DOI 10.36622/VSTU.2023.26.3.022
УДК 004.056.

НАУЧНО-ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ КАФЕДРЫ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ПРОГРАММЫ «КИБЕРПОЛИГОН»

А.Г. Остапенко, С.С. Куликов, А.А. Остапенко, Е.А. Москалева, Е.С. Петрова

Обучение современных специалистов в вузе требует активного участия студентов в проектной деятельности и научной деятельности кафедр. Требования со стороны работодателей и Минобразования неуклонно усложняются ввиду стремительного технического прогресса. Это приводит к необходимости формирования новых методов и подходов к обучению со стороны профессорско-преподавательского состава вуза. В 2022/2023 учебном году кафедра систем информационной безопасности Воронежского государственного технического университета успешно осуществила работу по созданию и внедрению в учебную деятельность студентов и аспирантов киберполигона. В статье предложена организация проектной и научной деятельности кафедры информационной безопасности на основе киберполигона и изложены организационные и правовые мероприятия для его функционирования.

Ключевые слова: киберполигон, кибердружина, информационная безопасность, организационно-правовое обеспечение программы, дорожная карта программы, проектная деятельность кафедры.

Введение

В 2022 году кафедра систем информационной безопасности Воронежского государственного технического университета (в лице ее профессорско-преподавательского состава и членов кибердружины) выступила с инициативой о создании киберполигона, как платформы для качественного развития учебно-научного процесса [1, 2].

Основные результаты проведенной работы следующие:

1) значительно возросла медиаактивность кафедры, что способствовало успешному набору первокурсников в 2022/2023 и 2023/2024 учебных годах и распределению выпускников кафедральных специальностей 2023 года, а также укреплению позиций кафедры на рынке труда (через встречи студентов с работодателями, регулярно проводимые кафедрой совместно с hh.ru);

2) систематическое и активное вовлечение студенчества в научно-исследовательский процесс кафедры (НИРС) обусловило в 2022 и 2023 годах публикацию свыше 40 ВАКовских статей в соавторстве со студентами-членами вузовской кибердружины. Неслучайно 14 из них стали стипендиатами Президента и Правительства Российской Федерации;

3) в рамках проекта «Безопасный Интернет» в 2022, 2023 годах кафедра подготовила и опубликовала ряд статей в выпусках научного журнала «Информация и безопасность», осуществила два выпуска сборника научных работ «Управление информационными рисками и обеспечение безопасности телекоммуникационных систем», выпустила в свет седьмую монографию серии «Теория сетевых войн».

Создание киберполигона существенно помогло выполнить столь масштабные задачи. Кроме того, потенциал созданного киберполигона позволит в будущем, как минимум, не снижать показатели кафедры. В учебной работе кафедры деятельность по созданию киберполигона и осуществлению его функционирования помогла в организации проектной деятельности студентов.

В статье мы делимся полученным опытом организации и планирования работы киберполигона. Ниже приводится проект дорожной карты этой программы, рассчитанной на среднесрочный период консолидации преподавательского состава кафедры и ее студенческого контингента, включая кибердружину.

Мероприятия программы

Правовые основы обеспечения информационной безопасности опираются на законы и Указы Президента Российской Федерации, правительственные директивы, а также ГОСТы и стандарты NIST, ISO/МЭК в области защиты информации и информационной безопасности. Вместе с тем, на уровне решаемых при создании киберполигона задач необходима соответствующая организационно-правовая конкретизация, которая и предлагается в настоящей статье. Причем, это делается на вузовском примере для создания корпоративного киберполигона учебного заведения.

В табл. 1 предложен план мероприятий для повышения публикационной активности участников.

