DOI 10.36622/VSTU.2023.26.1.012
УДК 004.056

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

В статье предложен подход к созданию «Киберполигона». В основе подхода лежит разбиение архитектуры на блоки. Такой подход представляет возможность развития и масштабирования системы в перспективе. Модульная архитектура обеспечит фундамент для развития предлагаемого решения и позволит модифицировать с учетом специфических тонкостей информационных сетей. В работе представлены схемы функционирования различных блоков общей архитектуры, учитывающие полное обеспечение пользователя полигона необходимой информацией и проверкой различных аспектов тестируемой сети. Предложенные в работе модули могут стать основой для обобщенной системы, которая позволит пользователю услугу по полноценному анализу выбранной информационной системы. Представленные результаты основаны на опыте уже созданных решений, с учетом их недостатков и преимуществ. Целью разработки архитектуры является повышение качества и результативности учебного процесса в исследовании атак на информационные системы и сети.

Ключевые слова: киберпространство, киберполигон, сеть, атака.

Введение

В информационных системах с каждым годом продолжает увеличиваться объем хранимой информации, включая сведения в сферах политики и обороноспособности страны, экономики, науки и техники, а также персональных данных граждан. Вследствие этого возрастает важность обеспечения защищенности информационных систем и информационно-телекоммуникационных сетей от нарастающих угроз информационного характера, которые могут быть реализованы злоумышленниками, постоянно совершенствующими арсенал используемых ими средств и устройств. Поэтому построение компьютерных полигонов в сфере информационной безопасности – активно обсуждаемая проблема, над решением которой работают многие отечественные и зарубежные исследователи. Киберполигон – это интерактивная, виртуальная локальная сеть любой организации, системы, с набором инструментов и программ, которые подключены к виртуальному (симулированному) Интернету. Он обеспечивает среду для приобретения практических навыков работы с сетевыми устройствами и организации безопасного места для разработки и тестирования программного обеспечения. На киберполигонах участники могут отработать навыки защиты информационных систем. Киберполигон может включать реальное оборудование и программное обеспечение или представлять собой комбинацию физических и виртуальных компонентов. На уровне Интернета он не только имитирует трафик, но и воспроизводит сетевые сервисы, такие как веб-страницы, браузеры, электронная почта и многое другое.

В образовательном процессе потребность при изучении методик тестирования сетевых средств защиты информации и защищенности информационных телекоммуникационных сетей в целом в работе в условиях реальных сетей не может быть реализована без компьютерных полигонов.

Подход к разработке архитектуры

По большому счету пользователя киберполигона интересует, как поведет себя имеющееся в его распоряжении программное обсечение (ПО) в условиях реализации в отношении этого ПО тех угроз, которые существуют в киберпространстве и определяются многообразием атак и

уязвимостей. Априорно ему не известны все эти угрозы и их параметры, поэтому он желает получить достаточно полное представление о них и риск-оценку успешной их реализации на свое ПО.

В этом контексте киберполигон обязан предоставить пользователю услугу по формированию (автоматизированному) баз данных атак и уязвимостей, регулярно регистрируемых и публикуемых в интернет-пространстве с тем, чтобы он мог выбрать интересующие и популярные у злоумышленников деструктивы. Отдельный модуль киберполигона должен сканировать соответствующие сайты и извлекать из них важные для риск-анализа параметры инцидентов кибервторжения (частота атак, размеры нанесенного ущерба и т.п.). В качестве аналитической визуализации пользователю уместно представить информационные карты, отражающие на текущий момент множество интернет-упоминаний о реализуемых атаках и используемых ими уязвимостей. Вероятно, для этого потребуется самостоятельный модуль, демонстрирующий пользователю общую (либо частную для ПО) картину деструктивных кибер-воздействий.

Важнейшим модулем киберполигона следует считать риск-анализатор, где вычисляются величины рисков для заданных пользователем уязвимостей ПО. При этом, должна быть предусмотрена возможность вероятностной риск-оценки одновременно для нескольких уязвимость и видов атак. Такой многовариантный анализ открывает перед пользователями возможность комплексного исследования собственного ПО в пространстве действующих киберугроз. Желательно здесь также привлечь модуль аналитической визуализации, давая тем самым информацию лицам принимающих решения по защите ПО.

