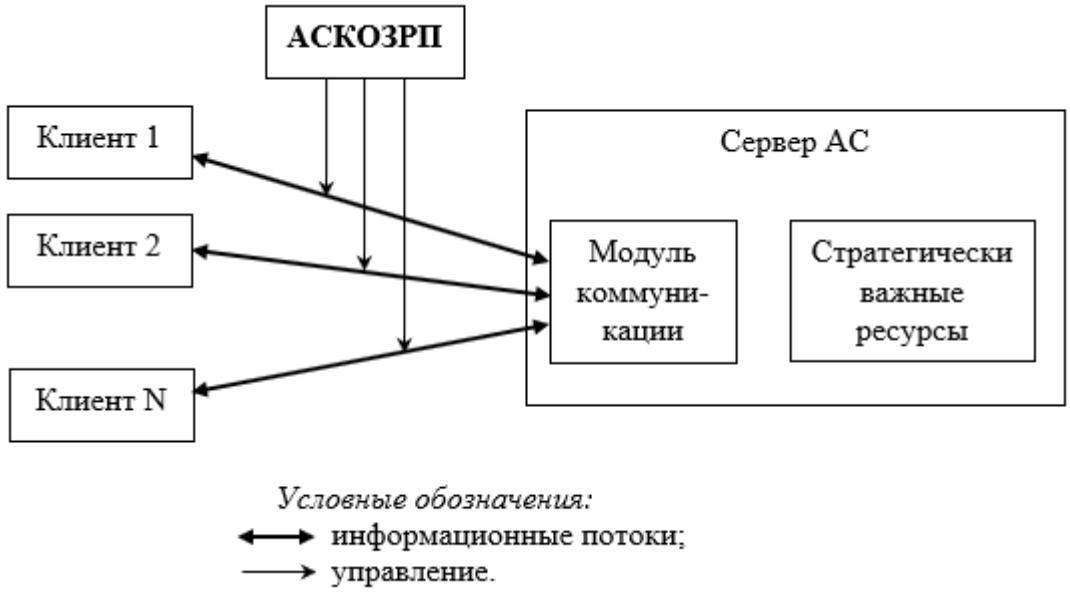

Рис. 3. Схема взаимодействия АСКОЗРП с клиентской и серверной частями основных АС предприятия

Применение дополнительных мер защиты стратегически важных ресурсов предприятия транспортного комплекса

Важно отметить, что помимо внедрения АСКОЗРП для защиты стратегически важных ресурсов предприятия в рамках комплексного подхода обеспечения безопасности необходимо применение дополнительных мер:

– внедрение системы обучения сотрудников: организация регулярных повышений квалификаций в области информационной безопасности; проведение тестирований, аттестаций сотрудников в области защиты информации; проведение «скрытых» тестов сотрудников (о возможности проведения подобных тестов сотрудники должны быть оповещены при устройстве на предприятие); применение методических мер противодействия социальной инженерии (своевременное оповещение сотрудников о новых методах социальной инженерии); применение технических средств противодействия побочным электромагнитным излучениям и наводкам (ПЭМИН) [10]: экранирование аппаратных ресурсов предприятия; применение механизмов зашумления (специальных устройств-генераторов шума);

– физическая изоляция максимального количества стратегически важных ресурсов предприятия;

– разработка алгоритма восстановления «зоны поражения» и «зоны карантина».

В рамках комплексного подхода важным аспектом построения АСКОЗРП является принцип связанности модулей. Таким образом, при применении злоумышленниками сложной целенаправленной атаки (*APT*), заключающейся в одновременной реализации нескольких угроз, АСКОЗРП обеспечит более высокий уровень информационной безопасности, чем совокупность несвязанных методов защиты. Кроме того, анализ данных, «собранных» модулями АСКОЗРП, позволит проводить расследования инцидентов и выявить новые стратегии атак.

Выводы

Эффективность автоматизированной системы защиты, состоящей из нескольких модулей, определяется эффективностью защиты наиболее «слабого звена», в связи с чем все перечисленные модули представленной АСКОЗРП должны функционировать максимально скоординировано. В разработанной схеме взаимодействия основных модулей АСКОЗРП субъектом управления и координации является МУиВ.

