Федеральное государственное бюджетное образовательное учреждение
высшего образования«Московский государственный технический университет
им. Н.Э. Баумана (национальный исследовательский университет)»
Федеральное государственное бюджетное образовательное учреждение
высшего образования«Калужский филиал МГТУ имени Н. Э. Баумана
(национальный исследовательский университет)»

НАУКОЕМКИЕ ТЕХНОЛОГИИ В ПРИБОРО- И МАШИНОСТРОЕНИИ И РАЗВИТИЕ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ВУЗЕ

Материалы
Всероссийской научно-технической конференции

Том 2

ИЗДАТЕЛЬСТВО МГТУ им. Н. Э. Баумана
Калуга 2019

УДК 378:001.891
ББК 74.58:72
Н34

Н34 **Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе**: материалы Всероссийской научно-технической конференции, 19 – 21 ноября 2019 г. Т. 2. – Калуга: Издательство МГТУ им. Н. Э. Баумана, 2019. –233 с.

В сборнике материалов Всероссийской научно-технической конференции представлены результаты научных исследований, выполненных учеными в течение ряда лет. Систематизированы материалы различных научных школ. Результатами научных исследований являются новые методы, вносящие вклад в развитие теории, а также прикладные задачи, воплощенные в конструкции и материалы.

УДК 378:001.891
ББК 74.58:72

СЕКЦИЯ 6.

ЭКОЛОГИЯ И БЕЗОПАСНОСТЬ

В.С. Карасев, М.С. Дятлова, Ю.М. Жукова

АНТРОПОГЕННОЕ ВОЗДЕЙСТВИЕ ПОЛИГОНОВ ЗАХОРОНЕНИЯ ТВЕРДЫХ КОММУНАЛЬНЫХ ОТХОДОВ НА ОКРУЖАЮЩУЮ СРЕДУ

Полигон для захоронения промышленных отходов является природоохранным сооружением и предназначен для захоронения, складирования и длительного хранения отходов производств и потребления. Несмотря на то, что развитие технологий по обработке и переработке твердых коммунальных отходов (далее – ТКО) не стоит на месте, всё же большая их часть продолжает поступать на полигоны. Масса мирового потока бытовых отходов составляет ежегодно около 400 млн. т., из которых 80% уничтожается путем захоронения. Такое количество, без преувеличения, достигает геологических масштабов: с мусором в биосферу попадает около 85 млн. т. органического углерода. В России, на сегодняшний день, накопилось 80 млрд. т. ТКО, ежегодно прибавляется около 50 млн. т. бытового мусора и 120 млн. т. промышленных отходов [1].

На полигоне ТКО концентрируются значительные объемы различных загрязняющих веществ, вследствие этого он является объектом потенциального загрязнения окружающей среды. В процессе эксплуатации полигона ТКО, а также в течение продолжительного времени после его рекультивации происходит эмиссия паров и парниковых газов в атмосферу, образуются фильтрационные сточные воды (далее – фильтрат), а также происходит изменение геопоказателей грунтов под влиянием тепла, выделяющегося в результате процессов «брожения», полигона, что приводит к увеличению фильтрационной способности грунтов и, как следствие, загрязнение самой почвы и грунтовых вод [2]. На небольших и несанкционированных свалках очистка поверхностных стоков и фильтрата не производится. При рекультивации и закрытие полигона все вышеуказанные проблемы остаются, т.к. процессы метаногенеза происходят еще порядка 25 лет после закрытия полигона.

Воздействие полигона на почвы прилегающих территорий выражается в стимулировании развития почвенной микробиоты, увеличении ее численности, биомассы и биоразнообразия, увеличении споровой биомассы в составе грибов, боле активном почвенном дыхании, также в почву попадают различные токсичные химические вещества, что делает ее не пригодной для использования в сельском хозяйстве.

Одним из значительных источников загрязнения водных объектов являются свалки, на которых в результате инфильтрации атмосферных осадков образуются фильтрационные сточные воды. Фильтрат, содержит целый ряд органических и неорганических, токсичных химических соединений, среди которых тяжелые металлы, галогенпроизводные, окисляемые и не окисляемые биологически органические вещества, азот в различных формах, соли и другие вещества, в концентрациях, превышающих в десятки и сотни раз их

установленные предельно-допустимые значения (ПДК) [3]. Образование фильтрата на свалках является основным фактором их негативного воздействия на окружающую природную среду. Проведенные предварительные исследования показали существование потенциальной опасности миграции загрязняющих веществ с фильтратом свалки на протяжении сотен лет [2].

В толще твердых бытовых отходов, складированных на полигонах, под воздействием микрофлоры происходит биотермический анаэробный процесс разложения органических составляющих отходов. В результате этого процесса образуется биогаз, основную объемную массу которого составляют метан и диоксид углерода. Наряду с названными компонентами биогаз содержит пары воды, оксид углерода, оксиды азота, аммиак, углеводороды, сероводород, фенол и в незначительных количествах другие примеси, обладающие вредным для здоровья человека и окружающей среды воздействием. Количественный и качественный состав биогаза зависит от многих факторов, в том числе, от климатических и геологических условий месторасположения полигона, морфологического и химического состава отходов, условий складирования (площадь, объем, глубина захоронения), влажности, плотности и т. д., и подлежит уточнению в каждом конкретном случае [4].

Увеличение содержания метана в атмосфере способствует усилению парникового эффекта, так как метан интенсивно поглощает тепловое излучение Земли в инфракрасной области спектра на длине волны 7,66 мкм. Метан занимает второе место после углекислого газа по эффективности поглощения теплового излучения Земли. Вклад метана в создание парникового эффекта составляет примерно 30% от величины, принятой для углекислого газа. С ростом содержания метана изменяются химические процессы в атмосфере, что может привести к ухудшению экологической ситуации на Земле. Естественно, возникает вопрос об управлении химическими и физическими процессами, в которых принимает участие метан. Если молекулы метана попадают в атмосферу, то они вовлекаются в процессы переноса и вступают в химические реакции, которые хорошо известны как качественно, так и количественно. Управление процессами непосредственно в атмосфере в глобальном масштабе практически исключено.

Состояние окружающей среды является одним из определяющих факторов состояния здоровья населения. Из окружающей среды мы черпаем необходимые нам для нормального функционирования ресурсы – воздух, воду, пищу. Неудовлетворительное качество этих ресурсов может сразу, а может через некоторое время, спровоцировать ухудшение самочувствия, развитие всевозможных заболеваний и как крайнее проявление – даже смерть [5].