В перспективе также необходим модуль с элементами искусственного интеллекта, дающий пользователю подсказки по обеспечению безопасности ПО. В этом случае представляемый киперполигоном сервис (по тренингу в рамках оценки последствий возможных деструктивных воздействия) становится достаточно полноценным.

Ко всему прочему, за пользователем должно оставаться право ввода дополнительных данных (скажем, финансовых ущербов) из собственной практики информационного противоборства.

Киберполигон это удобная возможность собственнику (хозяину) контролируемого и защищаемого информационного пространства (сети исследуемой организации) посмотреть на него глазами атакующего злоумышленника, «подлатать» выявленные технические и социальные уязвимости, тем самым снизив уровень возможного ущерба.

При этом хозяин (клиент полигона) объективно заинтересован во всестороннем исследовании своей собственности на предмет успешности реализации актуальных угроз, индуцированных как техническим, так и человеческим факторами.

Успех вышеизложенного, вне всякого сомнения, возможен лишь при наличии у киберполигона необходимого и достаточного потенциала в виде:

1. Блока непрерывной актуализации данных и знаний (рис. 1), необходимых киберполигону, включая автоматизированный сбор (в реальном масштабе времени) в интернет-пространстве сведений о зарегистрированных уязвимостях программного обеспечения и кибератаках, способствующих этому контентах в социальных сетях, а также – средствах технического, организационного и правового обеспечения кибербезопасности.

2. Блока программно-технического анализа кибербезопасности исследуемой организации (рис. 2). Здесь соответствующие модули автоматизировано осуществляют риск-анализ уязвимостей программного обеспечения, используемого организацией, что должно способствовать укреплению его защиты, в том числе с учетом оценки возможных ущербов для атакуемой сети.

3. Блока человеческого фактора кибербезопасности исследуемой организации (рис. 3). Здесь клиенту предлагается возможность установления локализации в соцсетях интересующих его сотрудников, а также выявление и риск-анализ генерируемых ими постов.

4. Блока целеполагания по обеспечению кибербезопаности исследуемой организации (рис. 4). Здесь клиенту предполагается на основе накопленной базы данных и знаний, а также сведений, почерпнутых при исследовании организации, средствами искусственного интеллекта формировать предложения по коррекции ее программно-технического и нормативно-правового обеспечения кибербезопасности.

Степень проработанности проекта такова:

1. На программном уровне осуществляется отработка модулей парсинга и риск-анализа уязвимостей программного обеспечения, парсинга и риск-анализа контентов сотрудников, распознавания и риск-анализа эмоциональных состояний сотрудников.

2. На уровне алгоритмизации находятся модули эмуляции оценки ущербов кибератак, формирования рекомендаций по укреплению кибербезопасности.

3. На уровне разработки методического обеспечения находятся соответствующие алгоритмы и методики.

Принципиальным отличием от аналогов предлагаемой архитектуры киберполигона следует считать учет не только программно-технического, но и человеческого факторов (как известно, весьма весомого для защиты информации). Именно такой (комплексный) подход к проблеме, по нашему мнению, должен особо заинтересовать вероятную клиентуру полигона.

Востребованность проекта значительно увеличит запуск в эксплуатацию блока целеполагания, дающего клиенту интеллектуальные подсказки по обеспечению кибербезопасности.

Впервые среди технических решений данного профиля, вводится автоматизированная актуализация данных и знаний о вредоносах (обеспечивается постоянная боеготовность полигонных служб к новым вызовам).