АСКОЗРП является программно-аппаратным комплексом обеспечения защиты, включающим набор функций, реализующих основные процессы защиты: обнаружение «врага» (функции МА, МИДУБ, ММ), препятствие дальнейшему распространению «врага» (функции МИДУБ, МВИПР), оповещение (функции МО), уничтожение «врага» (функции МВИПР).

При внедрении АСКОЗРП на транспортном предприятии необходимо учитывать особенности клиент-серверной архитектуры основных АС предприятия, а также территориальное распределение узлов ЛВС.

СПИСОК ЛИТЕРАТУРЫ

1. **Virvilis, N**. Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game? / N. Virvilis, D. Gritzalis, T. Apostolopoulos // 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing., – 2013. – P. 396-403. – DOI: 10.1109/UIC-ATC.2013.80.
2. **Chen, P.** A Study on Advanced Persistent Threats / P. Chen, L. Desmet, C. Huygens // Communications and Multimedia Security. – 2014. – P. 63-72. – DOI: 10.1007/978-3-662-44885-4_5.
3. **Кузнецова, Н. М.** Решение задачи автоматизации процессов защиты стратегически важных ресурсов предприятия от комплексных кибератак на основе анализа тактик злоумышленников / Н. М. Кузнецова, Т. В. Карлова, А. Ю. Бекмешов // Вестник Брянского государственного технического университета. – 2020. – № 7(92). – С. 48-53. – DOI: 10.30987/1999-8775-2020-7-48-53.

4. **Methods Dedicated to Fight Against Complex Information Security Theats on Automated Factories Systems** / T. V. Karlova, N. M. Kuznetsova, S. A. Sheptunov, A. Y. Bekmeshov // 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS). – 2016. – P. 23-27. – DOI: 10.1109/ITMQIS.2016.7751927.
5. **Федеральный закон** «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. – URL: http://www.consultant.ru/documents/cons_doc_LAW_220885 (дата обращения: 12.03.2021).
6. **ГОСТ Р ИСО/МЭК 15408-1-2012** Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель = Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model: нац. стандарт Российской Федерации : изд. офиц. : утв. и введ. в действие Приказом Федер. агенства по техн. регулированию и метрологии от 15 ноября 2012 г. № 814-ст. : введ. взамен ГОСТ Р ИСО/МЭК 15408-1-2008 : дата введ. 2013-12-01 / подг. Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»), Федеральным государственным унитарным предприятием «Ситуационно-кризисный Центр Федерального агенства по атомной энергии» (ФГУП «СКЦ Росатома») : Стандартинформ, 2014.
7. **Advanced social engineering attacks** / K. Krombholz, H. Hobel, et al. // Journal of Information Security and Applications. – 2015. – June. – P. 113–122. – DOI: 10.1016/j.jisa.2014.09.005.
8. **ATT&CK Matrix for Enterprise.** – URL: https://attacks.mitre.org (дата обращения: 12.03.2021). – Режим доступа: для зарегистрир. пользователей. – Текст. : электронный.
9. **Kim, Y.** Involvers' Behavior-based Modeling in Cyber Targeted Attack / Y. Kim, I. Kim // Eighth International Conference on Emerging Security Information, Systems and Technologies. – 2014. – P. 132–137. – ISBN 978-1-61208-376-6.
10. **Марков, А. С.** Организационно-технические проблемы защиты от целевых вредоносных программ типа StuxNet / А. С. Марков, А. А. Фадин // Вопросы кибербезопасности. – 2013. – № 1(1). – С. 28–36.