Исходя из всего вышеперечисленного можно сделать вывод: полигоны ТКО оказывают огромное влияние на состояние окружающей среды, так как являются потенциально опасными объектами, источниками загрязнений различного типа и характера.

Список литературы

[1]. *Подлипский И.И.* Эколого-геологическая характеристика полигонов бытовых отходов и разработка рекомендаций по рациональному природопользованию: автореф. дис. канд. геол.-минерал. наук: / Подлипский Иван Иванович. СПбГУ, 2014.-С.65-74.

[2]. *Беспалов В.И., Адамян Р.Г.* Анализ условий образования фильтрата на полигонах по захоронению твердых отходов потребления. URL: http://www.rusnauka.com/18_ADEN_2013/Tecnic/13_139660.doc.

[3]. *Горбачева С.М., Жукова Ю.М., Никулина С.Н., Семенова Е.И.* Концепция управления твердыми бытовыми отходами в Калужской области // Всероссийской научно-технической конференции. Калуга: Издательство МГТУ им. Н. Э. Баумана, 2015. – С.60-62.

[4]. *Гонопольский А.М., Миташева Н.И., Николайкина Н.Е., Мурашов В.Е., Кушнир К.Я.* Многостадийная технология очистки фильтрата полигонов твердых 100 бытовых отходов // Вода: химия и экология, №2, 2013г. – С.25-30.

[5]. Р *2.1.10.1920-04* «Руководство по оценке риска для здоровья населения при воздействии химических веществ, загрязняющих окружающую среду».

Карасев Владимир Сергеевич - студент КФ МГТУ им. Н. Э. Баумана. E-mail: v.karasev111@yandex.ru

Дятлова Марина Сергеевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: marina_gorbachev@list.ru

Жукова Юлия Михайловна – канд. техн. наук, КФ МГТУ им. Н.Э. Баумана. E-mail:

С.А. Зубова, О.А. Прокофьева, М.И. Морозенко

ИННОВАЦИОННЫЕ РЕШЕНИЯ ОЧИСТКИ АТМОСФЕРНОГО ВОЗДУХА ОТ ВЫБРОСОВ ЗАГРЯЗНЯЮЩИХ ВЕЩЕСТВ

В настоящее время на химический состав атмосферы существенное влияние оказывает деятельность общества. За последние два столетия технический прогресс ускорился на несколько порядков. Человек создает все новые чужеродные для планеты Земля соединения, которые уже не могут быть обезврежены в атмосфере до безопасных для природной среды и человека концентраций. Крупнейшими источниками загрязнения атмосферного воздуха являются предприятия электроэнергетики и металлургического комплекса. Сейчас общепризнано, что наиболее сильно загрязняет воздух промышленное производство [1].

Вредные вещества, такие как пары, газы, пыль, находящиеся в воздухе производственных помещений, через дыхательные пути, пищевой тракт могут попасть в организм человека и при определенных условиях вызвать острые или хронические отравления, или заболевания. Пыль оказывает вредное действие главным образом на дыхательные пути и легкие человека. При длительном воздействии пыли возможны серьезные поражения всего организма. Пыль, проникая глубоко в легкие, может привести к развитию в них заболевания — пневмокониоза, сущность которого заключается в развитии фиброза, т. е. замещении легочной ткани соединительной тканью.

Чтобы предотвратить возможное развитие различных заболеваний дыхательных путей необходимо применять в производстве и быту специальное газоочистное оборудование. Газоочистка, а также очистка воздуха от пыли выполняется при помощи вентиляционных газо- и пылеулавливающих агрегатов.

В данной работе проведен анализ разработок и установок профессионального воздухоочистного оборудования ООО «Плазкат».

Установки для очистки воздуха **Plazkat** применяются в таких сферах, как крупные промышленные предприятия, в специализированные помещения с большим выделением вредных веществ, а также в бытовые и складские помещения. [2].

Промышленные установки для очистки воздуха Plazkat встраиваются в систему вытяжной вентиляции. Очистка воздуха помещений рециркуляцией при подключении установок Plazkat становится более эффективной.

Оборудование Plazkat — это высокоэффективное оборудование для очистки воздуха (до 95% при любой нагрузке). Установки очищают воздух от запахов, газов, дыма, аэрозолей, пыли, смолы, паров, масел, искр, химических и биологических отходов промышленности и других вредных веществ без образования отходов.

В установке **Plazkat** очистка воздуха происходит за счет физико-химических реакций. В предлагаемых решениях реализовано совместное

действие как плазмохимического, так и каталитического методов воздействия на газообразные вещества-загрязнители. Степень очистки или степень разложения вредных газов была подтверждена многими протоколами замеров эффективности очистки, составленными аккредитованными лабораториями на разных предприятиях России [2,4].

Список удаляемых веществ: ментол, формальдегид, нафталин, углеводороды, метилмеркаптан, диметилсульфид, толуол, сольвенты, скипидар, спирты, бензол, ацетон, ксилол, этанол, кетоны, фенол, уксусная кислота, карбоновые кислоты, бутилацетат, пары масел, сернистый ангидрид, сероводород, азот, монооксид углерода, аммиак, ароматические углеводороды, дымовые газы.

Рассматриваемые современные **установки очистки запаха** могут использоваться не только на производстве, но и в быту. Преимущества систем: они избавляют атмосферу от неприятного аромата и эффективно заботятся об экологии.