Рис. 1. Схема функционирования блока актуализации данных знаний киберполигона

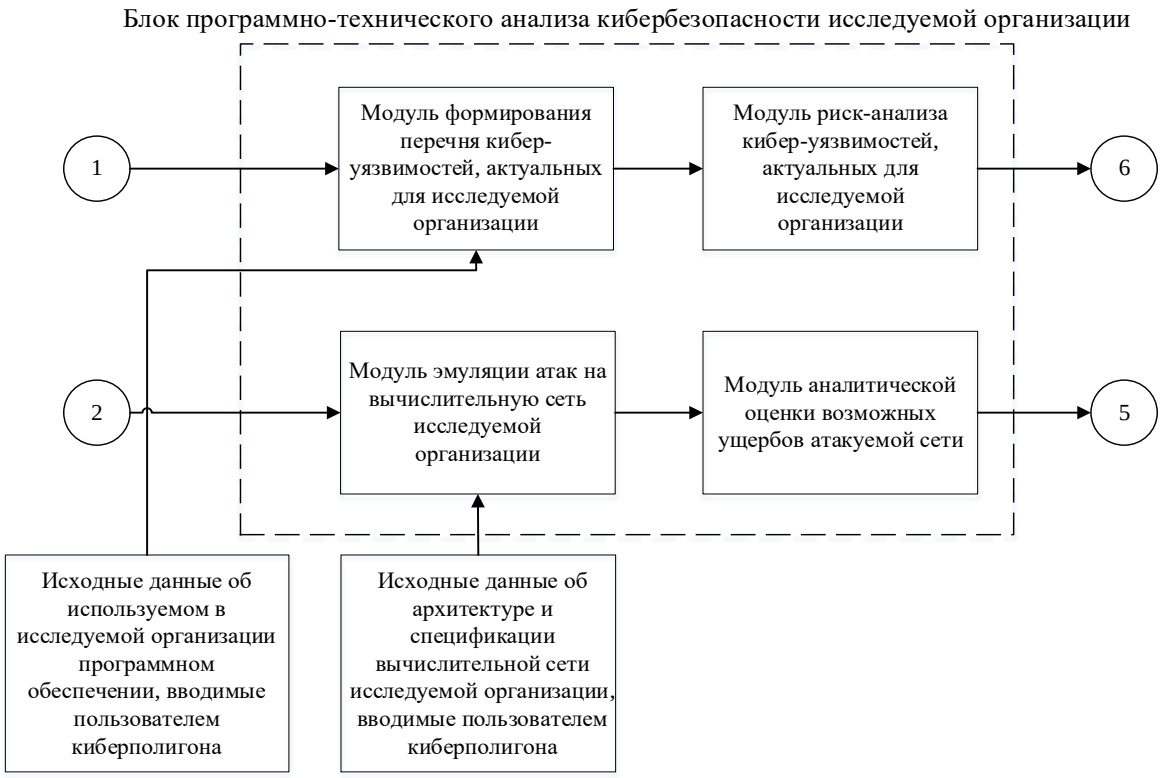

Рис. 2. Схема функционирования блока программно-технического анализа Киберполигона

Рис. 3. Схема функционирования блока учета человеческого фактора в обеспечении Киберполигона