1. **Virvilis, N**. Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game? / N. Virvilis, D. Gritzalis, T. Apostolopoulos // 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing., – 2013. – P. 396-403. – DOI: 10.1109/UIC-ATC.2013.80.
2. **Chen, P.** A Study on Advanced Persistent Threats / P. Chen, L. Desmet, C. Huygens // Communications and Multimedia Security. – 2014. – P. 63-72. – DOI: 10.1007/978-3-662-44885-4_5.
3. **Kuznetsova, N. M.** Solving the problem of automating the processes of protecting strategically important enterprise resources from complex cyber attacks based on the analysis of the tactics of violators / N. M. Kuznetsova, T. V. Karlova, A. Yu. Bekmeshov // Bulletin of the Bryansk State Technical University. – 2020. – № 7(92). – C. 48-53. – DOI: 10.30987/1999-8775-2020-7-48-53.
4. **Methods Dedicated to Fight Against Complex Information Security Theats on Automated Factories Systems** / T. V. Karlova, N. M. Kuznetsova, S. A. Sheptunov, A. Y. Bekmeshov // 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS). – 2016. – P. 23-27. – DOI: 10.1109/ITMQIS.2016.7751927
5. **Federal Law"** On the Security of the Critical Information Infrastructure of the Russian Federation " dated 26.07.2017 No. 187 FZ. - URL: http://www.consultant.ru/documents/cons_doc_LAW_220885 (accessed: 12.03.2021).
6. **GOST R ISO/IEC 15408-1-2012** Information Technology (IT). Methods and means of ensuring security. Criteria for evaluating the security of information technologies. Part 1. Introduction and general model = Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model: national Standard of the Russian Federation: ed. ofits.: approved and introduced. put into action by Order of Feder. tech agencies. regulation and metrology of November 15, 2012 No. 814-art.: introduction. instead of GOST R ISO/IEC 15408-1-2008: date of introduction. 2013-12-01 / subg. Limited Liability Company " Information Security Center "(LLC" CBI"), Federal Autonomous Institution "State Research and Testing Institute for Technical Protection of Information of the Federal Service for Technical and Export Control "(FAA "GNII PTZI FSTEC of Russia"), Federal State Unitary Enterprise " Situational Crisis Center of the Federal Atomic Energy Agency "(FSUE "SCC Rosatom"): Standartinform, 2014.
7. **Advanced social engineering attacks** / K. Krombholz, H. Hobel, et al. // Journal of Information Security and Applications. – 2015. – June. – P. 113–122. – DOI: 10.1016/j.jisa.2014.09.005.
8. **ATT&CK Matrix for Enterprise.** – URL: https://attacks.mitre.org (дата обращения: 12.03.2021). - Access mode: for registered users. users. - Text.: electronic.

9. **Kim, Y.** Involvers' Behavior-based Modeling in Cyber Targeted Attack / Y. Kim, I. Kim // Eighth International Conference on Emerging Security Information, Systems and Technologies. – 2014. – P. 132–137. –ISBN 978-1-61208-376-6.

10. **Markov, A. S.** Organizational and technical problems of protection against targeted malware such as StuxNet / A. S. Markov, A. A. Fadin / / Questions of cybersecurity. – 2013. – № 1(1). – P. 28-36.

Ссылка для цитирования:

Кузнецова, Н.М. Построение модульной структуры автоматизированной системы комплексного обеспечения защиты стратегически важных ресурсов предприятия транспорта / Н.М. Кузнецова, Т.В. Карлова, А.Ю. Бекмешов // Вестник Брянского государственного технического университета. – 2021. - № 9. – С. 36 - 42 . DOI: 10.30987/1999-8775-2021-9-36-42.

Статья поступила в редакцию 17.03.21.
Рецензент: к.т.н., доцент Брянского государственного технического университета Рытов М.Ю.
Статья принята к публикации 26.08.21.

Сведения об авторах:

Кузнецова Наталия Михайловна, к.т.н., доцент, Московский государственный технологический университет «СТАНКИН», e-mail: knm87@mail.ru.
Карлова Татьяна Владимировна, д. соц. н., к. т. н., профессор, Институт конструкторско-технологической информатики Российской академии наук, e-mail: karlova-t@yandex.ru.
Бекмешов Александр Юрьевич, к.т.н., доцент, Институт конструкторско-технологической информатики Российской академии наук, e-mail: b-a-y-555@yandex.ru.

Kuznetsova Natalia Mikhailovna, Candidate of Technical Sciences, Associate Professor, Moscow State Technological University "STANKIN"**,** e-mail: knm87@mail.ru.
Karlova Tatyana Vladimirovna, Doctor of Social Sciences, Candidate of Technical Sciences, Professor, Institute of Design and Technological Informatics of the Russian Academy of Sciences, e-mail: karlova-t@yandex.ru.
Bekmeshov Alexander Yurievich, Candidate of Technical Sciences, Associate Professor, Institute of Design and Technological Informatics of the Russian Academy of Sciences, e-mail: b-a-y-555@yandex.ru.