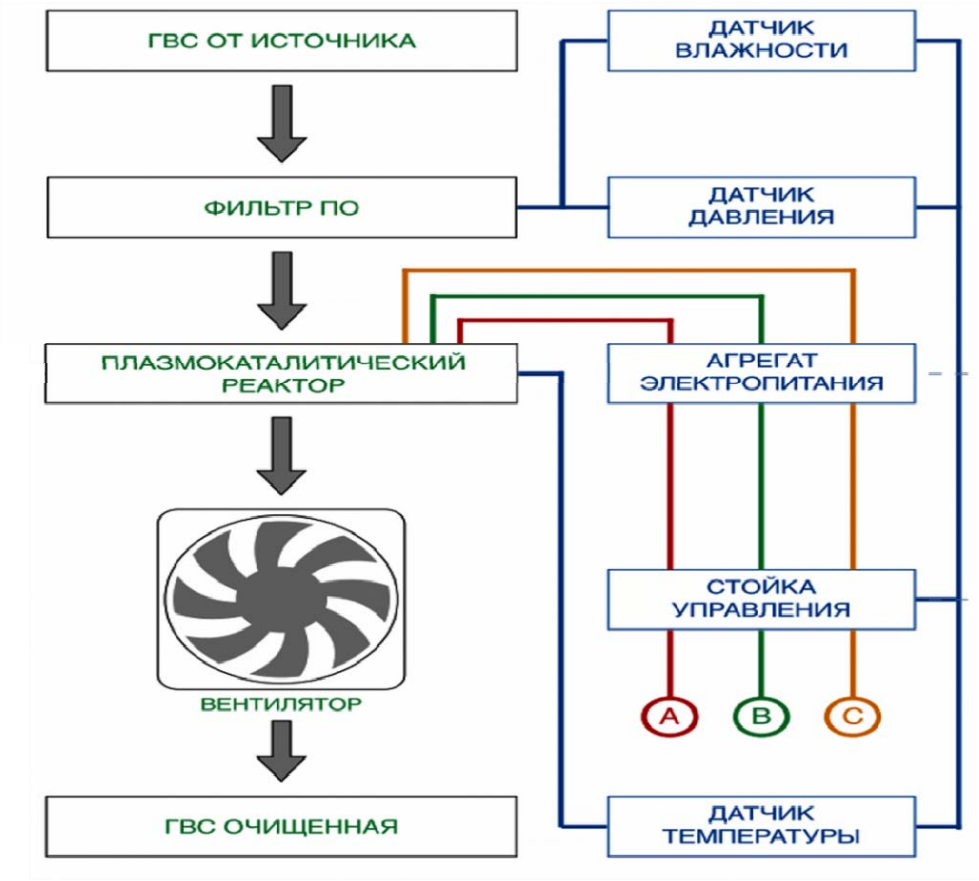


Рис. 1. Технологическая схема установки Plazkat

В установках ООО «Плазкат» используется запатентованная технология плазмо-каталитической очистки воздуха.

Вредные вещества, попадая на плазменный модуль установки, подвергаются бомбардировке активным кислородом и озоном, начинают переходить в активную форму, далее на наноструктурной поверхности катализатора, активный кислород и озон, вступают в гетерогенную реакцию разрушения образовавшихся радикалов, что приводит к образованию простейших

веществ, таких как вода, кислород, углерод. Технологическая схема установки Plazkat изображена на рис. 1.

Классификация продукции, выпускаемой ООО «Плазкат»:

1) Plazkat-standart.

Данная установка предназначена для очистки выбросов органических соединений различных видов, образующихся при различных технологических процессах (ароматические углеводороды, карбоновые кислоты, альдегиды, кетоны и т.д.). Установка эффективна для широкого диапазона данных веществ.

Эффективность очистки составляет **85-95%**. Области применения: очистные сооружения, литье пластмасс, покрасочные камеры, пропитка материалов, пищевое производство, шпалопропиточное производство, производство полимерных волокон, производство полимерных изделий методом экструзии и пултрузии, термопластавтоматы.

2) Plazkat-oxiz

Система Plazkat-oxiz применяется для удаления запахов различного состава и концентраций, для сильно запыленных выбросов аэрозолей, туманов и паров.

Система мобильная, может применяться на разных точках выброса. Легко монтируется в существующую вентиляционную систему. Эффективность очистки составляет 7**5-95%**. Области применения: кафе, рестораны, склады хранения реагентов, машины для производства кормов, канализационно-насосные станции, производственные помещения птицефабрик, силосные сооружения.

3) Plazkat-special

Plazkat-special - Высокопроизводительная модель с увеличенным количеством катализатора (в 2,5 раза), применяется при длительном выбросе (24х7) и/или высоких концентрациях Данная система используется для очистки воздуха производств от паров, сильных запахов, токсичных газов и аэрозолей. Эффективность очистки составляет **85-99%**. Области применения: литье в форму, полиэфирные и нановолокна, битумоварение, асфальтобетонные заводы, печи обжига, производство пищевых добавок и ароматизаторов, производство лекарственных препаратов, ёмкости хранения химических реактивов, ёмкости хранения горюче-смазочных материалов,

4) Plazkat-aqua.

Специфический запах воды является свидетельством наличия в жидкости тех или иных солей и микроорганизмов. Дополнительные примеси могут не только ухудшать качество воды, но и делать ее опасной для использования. Для удаления вредных микроорганизмов, химических элементов используется специальный **фильтр воды от запаха**. Оборудование Plazkat-aqua может использоваться как в быту, так и на производстве, в различных очистительных системах. Данная система применяется для очистки стоков электрохимическими методами. Для этого используется плазменно-каталитическое окисление под воздействием низкотемпературной газораз-

рядной плазмы с образованием активных реагентов и катализаторов. После того, как загрязненная вода поступает в установку через патрубок, она попадает в систему форсунок, и разбрызгивается на плазменные кассеты, которые выделяют необходимое количество озона O_3 и свободных радикалов, для окисления Fe^{2+} в Fe^{3+}, а лишний озон удаляется из системы вытяжным вентилятором, подготовленная вода поступает на пластины коагулятора, где осаждается железо, которое потом отстаивается и удаляется через патрубок. Выбор модели очистителя необходимо делать с учетом места установки, объема нагрузки, специфики примесей, дающих неприятный и опасный запах. Механизм работы различных видов очистительного оборудования для воды основывается на обеззараживании воды, улавливании молекул посторонних примесей. Эффективно действует с данной целью обратноосмотическая система, также активно применяются и адсорбционные фильтры с активированным углем. Для того, чтобы фильтрация и очистка от запахов имела отличный результат, нужно точно определить источник запаха. Следует учесть, что на интенсивность запаха может влиять температура жидкости. При правильном выборе очистного оборудования вода не только избавляется от запаха, но и становится абсолютно безопасной в использовании [3].

Продукция **Plazkat**, для очистки воздуха, применяется на: асфальтобетонных заводах, производствах химических веществ, при лазерной резке, при литье в форму, при литье пластмасс, нефтеперевалочных пунктах, свалках, полигонах, печах обжига, в покрасочных камерах, производствах ароматизаторов, при пропитке материалов, сварочных постах, складах дурнопахнущих материалов, станциях одорации газов, станциях технического обслуживания, при экструзии пластиков.

