DOI 10.36622/1682-7813.2024.27.2.005
УДК 004.056

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ СЕТЕВОЙ КОНТРРАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ КОРПОРАЦИИ (ЧАСТЬ II)

**Д.В. Щербакова, А.Ю. Пекло, Д.С. Печкин,
В.М. Питолин, О.Ю. Макаров, В.Н. Кострова**

Предлагается структура и содержание частных регламентов сетевой контрразведки, где для эффективной защиты нужно обеспечить управление инцидентами нарушения сетевой безопасности корпорации при атаках типа «сетевая разведка». Выделенные типы инцидентов предназначены для расширения имеющейся классификации инцидентов и ориентированы на сетевую разведку. Описание начальной фазы реагирования на инциденты содержится в «Частным регламенте обнаружения и регистрации контрразведкой инцидентов нарушения сетевой безопасности организации». Руководство по обнаружение инцидентов приведено в «Частном регламенте реагирования контрразведки на инциденты нарушения безопасности организации». Заключительный этап обработки инцидента описан в «Частном регламенте ликвидации последствий инцидентов нарушения сетевой безопасности организации при атаках типа «сетевая разведка». Предлагается план мероприятий по противодействию атаке типа «сетевая разведка».

Ключевые слова: частный регламент, сетевая разведка, контрразведка, инцидент.

Введение

Регламенты, связанные с инцидентами нарушения сетевой безопасности корпорации, имеют высокую актуальность в настоящее время. С ростом числа угроз информационной безопасности (ИБ) и усложнением атак, важно анализировать произошедшие инциденты и выявлять их причины, чтобы предотвратить подобные ситуации в будущем. Оперативное реагирование на инциденты является важным компонентом стратегии – обеспечения корпоративной ИБ. Исследование инцидентов позволяет выявлять уязвимые места в системах безопасности, обнаруживать новые угрозы, определять уровень защищенности компьютерных систем и разрабатывать меры для повышения уровня безопасности. Кроме того, исследование инцидентов может помочь установить ответственных за совершение атак и принять правовые меры.

Таким образом, для эффективного реагирования на вышеупомянутые инциденты чрезвычайно важно заблаговременно выстроить четкий план управления инцидентами, поскольку именно в момент наступления инцидента, в условиях стресса и возможного отсутствия ресурсов, требуется максимально корректно выполнить все необходимые процедуры реагирования.

Согласно нормативным документом по менеджменту информационной безопасности реагирование на инциденты должно включать несколько фаз [1-6]. Начальная фаза включает назначение команды реагирования, обучение ее и приобретение необходимых инструментов и ресурсов (описание данной фазы содержится в «Частном регламенте обнаружения и регистрации инцидентов нарушения сетевой безопасности организации при атаках типа «сетевая разведка»). Организации следует предпринимать меры, чтобы снизить риск возникновения инцидентов, но следует учитывать, оставшийся риск неизбежен. Обнаружение инцидентов крайне важно для предотвращения их последствий. Одна из основных задач во второй фазе - ограничить и восстановить нанесенный ущерб (руководство по обнаружение инцидентов приведено в «Частном регламенте реагирования на инциденты нарушения сетевой безопасности организации при атаках типа «сетевая разведка»). После того, как инцидент обработан, корпорация анализирует ущербы инцидента, вырабатывает меры для предотвращения будущих инцидентов (заключительный этап обработки инцидента описан в «Частном

регламенте ликвидации последствий инцидентов нарушения сетевой безопасности организации при атаках типа «сетевая разведка»).

Рис. 1 иллюстрирует схему обработки инцидентов атак типа «сетевая разведка» [7].