Таблица 1

Повышение публикационной активности участников программы

№ п п	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответствен-ный
1	В соответствии с задачами программы «Киберполигон» и требованиями современности принципиально перестроить работу аспирантуры кафедры, включая: - подбор в аспирантуру кандидатов с существенным списком трудов по вышеуказанной тематике и проведение с ними собеседования с учетом обязательства обеспечения требуемой публикационной активности в период обучения на кафедре; - внедрение в индивидуальные планы аспирантов кафедры (в качестве обязательных пунктов) пунктов подготовки статей и/или тезисов докладов, патентов по результатам их исследований, в том числе в кафедральных изданиях: научный журнал «Информация и безопасность», сборник научных трудов «Управление информационными рисками и обеспечение безопасности телекоммуникационных систем»; при аттестации аспирантов обращение особого внимания на выполнение плана подготовки ими публикаций; представление к именным стипендиям Президента Российской Федерации аспирантов, обладающих наибольшим количеством публикаций ВАКовского статуса по профилю реализуемых кафедрой программ и проектов; привлечение наиболее одаренных аспирантов к написанию рукописей,	Ежегодно в среднем 10 аспирантских научных публикаций	В течение каждого учебного года	Руководители аспирантов

Продолжение табл. 1

№ п п	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответствен-ный
	издаваемых кафедрой монографий серии «Теория сетевых войн».			
2	Введение в практику подготовку совместно с руководителями проектов и производственных практик научных публикаций: - студентами, наиболее удачно выполнившими актуальные курсовые работы; студентами, выполнившими оригинальные отчеты по производственной практике, - студентами-дипломниками, выполнившими выпускную квалификационную работу со значительной новизной и практической ценностью.	Ежегодно в среднем 10 студенческих научных публикаций	В течение каждого учебного года	Руководители курсового проектирования, практик и выпускных
3	В порядке реализации программы «Киберполигон» в издательстве «Горячая линия – Телеком» (г. Москва) издание книг серии «Теория сетевых войн», в частности, под редакцией РАН, в частности: - представление в издательство рукописи монографии с условным названием «Риски сетей интернета вещей»; - представление в издательство рукописи монографии с условным названием «Интеллектуальная картография киберпространства»; - представление в издательство рукописи монографии с условным названием «Социо-технический киберполигон»; - представление в издательство рукописи монографии с условным названием «Организационно-правовая защита сетей»; - представление в издательство рукописи монографии с условным названием «Интернет-девальвации традиционных ценностей».	Ежегодно в среднем 1-2 монографии Монография объемом около 300 страниц Монография объемом около 300 страниц Монография объемом около 300 страниц Монография объемом около 300 страниц Монография объемом около 300 страниц	По нижеприведенному календар-ному плану: Октябрь 2023 года Апрель 2024 года Октябрь 2024 года Февраль 2025 года Октябрь 2025 года	Заведующий кафедрой

Основной движущей силой научной деятельности кафедр является проведение НИР, ОКР и НИРС. Для качественной научной работы требуются материалы и средства. Для получения и/или увеличения финансирования проектов НИР и ОКР необходимо монетизировать их результаты, заинтересовывать и привлекать к совместной

работе фирмы и предприятия, занимающиеся соответствующим родом деятельности. Попутно это позволяет организовывать практическую деятельность и трудоустройство студентов.

В табл. 2 предложены мероприятия продвижения ожидаемых результатов научной деятельности кафедры ([3-6]). В табл. 3 предложены мероприятия по вовлечению студентов в научную, практическую и проектную деятельность.

Таблица 2

Увеличение объемов доходов от НИР, ОКР и услуг

Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
В целях формирования перспектив монетизации научно-технических продуктов кафедры по программе «Киберполигон» планируется:	Комплекс ПО «Киберполигон»	2024 год	Заведующий кафедрой
- приступить на кафедре к опытной эксплуатации полигонных: блока навигации по технологиям искусственного интеллекта и блока навигации по средствам тестирования на проникновение;	ПО блоков навигации	Сентябрь 2023 года	
- приступить на кафедре к опытной эксплуатации полигонных: блока симуляции инфраструктуры, а также – блока эмуляции сетевых атак;	ПО блоков эмуляции	Ноябрь 2023 года	
- осуществить интеграцию отлаженных блоков в общую пилотную полигонную систему;	Системное ПО	Январь 2024 года	
- путем проведения совместных киберучений опытная демонстрация системы для сотрудников базовых предприятий кафедры;	Результаты тестирования ПО на киберучениях	Март 2024 года Май 2024 года	
- с учетом полученных от специалистов замечаний доработка системы и создание ее демоверсии для предложения продукта широкому потребителю.	Демоверсия системы	Июнь 2024 года	