Увеличение производственных мощностей, потребовало воплощения новых идей при разработке и усовершенствовании газоочистных сооружений. В настоящее время разработаны и широко используются в эксплуатации установки очистки газов нового поколения.

Таким образом, разработанные сегодня новые технологии газоочистного оборудования не только снижают нагрузку на окружающую среду, но и решают вопросы рационального использования природных ресурсов. Правильно организованное пылеулавливание решает проблему экологии, обеспечивая нормативные показатели [1].

Список литературы

[1]. *Романова С. М., Степанова С.В,. Ярошевский А.Б., Шайхиев И.Г.* Экология // Министерство образования и науки РФ, Казанский национальный исследовательский технологический университет. —: КНИТУ, 2017. – С.94 – 100.

[2]. *Проектирование* и производство систем удаления запахов и очистки воздуха [Электронный ресурс] URL: http://plazkat.ru/_(дата обращения 19.10.2019)

[3]. *Сотникова Е.В., Дмитренко В.П., Сотников В.С.* Теоретические основы процессов защиты среды обитания // учеб. пособие. – СПб.: Лань, 2014.-С.576. [Электронный ресурс] http:e.lanbook.com/view/book/53691/

[4]. *Капустин В.И., Коржавый А.П.* Физико-химические методы экологического мониторинга. Кн.1. Назначение, схемы, конструкции // Изд-во МГТУ им. Н.Э. Баумана, 2014. - С.208.

Зубова София Александровна - студентка КФ МГТУ им. Н.Э. Баумана. E-mail: 2105sofi@mail.ru

Прокофьева Ольга Андреевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: prokofevaolya2016@yandex.ru

Морозенко Мария Ивановна - канд. техн. наук, доцент кафедры ИУ7-КФ «Экология и промышленная безопасность» КФ МГТУ им. Н.Э. Баумана.

Я.М. Литвинова, В.В. Коренец, С.Н. Никулина

ОСНОВНЫЕ ИСТОЧНИКИ ЗАГРЯЗНЕНИЯ ПОВЕРХНОСТНЫХ ВОД

Основными источниками загрязнения поверхностных вод является недостаточно очищенные сточные воды промышленных и коммунальных предприятий, отходы производства при разработке рудных ископаемых, рудников, сбросы водного и железнодорожного транспорта. Загрязняющие вещества, попадая в водоемы, приводят к значительному ухудшению качества вода, которое в основном проявляются в изменении физических свойств воды. Изменение химического состава воды, в частности, появление в ней вредных веществ, в наличии плавающих веществ на поверхности воды и откладывании их на дне водоемов [1].

Загрязнение поверхностных вод можно распределить на несколько типов:

1. Механическое - механическое загрязнение характеризуется попаданием в воду песка, шлама, ила и др. Механические примеси могут значительно ухудшать органолептические показатели и качество вод, а также отрицательно влияют на условия обитания рыб и состояние экосистем. Тепловое загрязнение связано с повышением температуры воды в результате смешивания с более нагретыми поверхностными или технологическими водами, в результате чего происходит изменение газового и химического состава воды, размножение анаэробных бактерий, рост количества гидробионтов и выделение ядовитых газов (сероводорода и метана).

2. Химическое - химическое загрязнение представляет собой изменение естественных химических свойств вода за счет увеличения содержания в ней вредных примесей как неорганической, так и органической природы (нефть и нефтепродукты, органические остатки, пестициды).

3. Бактериальное и биологическое - сточные воды содержат большое число микроорганизмов, в том числе болезнетворных (патогенных) бактерий, что делает эту воду опасной в санитарном отношении. В бытовых сточных водах встречаются бактерии брюшного тифа, дизентерии и другие возбудители желудочно-кишечных заболеваний, а также яйца гельминтов (глистов), поступающие в сточные воды с выделениями людей и животных.

4. Радиоактивное - радиоактивные вещества, попадающие в поверхностные и подземные воды, могут быть природного и искусственного происхождения. Наличие в воде природных радиоактивных веществ обусловлено соприкосновением ее с минералами, содержащими радиоактивные изотопы, а также взаимодействием с атмосферой, из которой в воду попадают. Степень радиоактивного загрязнения воды в этом случае обычно невелика.

5. Тепловое - тип физического (чаще антропогенного) загрязнения окружающей среды, характеризующийся увеличением температуры выше естественного уровня. Основные источники теплового загрязнения - выбросы в

атмосферу нагретых отработанных газов и воздуха, сброс в водоемы нагретых сточных вод.

Производственные сточные воды загрязнены в основном отходами и выбросами производства. Количественный и качественный состав их разнообразен и зависит от отрасли промышленности, ее технологических процессов. Их делят на две основные группы: содержащие неорганические примеси, токсические, и содержащие яды [2].

К первой группе относятся сточные воды содовых, сульфатных, азотно-туковых заводов, обогатительных фабрик свинцовых, цинковых, никелевых руд, в которых содержатся кислоты, щелочи, ионы тяжелых металлов и др. Сточные воды этой группы в основном изменяют физические свойства воды.

Сточные воды второй группы сбрасывают нефтеперерабатывающие, нефтехимические заводы, предприятия органического синтеза, коксохимические и др. В стоках содержатся разные нефтепродукты, аммиак, альдегиды, смолы, фенолы и другие вредные вещества. Вредоносное действие сточных вод этой группы заключается главным образом в окислительных процессах, вследствие которых уменьшается содержание в воде кислорода, увеличивается биохимическая потребность в нем, ухудшаются органолептические показатели воды.

Экологические проблемы, загрязнение воды приводят к распространению самых тяжелых заболеваний. Именно с этой жидкостью в организм могут попасть различные возбудители и патогенные организмы, уносящие сотни тысяч жизней.

Самые распространенные заболевания, которые приносит грязная вода - холера; тиф; лямблиоз; энтеровирус; амебиаз; шистосомоз; психические аномалии; гастрит; врожденные уродства; ожоги слизистых; онкология; нарушения репродуктивных функций. Независимо от причин загрязнения воды, профилактикой будет являться использование фильтрованной, бутилированной воды.