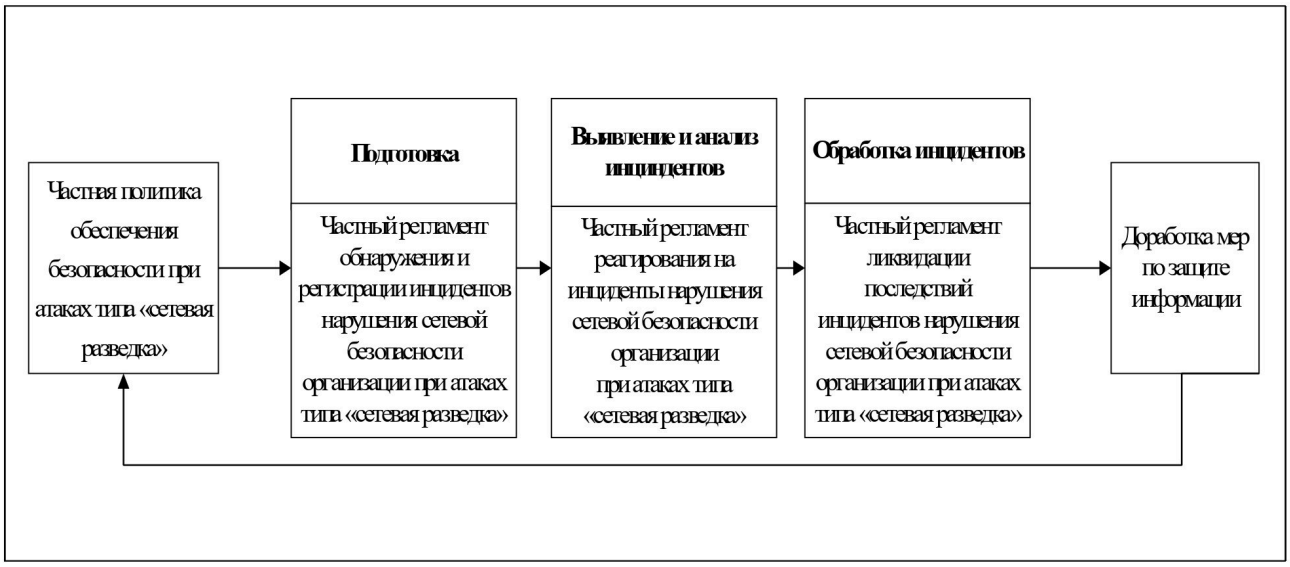

Рис. 1. Схема обработки инцидентов атак типа «сетевая разведка»

Частный регламент обнаружения и регистрации контрразведкой инцидентов нарушения сетевой безопасности. Классификация инцидентов, возникающих в ходе реализации сетевой атаки типа «сетевая разведка»

Согласно [7] инциденты ИБ, связанные со сбором информации, представляют собой действия, направленные на получение представления о возможных целях атаки, об окружающей их сетевой топологии и связанных с ними сервисах. Обычно такие инциденты начинаются с проведения разведки, включающей исследование сетевых устройств для поиска потенциальных объектов защиты. Она предусматривает также сбор информации о том, с кем эти объекты обычно связаны и как обмениваются информацией. Результатом сбора информации может быть выявление уязвимостей в сетевой среде, например, обнаружение открытых портов, уязвимых сервисов, слабых паролей и т.д. Эту информацию можно использовать для дальнейшего внедрения в систему или для последующей атаки. Таким образом, сетевая разведка — это один из этапов проведения кибератак и является важным компонентом общей стратегии злоумышленников по достижению своих целей. В свою очередь, обнаружение инцидентов ИБ, связанных со сбором информации, позволяет принимать меры по защите системы от потенциальных угроз.

Упомянутые типы инцидентов (табл.1) предназначены для расширения имеющейся классификации инцидентов и ориентированы на сетевую разведку. Они предоставляют общую базу для определения более подробных процедур обработки инцидентов.