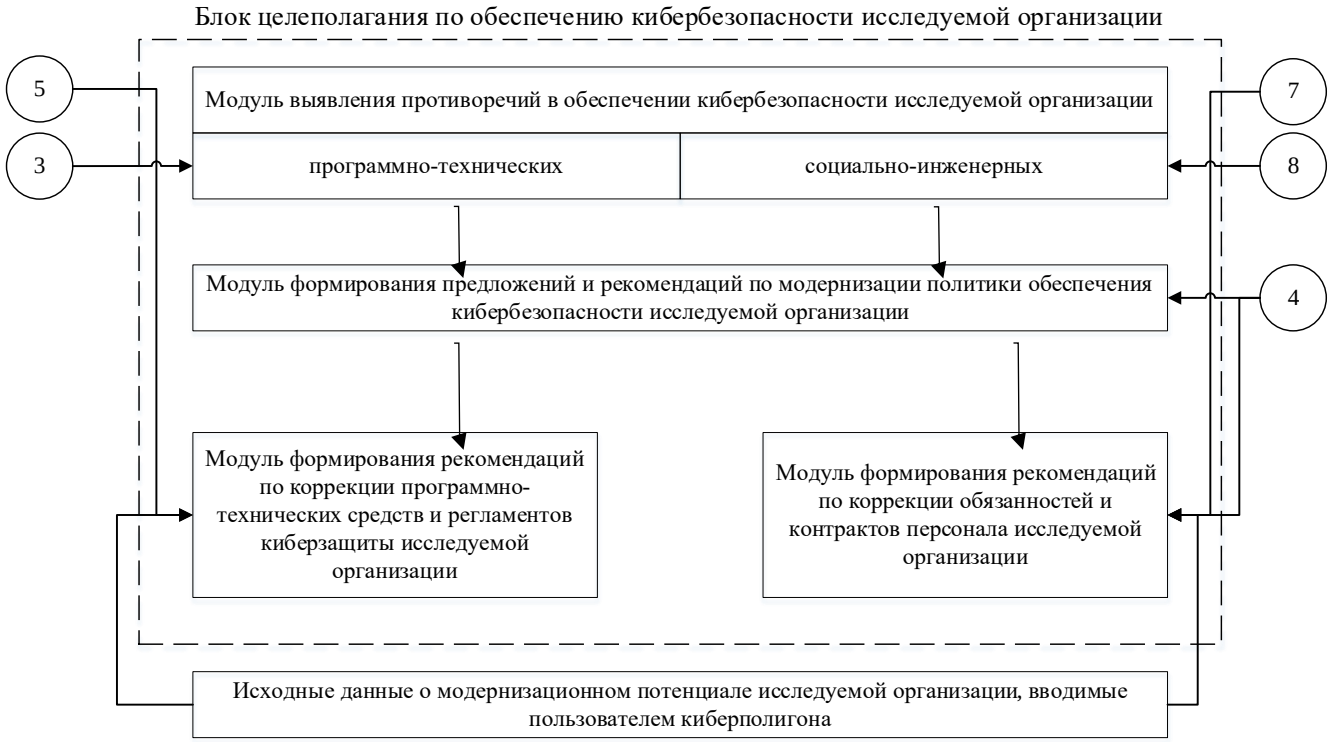

Рис. 4. Схема функционирования блока целеполагания

Сравнение с аналогами

Для объективной оценки создания киберполигона со всеми вышеперечисленными блоками необходимо рассмотреть уже существующие решения и учесть их недостатки. В настоящий момент на российском рынке представлены шесть крупных киберполигонов.

Ampire («Перспективный мониторинг»)

Представленное компанией «Перспективный мониторинг» решение включает в себя набор типовых шаблонов сети организации. Это может быть банк, офис или какое-либо предприятие промышленного производства. Компания также предлагает построение нового шаблона по условиям заказчика. Набор сценариев для атак задается вручную. Также решение предоставляет возможность проведения тренировок по концепции Red Team и Blue Team и индивидуальное обучение IT специалистов в области безопасности.

Решение может быть предоставлено в качестве программно-технического комплекса или в облачном варианте.

Преимуществами данного продукта являются:

- наличие возможности облачного подключения;
- практическое использование опыта компании в области пентестов и построения сценариев атак;
- возможности для индивидуального обучения специалистов.

Недостатками решения являются:

- отсутствие возможностей использования пользовательских сценариев и сторонних модулей;
- внедрение в учебный процесс ограничено использованием полигона только в режиме Blue Team;

BI.ZONE Cyber Polygon («Сбер» и «BI.ZONE»)

Каждый год проводится конференция «Cyber Polygon», организаторами которой являются «Сбер» и «BI.ZONE», при поддержке Интерпола и Центра кибербезопасности Всемирного экономического форума. Тематика ежегодных учений выбирается на основе текущей обстановки и актуальных киберугроз. Данное решение предлагает соревновательный вариант проведения. Задания могут выполняться как индивидуально, так и в составе заранее планируемых команд. Также существует услуга частного проведения учений для определенной организации.

Преимуществами данного продукта являются:

- актуализация тематики сценариев атак;
- бесплатное участие в соревновательном режиме.

Недостатками решения являются:

- отсутствие каких-либо пользовательских настроек, предпочтений и учета исходных данных;
- полное отсутствие возможностей внедрения подобного варианта в учебный процесс;
- невозможность развертывания на базе оборудования заказчика.