Рациональное потребление воды, охрана от загрязнений — главные задачи человечества. Пути решения экологических проблем по загрязнению вод ведут к тому, что прежде всего большое внимание следует уделять сбросам опасных веществ в реки. В промышленных масштабах необходимо усовершенствовать технологии по очистке сточных вод. В России необходимо ввести закон, который бы повышал взимание платы за сбросы. Вырученные средства должны направляться на разработку и сооружение новых экологических технологий [3].

За наименьшие выбросы плату нужно снижать, это будет служить мотивацией к сохранению здоровой экологической обстановки. Большую роль в решении экологических проблем играет воспитание подрастающего поколения. С ранних лет необходимо приучать детей к уважению, любви к природе. Внушать им, что Земля — наш большой дом, за порядок в котором ответственен каждый человек. Воду необходимо беречь, не лить ее бездумно, ста-

раться, чтобы в канализацию не попадали посторонние предметы и вредные вещества.

Список литературы

[1]. *Савичев О.Г.* Биологическая очистка сточных вод // Известия ТПУ. 2008. №1. URL: https://cyberleninka.ru/article/n/biologicheskaya-ochistka-stochnyh-vod-s-ispolzovaniem-bolotnyh-biogeotsenozov (дата обращения: 05.10.2019).

[2]. *Понкратова С.А., Емельянов В.М., Сироткин А.С., Шулаев М.В.* Математическое моделирование и управление качеством очистки сточных вод // Вестник Казанского технологического университета. 2010. №6. URL: https://cyberleninka.ru/article/n/matematicheskoe-modelirovanie-i-upravlenie-kachestvom-ochistki-stochnyh-vod (дата обращения 05.10.2019).

[3]. *Моисеева Е.* Проблемы очистки сточных вод // ГИАБ. 2010. №12. URL: https://cyberleninka.ru/article/n/problemy-ochistki-stochnyh-vod (дата обращения: 05.10.2019).

Литвинова Яна Михайловна - студентка КФ МГТУ им. Н.Э. Баумана. E-mail: yana.litvinova.1998@inbox.ru

Коренец Владлена Владиславовна - студентка КФ МГТУ им. Н.Э. Баумана. E-mail: yana.litvinova.1998@inbox.ru

Никулина Светлана Николаевна - канд. техн. наук, зам. зав. каф. по учебной работе ИУ7-КФ «Экология и промышленная безопасность» КФ МГТУ им. Н.Э. Баумана.

Т.С. Моторова, Е.Э. Комарова, О.В. Яковлева

ВОЗМОЖНОСТИ РАЦИОНАЛЬНОГО ВОДОПОЛЬЗОВАНИЯ В РАЙОНАХ С НЕДОСТАТОЧНЫМ ВОДООБЕСПЕЧЕНИЕМ

В современном мире одной из важнейших проблем природопользования является обеспечение населения водой высокого качества. Запасы и качество водных ресурсов определяются региональными условиями и особенностями круговорота воды, зависят от характера хозяйственной деятельности человека. Исходя из объективных реалий сегодняшнего дня и заглядывая в будущее, можно однозначно утверждать, что рациональное водопользование должно быть ориентировано, прежде всего, на необходимость полного воспроизводства водных ресурсов территории, как по количеству, так и качеству. Решение проблем водопользования актуально на сегодняшний день [1].

Переход к рациональному использованию водных ресурсов предусматривает совершенствование организационно – экономического механизма водопользования с целью уменьшения негативных эколого-экономических последствий. Он является важным для многих стран мира, где большие территории не имеют источников пресной воды или количество их сильно ограничено, это касается и Российской Федерации [2].

Цель данного исследования являлось выявление направления организации водообеспечения в районах, испытывающих водный дефицит, на основании передового опыта организации рационального водопользования.

Проведенное аналитическое исследование показало, что передовые страны, где имеются проблемы с обеспечением населения питьевой водой и где они успешно решаются, применяют комплекс мероприятий по рациональному водопользованию.

Так Израиль практически полностью решил проблему обеспечения населения безопасной и чистой питьевой водой. Самым действенным решением этой задачи стало использование доступного природного ресурса – морской воды, и внедрение передовых технологий по ее опреснению. Кроме этого в стране используются обширные запасы подземных грунтовых вод, которые достаточно соленые. Для их использования **применяются новейшие технологии опреснения и очистки** [1].

Сингапур, не имеющий собственных природных источников пресной воды, решает данную проблему комплексно. Используются накопительные емкости для воды, подвергаются очистке и опреснению воды океана, закупается питьевая вода и, наконец, очищают сточные воды, используя высокие технологии до питьевого качества. Полученная вода применяется в основном в технологических процессах, ее бутилируют для продажи населению [1].

Страны Средиземноморья решают проблемы водопользования, обращая внимание на минимизацию сбросов сточных вод в водоемы используя замкнутые циклы очистки воды с последующим ее использованием в производственных процессах и для нужд сельского хозяйства.

В Республике Казахстан для решения проблемы водообеспечения используют различные технологии водоподготовки минерализованной воды Каспийского моря. Так, в г. Актау используются опреснительные установки, применяются технологии обработки морской воды из Каспийского моря с использованием фильтрационной очистки воды с предварительной коагуляцией и флокуляцией, а также с обратноосмотическим опреснением и физико – химической корректировкой состава пресной воды [1].

Несмотря на богатые водные ресурсы России проблемы с обеспечением водой высокого питьевого качества имеются у населения обширных районов и территорий нашего государства. Одним из таких регионов, где проблема обеспечения водой населения стоит особенно остро, является Крым. Необходима продуманная система управления водным хозяйством региона, обеспечивающая такую конкуренцию на рынке водных ресурсов, которая бы служила рационализации их использования [2].

Полуостров стабильно испытывает нехватку питьевой воды. Для решения проблем требуется разработка мер по предотвращению загрязнения водных источников, сохранению их минерального состава, обеспечению высокого качества очистки сбрасываемых в водоемы сточных вод.

Проведенный анализ показал, что назрела необходимость повсеместного решения данных проблем для жителей Крыма.

Так организация современной водохозяйственной системы на территории Большой Феодосии отражает сложные взаимодействия между водными ресурсами, формирование которых обусловлено природными и антропогенными факторами, и потребностями в воде, определяемыми экономическими, экологическими и социальными факторами.

На территории Феодосии водоснабжение осуществляется из двух поверхностных и двух подземных источников [3].