Таблица 1

Классификация инцидентов, возникающих в ходе реализации сетевой атаки типа «сетевая разведка»

Идентификатор вектора	Категории инцидента	Описание категории инцидента	Критичность инцидента	Приоритет инцидента
VA_1	Инциденты, связанные с записями DNS	Отправка запроса на поиск DNS-записи на определенный IP-адрес приводит к тому, что DNS-записи на компьютере или другом устройстве заменяются на ошибочные данные	2	Средний
VA_2	Большое количество запросов ECHO_REQUEST	Для идентификации узла со стороны нарушителя, атакуемый хост получает большое количество запросов типа ECHO_REQUEST, что приводит к переполнению канала	1	Низкий
VA_3	Инциденты, связанные с отправкой нестандартных сообщений	На сервер поступает большое количество ICMP/UDP сообщений, которые не проверяются на превышение допустимого объема для такого типа данных. Последствия могут быть следующими: сброс соединений или существенное снижение скорости передачи данных через соединение	3	Высокий
VA_4	Использование Снифер-пакетов	Осуществляется перехват и анализ сетевых пакетов, передаваемых по сети. Это может быть выполнено с помощью программного обеспечения, которое слушает и записывает трафик в режиме реального времени. Снифферы могут использоваться для перехвата конфиденциальных данных, таких как логин и пароль от учетной записи, номера кредитных карт и т.п.	2	Средний

Продолжение табл.1

Идентификатор вектора	Категории инцидента	Описание категории инцидента	Критичность инцидента	Приоритет инцидента
Все вектора	Запуск нештатного сканирования сети	Запуск разведывательного ПО (сетевые сканеры), которое представляет собой отдельный исполняемый файл или службу, запущенные через командную строку	4	Критичный
	Обход фильтра (правил)	Использование различных методов обхода ограничений доступа к ресурсам в сети. Обход фильтра может дать злоумышленникам доступ к информации о топологии сети и к установленным правилам безопасности	4	Критичный

Регистрация и подтверждение инцидентов безопасности

Перечень необходимых функций средств защиты информации, предназначенных для обнаружения и регистрации инцидентов, в рамках защиты от атаки типа «сетевая разведка» [8], представлен в табл. 2.

Таблица 2

Необходимые функции средств защиты информации, предназначенных для обнаружения и регистрации инцидентов

Тип инцидента	Функций обнаружения и регистрации инцидента
Инциденты, связанные с записями DNS	Учёт параметров пораженных узлов (IP-адрес и MAC-адрес), а также характеристик связанных событий (IP-адреса, порты и географическое местоположение атакующих и атакуемых узлов).
Большое количество запросов ECHO_REQUEST	Мониторинг производительности пакетов. Поиск аномалий фрагментации пакетов
Инциденты, связанные с отправкой нестандартных сообщений	Сохранение времени начала и конца сессии, количество переданных и полученных байтов.
Атака сниффер-пакетами	Обнаружение связи между узлами, в которых одна из них является узлом-источником, а другой узлом-получателем. Причем события могут быть зарегистрированы при срабатывании разных правил.
Запуск нештатного сканирования сети	Определение категории источников угроз узловых событий (например: логины пользователей, контроль процессов, системная активность).
Обход фильтра (правил)	Контроль целостности набора исполняемых и конфигурационных файлов

В случае подтверждения факта возникновения инцидента безопасности администратор информационной безопасности заполняет карточку инцидента безопасности и принимает решение о его регулировании.

Пример заполненной карточки инцидента безопасности, в которой включена информация об инциденте, произошедшего в ходе реализации атаки типа «сетевая разведка», представлен на рис. 2.

Статус инцидента	В процессе регулирования
Тип инцидента	Выход за нижнюю границу количества ICMP/UDP сообщений
Предполагаемый тип угрозы ИБ	Удаленное вмешательство
Нарушитель	Внешний
Последствия инцидента	Нарушение работоспособности сервера
Объект, которому нанесен ущерб	Сервер
Действия, предпринятые для урегулирования инцидента	Блокирование доступа сервера к сети

Рис. 2. Пример карточки инцидента, произошедшего в ходе реализации атаки типа «сетевая разведка»

Частный регламент реагирования на инциденты нарушения безопасности организации при атаках типа «сетевая разведка»

Данный документ разработан для того, чтобы определить порядок действий корпорации в случае обнаружения инцидента нарушения безопасности при атаках, связанных с сетевой разведкой. После того, как масштаб и серьезность влияния инцидента на штатное функционирование корпорации будут установлены согласно ранее предложенному регламенту, необходимо в первую очередь следовать плану реагирования, который был заранее подготовлен. Таким образом, эксперты по информационной безопасности будут знать, какие действия необходимо предпринять для быстрого устранения инцидента, а заранее подготовленный план позволит значительно сократить время на подготовительных процедурах и быстрее приступить к работе. Важно понимать, что в ряде случаев, особенно при серьезных инцидентах, может потребоваться дополнительное взаимодействие с третьими сторонами, которые окажут дополнительную помощь в расследовании инцидента и устранении возможных проблем.