Таблица 3

Вовлечение обучающихся в программу

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответствен-ный
1	В рамках реализации программы «Кибеполигон» и стратегического проекта «Безопасный Интернет» массированное внедрение в курсовое проектирование и производственные практики кафедры элементов НИРС, прежде всего, в части: - целеполагания проектной деятельности по формализации: актуальности исследования, его предмета и объекта, выявленных в	Проекты, соответ-ствующие требованиям современ-ности	Регулярно в течение каждого учебного года	Руководители проектов и практик от кафедры и базовых предприятий

Продолжение табл. 3

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
	аналогах противоречий, цели исследования и его задач по разрешению обозначенных противоречий, ожидаемых результатов решения поставленных задач, оценки их новизны и практической ценности; методологии риск-анализа, предусматривающей на основе данных моделирования или статистики оценку рисков реализации кибератак в виде функции произведения величины ущерба на вероятность его наступления, построение риск-ландшафтов сценариев (векторов) атак и используемых ими уязвимостей, выявление наиболее опасных сочетаний сценарий – уязимость, требующих особого внимания с точки зрения обеспечения информационной безопасности; - создания и практического использования методического обеспечения организационно-правового и технического регулирования рисков успешной реализации сетевых атак, широко применяемых в современном кибер-противоборстве в отношении элементов критической информационной инфраструктуры Российской Федерации, ее корпораций и учреждений; - расширения практики подготовки (по наиболее удачным результатам проектирования) научных статей, докладов и патентов в соавторстве с руководителями проектов.			
2	В рамках реализации программы «Киберполигон» и стратегического проекта «Безопасный Интернет» включение в повестку регулярно проводимых кураторских интернет-часов вопросов научно-исследовательской деятельности кафедры с информацией по: - направлениям и руководителям исследований самых перспективных	Пропаганда среди студенчества направлений и результатов научной деятельности кафедры	Ежемесячно в течение каждого учебного семестра	Кураторы учебных групп кафедры

Окончание табл. 3

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
	аспектов обеспечения информационной безопасности, реализуемых на кафедре в части защиты интернета вещей, создания киберполигона, картографии защищаемого киберпространства, мониторинга социо-информационного пространства и др.; - существу научных достижений кафедры, включая издаваемые ею статьи в научном журнале «Информация и безопасность» и сборнике научных трудов «Управление информационными рисками и обеспечение безопасности телекоммуникационных систем», а также - монографии серии «Теория сетевых войн»; - практическим разработкам студентов-членов кибердружины, представляющим научно-технический интерес для оценки и регулирования рисков прежде всего в рамках программы «Киберполигон» и стратегического проекта «Безопасный Интернет», реализуемых кафедрой; кибердружинникам, удостоенных именных стипендий Правительства Российской Федерации и Президента Российской Федерации по результатам своей НИРС в рамках вышеперечисленных проектов и программ, реализуемых кафедрой			
3	В рамках реализации программы «Киберполигон» и стратегического проекта «Безопасный Интернет» публичное освещение деятельности наиболее успешных кибердружинников в вузовских и иных СМИ, включая представление их к именным стипендиям и прочим поощрениям, распределение в аспирантуру кафедры.	Публикации в СМИ и именные стипендиаты	Регулярно в течение каждого учебного года	Заведующий кафедрой

С учетом массового вовлечения студентов и аспирантов (табл. 3), функционирующая на кафедре (в рамках программы «Киберполигон» и

стратегического проекта «Безопасный Интернет») кибердружина фактически является молодежной научной лабораторией, где вокруг профессоров и докторантов кафедры постоянно кристаллизуются коллективы студентов с высоким творческим потенциалом, систематически ведутся фундаментальные исследования, реализуются практические разработки по актуальным направлениям: защита интернета вещей [4], картография защищаемого киберпространства, борьба с деструктивным контентом [3], выявление лиц с высоким риском девиантного поведения [2], эмуляция кибератак [5] и т. п., расширяются творческие контакты с заинтересованными организациями, которые предоставляют кибердружинникам дистанционный доступ к своим вычислительным ресурсам для реализации совместных программ типа «Киберполигон». Вследствие этого логично создавать на кафедре молодежные научные лаборатории (табл. 4).