Феодосийское водохранилище является основным источником хозяйственно – питьевого водоснабжения. Расчетный срок службы водохранилища, из условий заиливания, составляет 50 лет. За 40 лет эксплуатации произошло значительное заиливание южной части водохранилища, полностью заилен подводящий канал [4]. Три весенних месяца вода на водоочистные сооружения поступает с мутностью до 150 мг/л. Повышается содержание органических веществ, водохранилище постоянно зарастает зеленью, а при заполненном объеме происходит интенсивное ее гниение.

Фронтовое водохранилище – заилен подводящий канал. Водовод находится в аварийном состоянии.

Также для водоснабжения используются субашские источники.

Соотношение между местными водными ресурсами и фактическими потребностями в них населения и отдельных отраслей хозяйства не совпадают. Большая Феодосия – вододефицитный регион. Доля феодосийского, фронтового водохранилищ и субашских источников в балансе водоснабжения района Большая Феодосия составляет соответственно 64, 32 и 4 % [3]. Ранее покрытие дефицита в пресной воде обеспечивалось за счет подачи днепровской

воды по каналу и наполнением наливных водохранилищ. Водообеспечение в настоящее время не удовлетворяет потребностям Большой Феодосии.

Водопроводные очистные сооружения построены в 1978 году, имеют традиционную схему водоподготовки.

Очистка сточных вод осуществляется на двух очистных станциях по традиционным технологиям (механическая, биологическая очистка).

Для решения водных проблем Большой Феодосии видится необходимость комплексного подхода, это в первую очередь восстановление и использование уже имеющихся двух поверхностных и двух подземных источников [4].

С другой стороны для решения проблемы дефицита воды перспективно использование для водоснабжения воды Черного моря. Использование морской воды может быть альтернативой существующей системы водообеспечения для отдельных отраслей. Мировой опыт и опыт, имеющийся в нашей стране опреснения морской воды, может быть полезен.

Опреснение воды – это совокупность способов и технологий её обработки, позволяющая добиться понижения концентрации растворённых солей до величины менее 1 г/дм3, в результате чего вода становится пригодной для удовлетворения технических и хозяйственных нужд. Выбор метода и технологии опреснения воды зависит от предъявляемых к воде требований по качеству и солесодержанию, а также технико-экономических показателей [5].

Применение мембранных технологий позволяет довести водные показатели до необходимых требований и, при использовании предварительной очистки воды, а также в дальнейшем при доведении ее до требуемой кондиции – соответствия питьевому качеству.

Организация рационального водопользования включает также возможность повторного использования очищенных сточных вод. На действующих очистных станциях применяются традиционные методы и схемы очистки. Очищенные воды сбрасываются в водоем. Решение вопроса сокращения объемов сброса видится в организации систем их доочистки на очистных станциях с дальнейшим использованием.

Проведение третичной очистки дает возможность использования этой воды для нужд технического водоснабжения определенных производств, а также в сельском хозяйстве для полива сельскохозяйственных культур.

Создание оборотных систем водоснабжения позволит улучшить экологическое состояние данного района, уменьшить объемы забора свежей воды и сброса сточных вод.

Предлагаемый на перспективу комплексный подход в решении проблемы водообеспечения в Большой Феодосии актуален для всего полуострова, испытывающего водный дефицит.

Список литературы

[1]. *Маслова Л.Ф.* ГЛОБАЛЬНЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ СОХРАНЕНИЯ ПИТЬЕВЫХ РЕСУРСОВ / Л.Ф. Маслова // Вестник АПК Ставрополья. — 2015. — № 3. — С. 180-183. — ISSN 2222-9345. — Текст:

электронный // Электронно-библиотечная система «Лань»: [сайт]. — URL: https://e.lanbook.com/journal/issue/303698 (дата обращения: 28.09.2019). — Режим доступа: для авториз. пользователей.

[2]. *Ляшевский В.И.* К проблеме опреснения морской воды в Крыму / В.И. Ляшевский, А.М. Джапарова // Таврический вестник аграрной науки. — 2015. — № 1. — С. 63-68. — ISSN 2542-0720. — Текст: электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/journal/issue/309699 (дата обращения: 16.10.2019). — Режим доступа: для авториз. пользователей.

[3]. *Соцкова Л.М.* ВОДНЫЕ РЕСУРСЫ И ПРОБЛЕМЫ ВОДОХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ НА ТЕРРИТОРИИ БОЛЬШОЙ ФЕОДОСИИ / Л.М. Соцкова, В.О. Яшенков, Е.В. Локтева // Ученые записки Крымского федерального университета имени В.И Вернадского. География. Геология. — 2011. — № 1. — С. 247-257. — ISSN 2413-1717. — Текст: электронный // Электронно-библиотечная система «Лань»: [сайт]. — URL: https://e.lanbook.com/journal/issue/299799 (дата обращения: 16.10.2019). — Режим доступа: для авториз. пользователей.

[4]. *Позаченюк Е.А.* Водохозяйственный комплекс территории Большая Феодосия, как основа устойчивого развития региона / Е.А. Позаченюк, М.Ю. Лукьянова // Геополитика и экогеодинамика регионов. — 2013. — № 2-1. — С. 148-159. — ISSN 2309-7663. — Текст: электронный // Электронно-библиотечная система «Лань»: [сайт]. — URL: https://e.lanbook.com/journal/issue/299958 (дата обращения: 28.09.2019). — Режим доступа: для авториз. пользователей.

[5]. *Смирнов В.А.* ПРОБЛЕМЫ ПОЛУЧЕНИЯ ПИТЬЕВОЙ ВОДЫ И ПУТИ ИХ РЕШЕНИЯ / В.А. Смирнов, Н.М. Попов // Труды Костромской государственной сельскохозяйственной академии. — 2018. — № 88. — С. 130-138. — Текст: электронный // Электронно-библиотечная система «Лань»: [сайт]. — URL: https://e.lanbook.com/journal/issue/309170 (дата обращения: 28.10.2019). — Режим доступа: для авториз. пользователей.

Моторова Татьяна Сергеевна - студент КФ МГТУ им. Н.Э. Баумана. Кафедра: ИУ7-КФ «Экология и промышленная безопасность». E-mail: motorova2013@yandex.ru

Комарова Елена Эдуардовна - студент КФ МГТУ им. Н.Э. Баумана. Кафедра: ИУ7-КФ «экология и промышленная безопасность». E-mail: elena2261998@mail.ru

Яковлева Ольга Владимировна - канд. техн. наук, КФ МГТУ им. Н.Э. Баумана.