Меры реализации по реагированию на инциденты безопасности

В табл. 3 сведены первоочередные меры предотвращения инцидентов, связанных с сетевой разведкой.

Таблица 3

Меры реализации по реагированию на инциденты безопасности

Категория инцидента	Последовательность реагирования	Первоочередные меры предотвращения
Большое количество запросов ECHO_REQUEST	6-я	Отключение атакованного устройства от сети
Инциденты, связанные с записями DNS	5-я	Отключение DNS-преобразователей
Инциденты, связанные с отправкой нестандартных сообщений	4-я	Блокирование ICMP-пакетов
Атака сниффер-пакетами	3-я	Отключение служб, которыми может быть определено новое устройство и добавлено в список устройств
Запуск нештатного сканирования сети	2-я	Полнотекстовый поиск адреса злоумышленников на рабочих станциях, в том числе в ветках реестра
Обход фильтра (правил)	1-я	Отключить функцию обмена файлами в локальной сети

Негативные последствия, которые порождает инцидент в ходе реализации атаки типа «сетевая разведка»

Возможные негативные последствия от инцидентов в ходе реализации атаки типа «сетевая разведка» представлены в табл. 4.

Таблица 4

Возможные негативные последствия от инцидентов в ходе реализации сетевой атаки типа «сетевая разведка»

Категория инцидента	Возможные негативные последствия
Инциденты, связанные с записями DNS	Кэширование недействительных DNS-записей, что может привести к перенаправлению пользователей на фишинговые сайты или зловредные ресурсы
Большое количество запросов ECHO_REQUEST	Утечка пакетов сети
Инциденты, связанные с отправкой нестандартных сообщений	Нарушение функционирования сетевых служб, ненормального использования ресурсов системы
Использование сниффер-пакетов	Перехват конфиденциальных данных, таких как логин и пароль от учетной записи

Продолжение табл.4

Категория инцидента	Возможные негативные последствия
Запуск нештатного сканирования сети	Сбои в работе сетевых устройств, продолжительное отсутствие связи
Обход фильтра (правил)	Обход установленного правила доступа к ресурсу, используя другой путь

План мероприятий по противодействию атакам типа «сетевая разведка»

Настоящий план разработан с целью установления общих правил, требований и процедур контроля (анализа) защищенности в корпорации. Меры защиты информации, реализация которых описана в рамках настоящего регламента, представлены в табл. 5.

Таблица 5

Меры реализации по реагированию на инциденты безопасности

№ п/п	Мероприятия по противодействию сетевой атаки	Срок исполнения	Дополнительные мероприятия
1	Сбор, запись и хранение информации о событиях безопасности	В течение 60 мин. после получения информации об инциденте	1. Анализ данных средств, предназначенных для обнаружения и регистрации инцидентов. 2. Установка последовательности реагирования на инциденты для противодействия вероятной атаке
2	Анализ проявившихся уязвимостей	В течение 2 часов с момента регистрации инцидента	1. Поиск уязвимостей, обусловленных ошибками кода. 2. Проверка настройки и средств защиты информации, и корректности работы средств защиты информации (СЗИ).
3	Сотрудниками организации, назначенными ответственными за обеспечение безопасности	В течении суток с момента выявления инцидента	Выполнение плана, сформированного по результатам анализа уязвимостей.