Таблица 4

Создание молодежных научных лабораторий

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
1	Создание студенческих коллективов с высоким потенциалом под руководством профессоров и докторантов кафедры.	Перспективная дружина, действующая научная лаборатория, научные результаты кафедры	Сентябрь 2023	Заведующий кафедрой
2	Проведение фундаментальных исследований, реализация практических разработок по актуальным направлениям		В течение учебного года	Руководитель коллектива
3	Расширение творческих контактов с заинтересованными организациями		В течение учебного года	Заведующий кафедрой, руководители коолективов
4	Освещение результатов работы кибердружины в вузовских и иных СМИ с целью активного вовлечения в ее ряды наиболее талантливой молодежи		В течение учебного года	Руководитель коллектива
5	Распределение лучших кибердружинников в аспирантуру кафедры и продолжение на базе вуза деятельности в целях обеспечения информационной безопасности Российской Федерации.		Июнь 2023	Заведующий кафедрой

Вовлечение студентов и аспирантов в работу по киберполигону (табл. 3) и создание для этого творческих коллективов по тематикам работ (табл. 4) облегчает задачу развития и продолжения научных наработок кафедры. Привлекаемые к проектам и НИР на базе киберполигона творчески мыслящие успешные студенты продолжают свою деятельность в аспирантуре и впоследствии пополняют преподавательский состав кафедры, тем самым омолаживая и подпитывая его.

С целью привлечения талантливых студентов в аспирантуру и в дальнейшем к работе на кафедре необходимо проводить мероприятия по разъяснению преимуществ преподавательской и научной деятельности в вузе (табл. 5). В целях обеспечения успешной защиты диссертаций, подготовленных аспирантами и

докторантами кафедры по программе «Киберполигон», необходимо проводить ряд соответствующих мероприятий, как например показано в табл. 6.

Таблица 5

Омоложение кадров кафедры

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
1	Участие аспирантов в подготовке и проведении для младшекурсников мастер-классов по актуальным вопросам обеспечения информационной безопасности	Молодежный резерв педагогического состава кафедры	В течение учебного года	Руководитель аспиранта
2	Проработка вопросов о приобретении аспирантами педагогического стажа при реализации учебной работы в вузе		В течение учебного года	Заведующий кафедрой
3	Введение в практику подготовку аспирантами методических указаний по результатам своей педагогической деятельности		В течение учебного года	Руководитель аспиранта
4	Регулярное поддержание связей с выпускниками, проявившими склонности к педагогической деятельности, с целью привлечения их к учебному процессу на кафедре		В течение учебного года	Заведующий кафедрой, ответственный за производственную практику преподаватель
5	Подбор кадров на педагогическую работу среди «ветеранов» кибердружины и участников программы «Киберполигон».		Июнь 2023	Заведующий кафедрой

Таблица 6

Подготовка кадров высшей квалификации

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
1	Установление контактов для доработки научно-квалификационных работ (НКР) под требования диссертационных советов, функционирующих на базовых предприятиях кафедры.	Предложения по созданию диссертационных советов	2024 год	Заведующий кафедрой
2	Проведение требуемых защит НКР в параллельных советах и формирование предложений по открытию диссертационного совета ВГТУ по соответствующей специальности.			