К.В. Бочарова, М.Е. Сафронова, С.А. Кусачева

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ ВОЗМОЖНОСТИ МИКРОБИОЛОГИЧЕСКОЙ УТИЛИЗАЦИИ БИОПОЛИМЕРОВ И НЕФТЕПРОДУКТОВ

В настоящее время имеет огромную актуальность проблема повреждения зданий, сооружений, строительных материалов, вызванная заселением и развитием микроорганизмов: бактерий, грибов, актиномицетов, так как они могут наносить серьезный вред конструкциям зданий и сооружений.

Эта проблема широко известна как биокоррозия. Биокоррозия – разрушение конструкционных материалов под действием микроорганизмов и продуктов их метаболизма. Чаще всего на материалах это проявляется в виде изменения окраски или появления грибковых пятен. В России уровень биокоррозии существенно превышает нормы, принятые в Европе и в мире: многие строительные материалы (бетон, штукатурка, кирпич, герметики, сухие смеси и прочее) могут даже в условиях средних широт, особенно при температуре выше 20ºС и относительной влажности выше 70%, подвергаться воздействию различных микроорганизмов, что приводит к серьезному биоповреждению строительных материалов [1].

Немалую проблему представляют собой отходы полимерных материалов, загрязненные нефтепродуктами. К ним относятся фильтровальные материалы, емкости, нетканая ветошь.

Нефтепродукты, образующиеся в процессе переработки и использования нефти, вредны для окружающей среды. Серьезной проблемой является несоблюдение норм безопасности при добыче и транспортировке нефти [2].

Объем отходов нефтепродуктов, попадающих в окружающую среду, во множество раз превышает тот, с которым природа способна справиться самостоятельно. Поэтому правильная и простая утилизация и переработка данного вида жидкостей, их повторное использование – весьма актуальная проблема.

Из перечня известных методов оценки воздействия микроорганизмов на материалы можно выделить следующие:

1. Методы оценки физико-технических параметров;
2. Биохимические и микробиологические методы;
3. Инфракрасная и электронная микроскопия;
4. Спектрофотометрические методы;
5. Хроматографические, электромагнитные и электрохимические методы.

Методы групп № 2, 5 не подходят для использования в условиях имеющегося лабораторного оборудования. Метод №1 нельзя использовать для испытаний твердых материалов. Для подтверждения факта биологического воздействия на полимерные материалы наиболее подходящими представляются способы групп №3, 4. В условиях природного микробиоценоза наблю-

дается одновременная ассимиляция разных фракций нефти различными группами микроорганизмов [3]. Таким образом, использование биоценоза активного ила, отличающегося разнообразием состава, может оказаться эффективным способом решения проблемы.

При этом биохимический метод требует использования большого количества специализированных реактивов. Микробиологический метод больше подходит для применения в условиях имеющейся микробиологической лаборатории. Он основан на определении степени биообрастания материалов после погружения их в модельную среду. Представленные методы предполагают необходимость использования специализированных культур микроорганизмов для оценки биостойкости образцов. С целью повышения доступности и применимости предложен способ оптимизации методик использованием биоценоза активного ила сооружений биологической очистки в качестве модельной среды. Это позволяет применять методики без дополнительных затрат на поиск и заказ культур грибов и бактерий. Кроме того, данный состав модельной среды позволит изучить биологическое воздействие на полимерные материалы в условиях, максимально приближенных к реальным. Основа для нанесения исследуемых полимерных материалов представляет собой цементно-песчаный раствор, моделирующий мелкозернистый бетон. Образцы строительных материалов были изготовлены размером 160х35х35 мм. Исследуемые полимерные составы были выбраны как базовые варианты защитных покрытий:

- низковязкая эпоксидная смола на основе ЭД-20;
- силикат натрия («жидкое стекло»).

Для исследования физико-технических параметров провели контроль за весом исследуемых образцов до и после выдержки в модельной среде.

В результате данной работы подобран и отработан оптимальный способ тестирования полимерных материалов на устойчивость к биологическому воздействию и выполнено обоснование использования активного ила сооружений биологической очистки для совместной утилизации полимерных материалов и нефтепродуктов.

Список литературы

[1]. *Карпенко Н.И.* Проблема биоповреждений и биозащиты строительных материалов, изделий и сооружений / Н.И. Карпенко, В.Г. Ерофеев, В.Ф. Смирнов, Е.А. Морозов, А.Д. Богатов // Материалы международной научно-технической конференции «Биоповреждения и биокоррозия в строительстве». – Саранск: Изд-во Мордовского университета.- 2004 - С. 6-11.

[2]. *Ерофеев В.Т.* Микробиологическое разрушение материалов. / В.Т. Ерофеев, В.Ф. Смирнов, Е.А. Морозов.- М.: Высшая школа, 2011.- 124 с.

[3]. *Ассоциация* штаммов бактерий-нефтедеструкторов и способ ремедиации нефтезагрязненных объектов: пат. №2509150 Российская Федерация. № 2012116827/10 / Ильичева Т.Н., Мокеева А.В., Шестопалов

А.М., Емельянова Е.К., Алексеев А.Ю., Забелин В.А. ; заявл. 24.04.2012 ; опубл. 10.03.2014 ; Бюл. №7.- 13 с.

Бочарова Ксения Владимировна – эколог ООО «Агроторг», г. Москва, E-mail: bocharova.kv@gmail.com,

Сафронова Мария Евгеньевна – студентка КФ МГТУ им. Н.Э. Баумана. e-mail: svetlaya.dom@mail.ru,

Кусачева Светлана Александровна – доцент, канд. биол. наук КФ МГТУ им. Н.Э. Баумана. e-mail: Safronova2@mail.ru

СЕКЦИЯ 7.

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАЗЕМНЫХ ТРАНСПОРТНО – ТЕХНОЛОГИЧЕСКИХ СИСТЕМАХ И КОМПЛЕКСАХ. ПРИКЛАДНЫЕ ПРОБЛЕМЫ МЕХАНИКИ

Зар Ни Лин, К.В. Чижевский, В.Н. Сидоров, В.М. Алакин

АНАЛИЗ МЕЖДУНАРОДНЫХ ЕЗДОВЫХ ЦИКЛОВ АВТОМОБИЛЯ

В разных странах применяются различные методы контроля токсичности и дымности отработанных газов (ОГ). Они отличаются программами испытаний, моделирующих режимы работы двигателя, а также применяемой измерительной аппаратурой и методиками отбора проб. При оценке токсичности ОГ используют два принципиально разных метода исследований: испытание на установившихся режимах с постоянными параметрами двигателя и испытания на переходных режимах при изменении указанных параметров.