Jet CyberCamp («Инфосистемы Джет»)

Компания «Инфосистемы Джет» разработала свое решения киберполигона, которое предназначалось для внутреннего использования, в частности обучения сотрудников центра безопасности, занимающихся тестированием на проникновение. Данный продукт рассчитан на повышение квалификации специалистов по информационной безопасности. Предлагается комплексный подход к проведению тренировок, начиная теоретическими занятиями. Заканчивая практической отработкой навыков. Решение доступно в двух видах: облачный вариант на платформе владельца или развертывание на мощностях заказчика.

Преимуществами данного продукта являются:

- актуализация тематики сценариев атак;
- модульная система для реалистичной имитации инфраструктуры;
- индивидуальный подбор сценариев тренировок.

Недостатками решения являются:

- сборка системы заказчика не учитывает включение пользовательских модулей или сценариев;
- покупка или аренда решения не исключает проблему необходимости мощностей для его установки.

The Standoff (Positive Technologies)

Решение Positive Technologies представляет собой реалистичный макет атакуемой инфраструктуры, где участники могут наблюдать последствия атак. Продукт предлагает участие только в рамках соревнований, которое происходит на физической модели владельца полигона. Также компания разработала онлайн-платформу для киберучений, на которой любой желающий может попробовать свои силы.

Преимуществами данного продукта являются:

- воссоздание реальных процессов, существующих в различных сферах и компаниях;
- большой выбор режимов и сценариев взаимодействия с физической и виртуальной моделью;
- возможность участия в качестве команды защиты без заранее подготовленного сценария.

Недостатками решения являются:

- участие происходит исключительно в рамках соревнований;
- отсутствует возможность арендовать или купить настроенную инфраструктуру;
- невозможно использовать свои модули и наработки, в то числе в рамках учебного процесса.

«Киберполигон» (ООО «Киберполигон»)

Решение от данного производителя представляет собой виртуальную инфраструктуру, с возможностью проведения тренировок как для атакующей команды, так и для команды защитников. Платформа построена на модульной основе, поэтому заказчик может выбрать необходимые ему модули. Решение разработано в виде облачной платформы, но также может быть интегрировано в инфраструктуру заказчика.

Преимуществами данного продукта являются:

- наличие модуля для обучения сотрудника антифишинговым сценариям;
- возможность участия команд атаки и защиты одновременно;
- модульная архитектура.

Недостатками решения являются:

- невозможно использовать свои модули и наработки, в то числе в рамках учебного процесса;
- отсутствует возможность использования исходных данные клиента;
- отсутствие систем мониторинга.

Национальный киберполигон («Ростелеком»)

Данный инструмент создан как платформа, нацеленная на широкую аудиторию пользователей, как ИБ специалистов, так и студентов. Она предлагает большой спектр преднастроенных сегментов в разных сферах общества и промышленности. Решение предлагает варианты использования как в рамках соревнований, так и покупка или аренда, для настройки под клиента.

Преимуществами данного продукта являются:

- большой выбор готовых инфраструктур;
- актуальные сценарии атак;
- подробный отчет о результатах работы.

Недостатками решения являются:

- решение предлагает использовать только свои готовые варианты сетей;
- отсутствует возможность использования исходных данные клиента;
- невозможно использовать свои модули и наработки, в то числе в рамках учебного процесса.

Зарубежные аналоги в большинстве своем похожи на описанные выше российские варианты. Все они являются почти копиями друг друга. Отличия составляют только набор подготовленных сетевых сред и варианты развития процесса использования. Данные решения реализованы в качестве облачной инфраструктуры, поэтому развернуты только на стороне владельца. Ни один из вариантов не может предложить использование клиентских данных для построения сети или развития векторов атак.

Исходя из рассмотренных аналогов, можно сделать вывод о том, что:

- ни одно из существующих решений не способно в полном объеме подстроиться под нужды учебного процесса;
- перечисленные полигоны лишь частично могут отразить потребности заказчика в использовании собственных исходных данных как по векторам атак, так и установленном программном обеспечении;
- существующие продукты не поддерживают использование сторонних модулей (напр. модули разработанные студентами).

В связи с этим актуальным является разработка «Киберполигона» с использованием модульной системы и блоков (рис.1-4).