Продолжение табл. 6

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
3	Проработка вопроса о создании объединенного диссертационного совета ВГТУ совместно с другими организациями.	Предложения по созданию диссертационных советов	2024 год	Заведующий кафедрой

Поскольку обучение студентов по специальностям, связанным с информационной безопасностью в конечном итоге подразумевает подготовку квалифицированных специалистов по информационной безопасности, то вместе с научно-исследовательской деятельностью на киберполигоне (табл. 1, 3, 4) и деятельностью, направленной на обеспечение творческих и квалифицированных кадров кафедры (табл. 4-6), нельзя забывать о том, на что собственно эта деятельность направлена. Так в целях реализации положений Доктрины информационной безопасности Российской Федерации [7] кафедра должна заниматься установлением и укреплением связей и партнерских отношений с органами власти и спецслужбами РФ (Главное управление специальных программ Президента России, ФСБ и ФСТЭК России). Такие отношения могут быть сформированы как на региональном, так и на более высоком уровне. Пример планирования подобной деятельности приведен в табл. 7.

Таблица 7

Развитие инфраструктуры научно-исследовательской деятельности

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
1	Деятельность по предотвращению интернет-девальвации традиционных ценностей путем: - риск-анализа статистических данных роста количества адептов деструктивных идеологий (мультигендерства, ЛГБТ, чайлдфри и др., распространяемых в информационном пространстве и внедряемых в общественное сознание коллективным Западом); - развития организационно-правового обеспечения противодействия вышеуказанным идеологемам в области законодательства, пропаганды, образования и воспитания молодежи Российской Федерации.	Методическое и организационно-правовое обеспечение защиты информационного пространства	2024 год	Заведующий кафедрой, руководители творческих лабораторий
2	Установление контактов и партнерских связей с отечественными регуляторами в сфере обеспечения информационной безопасности	Апробируемое обеспечение киберполигона	2024 год	Заведующий кафедрой

Продолжение табл. 7

№ пп	Проводимые мероприятия	Ожидаемый результат	Сроки	Ответственный
	на предмет использования результатов программы «Киберполигон» для: - тестирования корпоративных сетей на основе проведения киберучений отражения сетевых атак, в том числе с учетом угроз, человеческого фактора, порождаемых персоналом защищаемых систем; - совершенствования не только технического, но и организационно-правового обеспечения противодействия сетевым вторжениям с различными используемыми уязвимостями и векторами атаки.			
3	Совместно с ИПУ РАН и ФУ при Правительстве РФ формирование Научно-образовательного центра (НОЦ) управления информационными рисками, имея в виду: - консолидацию интеллектуальных потенциалов участников НОЦ, созданных там методических обеспечений оценки и регулирования рисков; - удаленный доступ к информационным ресурсам партнеров НОЦ, расширяющий возможности разработчиков киберполигона; - ьсовместное использование продуктов программы «Киберполигон» в учебном процессе и научных исследованиях в сфере обеспечения информационной безопасности Российской Федерации.	Центр коллективного пользования	2024 год	Заведующий кафедрой

Заключение

Создание киберполигона является достаточно амбициозной задачей, укрепляющей имидж Воронежского государственного технического университета в научно-образовательном пространстве региона и страны, так как в случае ее успешного решения перед его преподавателями и студентами специальностей в сфере обеспечения информационной безопасности открываются широкие перспективы принципиальной перестройки учебного процесса в части перевода лабораторного практикума,

курсового и дипломного проектирования на рельсы реальной отработки механизмов сетевого противоборства в кибернетическом пространстве. В этом случае для студентов появляется возможность дистанционно приобретать знания и навыки защиты информационных систем и сетей различного назначения от многообразия векторов кибератак, использующих многочисленные уязвимости программного обеспечения. Появляется перспектива организации и проведения виртуальных кибер-учений для телекоммуникационных структур с произвольной топологией и спецификацией.

Принципиальным достоинством киберполигона является возможность в ходе вышеупомянутых учений осуществить оценки и регулирования рисков, т. е. возможность управления защищенностью тестируемых систем и сетей [1]. Здесь студенту и аспиранту открывается перспектива отработки проектных решений в реальных ситуациях борьбы с различными вредоносами, настройки подсистем защиты в целях обеспечения безопасности исследуемых объектов [1-6]. Для этого планируется интеллектуальная поддержка создания программно-технического и организационно-правового обеспечения, адекватного информационным атакам злоумышленников.

При этом отличительной особенностью проектируемого киберполигона является его социотехническая направленность, учитывающая человеческий фактор, являющийся причиной многих сетевых и системных ущербов.