Продолжение табл.5

№ п/п	Мероприятия по противодействию сетевой атаки	Срок исполнения	Дополнительные мероприятия
4	Проверка состава технических средств, программного обеспечения и СЗИ на соответствие действующей эксплуатационной документации	Немедленно	Проверка работоспособности ПО и СЗИ
5	По эксплуатационной документации анализ ПО и СЗИ на корректность их настроек	В течении суток после регистрации инцидента	При необходимости обновление настроек ПО и СЗИ, в том числе с использованием резервных копий и (или) дистрибутивов
6	Блокировка новых протоколов и приложений	Немедленно	Удаление или запрет доступа к ненужному и потенциально уязвимому ПО
7	Отключение неиспользуемых портов	Немедленно	При необходимости использование фильтрации трафика на основе IP-адреса или порта
8	Настройка ПО на конечных точках для фильтрации сетевого трафика	В течении часа с момента получения информации об инциденте безопасности	-
9	Прерывание и проверка сеансов SSL / TLS, чтобы проверить зашифрованный веб-трафик на предмет активности злоумышленников	Немедленно	-

Частный регламент ликвидации последствий инцидентов нарушения сетевой безопасности организации при атаках типа «сетевая разведка»

Сразу после выявления инцидента необходимо принять оперативные меры по устранению его последствий. Следующий этап требует анализа причин и комплекса действий, направленных на предотвращение возможного повторения подобного события. План по ликвидации последствий инцидентов состоит из следующих мероприятий (табл. 6).

Таблица 6

План мероприятий по противодействию атаке типа «сетевая разведка»

Категория инцидента	Возможные негативные последствия	План ликвидации последствий
Инциденты, связанные с записями DNS	Кэширование недействительных DNS-записей, что может привести к перенаправлению пользователей на фишинговые сайты или зловредные ресурсы	1. Ограничение передачи зоны DNS. 2. Отключение рекурсии DNS 3. Запуск собственного DNS-сервера возможен с использованием выделенного сервера или облака 4. Использование DNSSEC. DNSSEC представляет собой набор стандартов, обеспечивающих аутентификацию ответов DNS-серверов с помощью цифровой подписи и системы публичных ключей
Большое количество запросов ECHO_REQUEST	Утечка пакетов сети	1. Замена проблемного оборудования, если расследование привело к неправильной работе устройства. 2. Отключение IPv6 на всех доступных сетевых интерфейсах. Тогда, у всех активных в сети приложений не будет другого выбора, кроме как использование IPv4 протокола. 3. Проверка неправильно подключенных кабелей или портов. 4. Перезапуск маршрутизатора и оборудования. 5. Обновление программного обеспечения на сетевых устройствах
Инциденты, связанные с отправкой нестандартных сообщений	Нарушение функционирования сетевых служб, ненормальное использование ресурсов системы	1. Проверка настройки сетевого оборудования. 2. Анализ трафика в сети с помощью ПО мониторинга сети. 3. Отключение ненужных сервисов и служб.
Применение снифферпакетов	Перехват конфиденциальных данных, таких как логин и пароль от учетной записи	1. Отключение злоумышленника от активной сессии. 2. Удаление сниффера с помощью антивируса.

Продолжение табл.6

Категория инцидента	Возможные негативные последствия	План ликвидации последствий
Запуск нештатного сканирования сети	Сбои в работе сетевых устройств, продолжительное отсутствие связи	1. Обновление правил фильтрации трафика. 2. Просмотреть содержимое пакетов и определить их источники и назначение. 3. Ограничить доступ к сети только для определенных пользователей или групп пользователей.
Обход фильтра (правил)	Обход установленного правила доступа к ресурсам	1. Идентификация уязвимостей обхода правил доступа. 2. Проверка включения СЗИ. 3. Обновление имеющихся правил фильтрации трафика.

Причины и условия возникновения инцидентов безопасности

Для выявления причин и условий возникновения инцидентов безопасности разработана табл. 7, где представлено соотношение инцидентов безопасности с возможными потенциальными факторами их возникновения.