Заключение

Таким образом, в настоящей работе предложен облик архитектуры «Киберполигона», использование которой позволит по-новому посмотреть на киберпространство и протекающие в нем процессы. Перспектива разработки компьютерного полигона заключается в возможности практического применения его в учебном процессе для формирования у обучающихся компетенций, связанных с противодействием компьютерным атакам, с учетом ограниченности ресурсов виртуальной инфраструктуры.

Список литературы

14. Noponen S. Cybersecurity of Cyber Ranges: Threats and Mitigations / S. Noponen, J. Parssinen, J. Salonen // International Journal for Information Security Research (IJISR). 2022. V. 12. Is. 1. URL: https://infonomics-society.org/wp-content/uploads/Cybersecurity-of-Cyber-Ranges.pdf (дата обращения 10.02.23).

15. Архангельский О.Д. Практические подходы к созданию инфраструктуры индустриального киберполигона / О.Д. Архангельский, Д.В. Сютов, А.В. Кузнецов // Автоматизация в промышленности. 2020. № 1. С. 52−57.

16. Демьянов А. Тестирование кибербезопасности встроенных систем с помощью их цифрового двойника/ А. Демьянов // Электроника: наука, технология, безопасность. 2021. № 7 (208). С. 126−29.

17. Ульянов А.Н. Качество плюс наглядность применение технологий виртуализации вычислительных ресурсов в информационно-образовательной среде. / А.Н. Ульянов, М.Г. Столяров, И.В. Стельмах // ВВО. 2021. № 6 (33).

18. Назарова О.Г. Информационная безопасность в период становления цифровой экономики в России / О.Г. Назарова, А. . Клименко. // Экономика. Социология. Право. 2020. № 2 (18).

19. Пономарев И.М. Проектирование киберполигона в области информационной безопасности / И.М. Пономарев, А.А. Селиверстов, Г.А. Пеннер, И. Р. Зулькарнеев // URL:

https://elibrary.ru/download/elibrary_49518849_69459054.pdf (дата обращения 10.02.23).

20. Монахов М.Ю. О возможностях использования киберполигонов в качестве оценочных средств определения уровня сформированности компетенций / М.Ю. Монахов, А.В. Тельный, Д.В. Мишин // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 269-277.

Финансовый университет при Правительстве Российской Федерации

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 19.02.2023

Информация об авторах

Остапенко Григорий Александрович – д-р. техн. наук, профессор, проректор, Финансовый университет при Правительстве Российской Федерации, e-mail: mnac@comch.ru

Куликов Сергей Сергеевич – канд. техн. наук, Воронежский государственный технический университет, e-mail: mnac@comch.ru

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

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

DEVELOPMENT OF A CYBER POLYGON ARCHITECTURE TO IMPROVE THE QUALITY AND EFFECTIVENESS OF THE TRAINING PROCESS IN THE STUDY OF ATTACKS ON INFORMATION SYSTEMS AND NETWORKS

G.A. Ostapenko, S. S. Kulikov, A.V. Konoplin, A.A. Ostapenko

The article proposes an approach to creating a Cyberpolygon. The approach is based on the partitioning of the architecture into blocks. This approach presents an opportunity to develop and scale the system in the future. The modular architecture will provide a foundation for the development of the proposed solution and allow modification to take into account the specific subtleties of information networks. In the work schemes of functioning of different blocks of general architecture, taking into account full maintenance of the polygon user with necessary information and verification of different aspects of tested network are presented. The modules proposed in the work can become the basis for a generalized system that will allow the user to fully analyze the selected information system. The presented results are based on the experience of already created solutions, taking into account their disadvantages and advantages. The purpose of developing the architecture is to improve the quality and effectiveness of the learning process in the study of attacks on information systems and networks.

Keywords: cyberspace, cyber training ground, network, attack.

Submitted 19.02.2023

Information about the authors

Grigory A. Ostapenko - Doctor of Technical Sciences, Professor, Vice-Rector, Financial University under the Government of the Russian Federation, e-mail: mnac@comch.ru

Sergey S. **Kulikov** - PhD (technical sciences), Voronezh State Technical University, e-mail: mnac@comch.ru

Alexander V. **Konoplin** - Student, Voronezh State Technical University, e-mail: mnac@comch.ru

Alexander A. **Ostapenko** - Student, Voronezh State Technical University, e-mail: mnac@comch.ru