Все вышеизложенное поднимет на качественно новый уровень состояние учебного и научного процесса, обеспечит повышенный профессиональный успех выпускников университета по специальностям в области обеспечения информационной безопасности.

Кроме того, при всей масштабности программы ее реализация даст весьма значительную экономию в приобретении специального оборудования, необходимого для образовательной и исследовательской деятельности, за счет виртуализации и дистанционного ее осуществления.

Список литературы

1. Остапенко Г.А. Киберполигон как проект управления информационными рисками / Г.А. Остапенко, В.И. Белоножкин, А.А. Остапенко, М.Е. Волкова // Информация и безопасность. 2023, Т. 26, Вып. 1. С. 9-16.

2. Остапенко Г.А. Разработка архитектуры киберполигона для повышения качества и результативности учебного процесса в исследовании атак на информационные системы и сети / Г.А. Остапенко, С.С. Куликов, А.В. Коноплин, А.А. Остапенко // Информация и безопасность. 2023, Т. 26, Вып. 1. С. 101-108.

3. Сердечный А.Л. Создание киберполигона: блок навигации по средствам тестирования на проникновение / А.Л. Сердечный, А.А. Карданов, А.Т. Труфанов // Информация и безопасность. 2023, Т. 26, Вып. 2. С. 177-190.

4. Сердечный А.Л. Создание киберполигона: блок навигации по технологиям искусственного интеллекта и машинного обучения / А.Л. Сердечный, А.Т. Труфанов, А.А. Карданов // Информация и безопасность. 2023, Т. 26, Вып. 2. С. 211-224.

5. Куликов С.С. Создание киберполигона: формирование блока эмуляции и сканирования инфраструктуры / С.С. Куликов, А.И. Саушкин // Информация и безопасность. 2023, Т. 26, Вып. 2. С. 285-292.

6. Куликов С.С. Создание киберполигона: формирование блока симуляции / С.С. Куликов, В.К. Федоров // Информация и безопасность. 2023, Т. 26, Вып. 2. С. 293-302.

7. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения 20.08.2023).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 26.08.2023

Информация об авторах

Остапенко Александр Григорьевич – д-р техн. наук, заведующий кафедрой, Воронежский государственный технический университет, email: alexanderostapenkoias@gmail.com

Куликов Сергей Сергеевич – канд. техн. наук, доцент, Воронежский государственный технический университет, email: email: alexanderostapenkoias@gmail.com

Остапенко Александр Алексеевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, Воронежский государственный технический университет, email: alexanderostapenkoias@gmail.com

Петрова Елена Сергеевна – старший преподаватель, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

SCIENTIFIC AND PROJECT ACTIVITY OF THE DEPARTMENT OF INFORMATION SECURITY SYSTEMS WITHIN "CYBER TRAINING GROUND" PROGRAM

A.G. Ostapenko, S.S. Kulikov, A.A. Ostapenko, E.A. Moskaleva, E.S. Petrova

Training modern specialists at a university requires the active participation of students in project activities and scientific activities of departments. Requirements from employers and the Ministry of Education are steadily becoming more complex due to rapid technological progress. This leads to the need for the formation of new methods and approaches to learning on the part of the teaching staff of the university. In the 2022/2023 academic year, the Department of Information Security Systems of the Voronezh State Technical University successfully carried out work to create and implement a cyber training ground in the educational activities of students and postgraduates. The article proposes the organization of project and scientific activities of the Department of Information Security on the basis of a cyber training ground and outlines organizational and legal measures for its functioning.

Keywords: cyber training ground, cyber squad, information security, organizational and legal support of the program, program roadmap, project activities of the department.

Submitted 26.08.2023

Information about the authors

Alexander G. Ostapenko – Dr. Sc. (Technical), Head of the Department, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Sergey S. Kulikov – Cand. Sc (Technical), Associated Professor, Voronezh State Technical University, email: alexanderostapenkoias@gmail.com

Alexander A. Ostapenko – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Elena S. Petrova – Senior Lecturer, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com