Таблица 7

Причины и условия возникновения инцидентов безопасности

Категория инцидента	Причины и условия возникновения инцидентов безопасности
Инциденты, связанные с записями DNS	Неправильно настроенные серверы и несинхронизированные базы данных
Большое количество запросов ECHO_REQUEST	Нет списка IP-адресов, по которым разрешен/запрещен обмен сообщениями по протоколу ICMP, а также отсутствие фильтрования пакетов ICMP
Инциденты, связанные с отправкой нестандартных сообщений	Использование уязвимостей повышения привилегий, неправильная конфигурация систем, недостаточный контроль доступа к системам и ресурсам
Применение сниффер-пакетов	Открытый доступ к учетной записи системного пользователя.
Запуск нештатного сканирования сети	Большое количество открытых портов
Обход фильтра (правил)	Использование правил средств защиты информации, которые встроены «по умолчанию»

Заключение

Предложенные регламенты носят достаточно обобщённый характер и применимы для корпораций различного профиля деятельности. Степень их формализации позволяет эффективно использовать эти инструменты для широкого многообразия векторов атак типа «сетевая разведка». Адаптация данных регламентов к специфике защищаемых систем может существенно повысить защищённость.

Список литературы

1. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения. URL: https://docs.cntd.ru/document/1200180385 (дата обращения: 12.01.24).

2. ГОСТ Р 59709-2022. Защита информации. Управление компьютерными инцидентами. Термины и определения. URL: https://docs.cntd.ru/document/1200194355 (дата обращения: 12.01.24).

3. ГОСТ Р 59710-2022. Защита информации. Управление компьютерными инцидентами. Общие положения. URL: https://docs.cntd.ru/document/1200194356 (дата обращения: 12.01.24).

4. ГОСТ Р 59711-2022. Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами. URL: https://docs.cntd.ru/document/1200194357 (дата обращения: 12.01.24).

5. ГОСТ Р 59712-2022. Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты. URL: https://docs.cntd.ru/document/1200194358 (дата обращения: 12.01.24).

6. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности URL: https://docs.cntd.ru/document/1200068822. (дата обращения: 12.01.24).

7. ГОСТ Р ИСО/МЭК то 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

8. Комплект документации на ViPNet TIAS. URL: https://infotecs.ru/ (дата обращения: 12.01.24).

Московский государственный университет имени М.В. Ломоносова
Moscow State University named after M.V. Lomonosov

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 07.02.2024

Информация об авторах

Щербакова Дарья Владимировна – аспирант, Московский государственный университет имени М.В. Ломоносова, e-mail: alexanderostapenkoias@gmail.com

Пекло Арина Юрьевна – студентка, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Печкин Дмитрий Сергеевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Питолин Владимир Михайлович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Макаров Олег Юрьевич – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Кострова Вера Николаевна – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

ORGANIZATIONAL AND LEGAL SUPPORT OF NETWORK COUNTERINTELLIGENCE ACTIVITIES OF THE CORPORATION (PART II)

**Shcherbakova, A.Yu. Peklo, D.S. Pechkin,
V.M. Pitolin, O.Yu. Makarov, V.N. Kostrova**

The structure and content of private regulations of network counterintelligence is proposed, where for effective protection it is necessary to ensure the management of incidents of violations of the network security of the corporation in attacks of the type of "network intelligence". The selected types of incidents are designed to expand the existing classification of incidents and are focused on network intelligence. The description of the initial response phase to incidents is contained in the “private regulations for detecting and registering counterintelligence of incidents of the organization’s network security.” The guide for the detection of incidents is given in the "private regulation of counterintelligence response to incidents of the organization’s security." The final stage of the processing of the incident is described in the “private regulation of the elimination of the consequences of impaired network security violations in attacks of the type of “network intelligence”. The action plan is proposed to counteract an attack type “Network intelligence”.

Keywords: private regulations, network intelligence, counterintelligence, incident.

Submitted 07.02.2024

Information about the authors

Daria V. Shcherbakova – graduate student, Moscow State University named after M.V. Lomonosov, e-mail: alexanderostapenkoias@gmail.com.

Arina Yu. Peklo – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com.

Dmitriy S. Pechkin – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com.

Vladimir M. Pitolin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Oleg Yu. Makarov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Vera N. Kostrova – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com