Режимы работы автомобильных моторов весьма разнообразны и зависят от характера эксплуатации транспортного средства. На основании статистических исследований установлено, что в условиях уличного движения в городах Европы время работы на разных режимах составляют: на холостом ходу при средних частотах вращения 35%, на режимах с постоянными частотами вращения с нагрузкой 29%, с ускорением 22%, с замедлением 14%. Каждый из перечисленных режимов характеризуется различиями процентного содержания токсичных компонентов в ОГ. Для определения показателей токсичности ОГ двигатели испытывают на переходных режимах - по так называемым ездовым циклам.

Европейский ездовой цикл. В Европейских странах для оценки токсичности ОГ серийных легковых и легких грузовых автомобилей полной массой до 3,5 т применяют ездовой цикл NEDC (New European Driving Cycle) (рис.1) [3]. Этот цикл продолжительностью 1220 с состоит из двух частей. Первая часть цикла - городской ездовой цикл UDC (Urban Driving Cycle) с максимальной скоростью движения 50 км/ч включает четыре последовательных ездовых цикла и имитирует условия движения автомобиля по городу [1]. Вторая часть цикла - скоростной загородный цикл EUDC (Extra Urban Driving Cycle) с максимальной скоростью движения 120 км/ч имитирует условия движения автомобиля по магистрали [1]. В ездовом цикле NEDC автомобиль испытывается на беговых барабанах после запуска холодного двигателя и его прогрева на холостом ходу в течение 40 с. В процессе испытаний все выхлопные газы собираются в мешки по методу CVS. Массовые доли вредных веществ, которые определены при анализе выхлопных газов, собранные в мешок в процессе всего цикла испытаний, относят к пройденному пути [1]. Определенные таким образом удельные массовые выбросы токсичных компонентов (в г/км) сравниваются с предельно допустимыми нормами. Начиная со стандарта EURO-3 (2000 г.) вместо ездового цикла NEDC используется модифицированный ездовой цикл MNEDC (Modified New European Driving Cycle), в котором отменена предварительная работа двигателя в течение 40 с до начала измерения ОГ. При этом холодный пуск включен в программу тес-

та. Испытуемое транспортное средство предварительно должно быть выдержано при температуре -7 градусов минимум 6 часов.

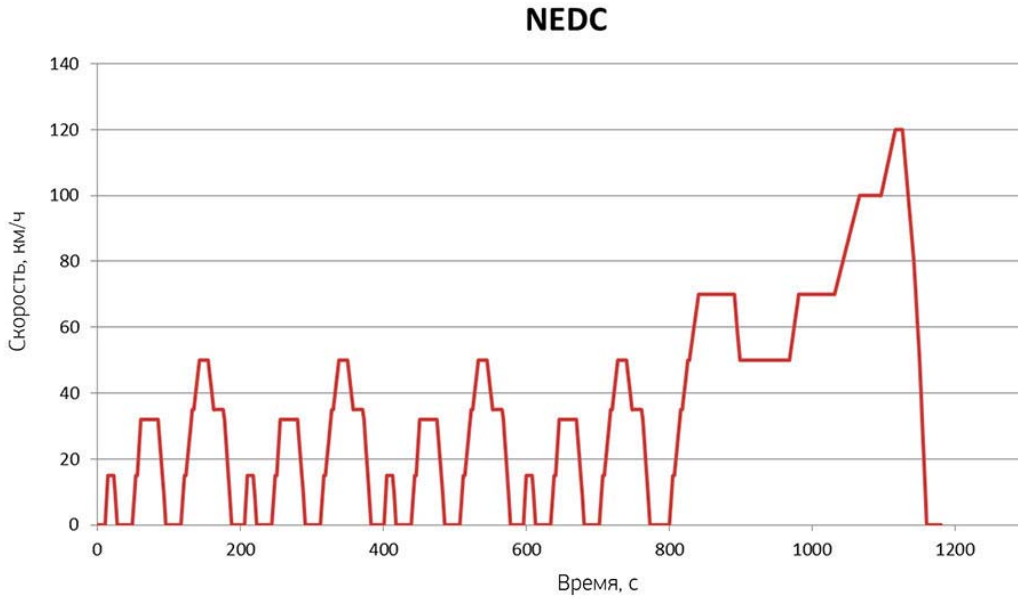


Рис. 1. Европейский ездовой цикл

В последнее время для испытаний легковых автомобилей на токсичность применяют модернизированный ездовой цикл. Этот цикл включает четыре набора городских режимов и дополнительный набор режимов EUDC, имитирующий движение автомобиля по городу. При этом общее время выполнения цикла составляет 1220 с (с учетом начальных 40 с работы двигателя в режиме холостого хода), длина условного пути движения автомобиля - 11 км, средняя скорость движения - 33,6 км/ч, максимальная скорость движения - 120 км/ч или, для автомобиля с двигателем небольшой мощности, - 90 км/час [1].

Европейский городской ездовой цикл полностью воспроизводит эксплуатационные условия: работа двигателя автомобиля в режиме минимальной частоты вращения активного холостого хода (имитация ожидания зеленого света светофора на перекрестке), трогание автомобиля с места и разгон до определенной скорости, движение с установившейся скоростью на определенном участке, переключение передач с низшей на высшую или в обратном порядке, разгон автомобиля от одной скорости к другой, торможение двигателем с одной скорости к другой или к полной остановке, служебное торможение до полной остановки с использованием рабочей тормозной системы.

Японский ездовой цикл. В Японии испытания автомобилей с количеством пассажиров менее 10 и массой менее 2,5 т проводятся по двум ездовым циклам (рис.2) [3]: холодные испытания по 11 режимному циклу без предварительного прогрева двигателя, и с предварительным прогревом двигателя по 10-15 режимному циклу. Каждая фаза цикла длится 120 с, что соответствует дистанции 1021 м, средняя скорость движения составляет 30,6 км/час. Длина 10-15 режимного цикла - 4,16 км, время выполнения - 660 с, макси-

мальная скорость движения - 70 км/ч, средняя скорость движения - 22,7 км/час.

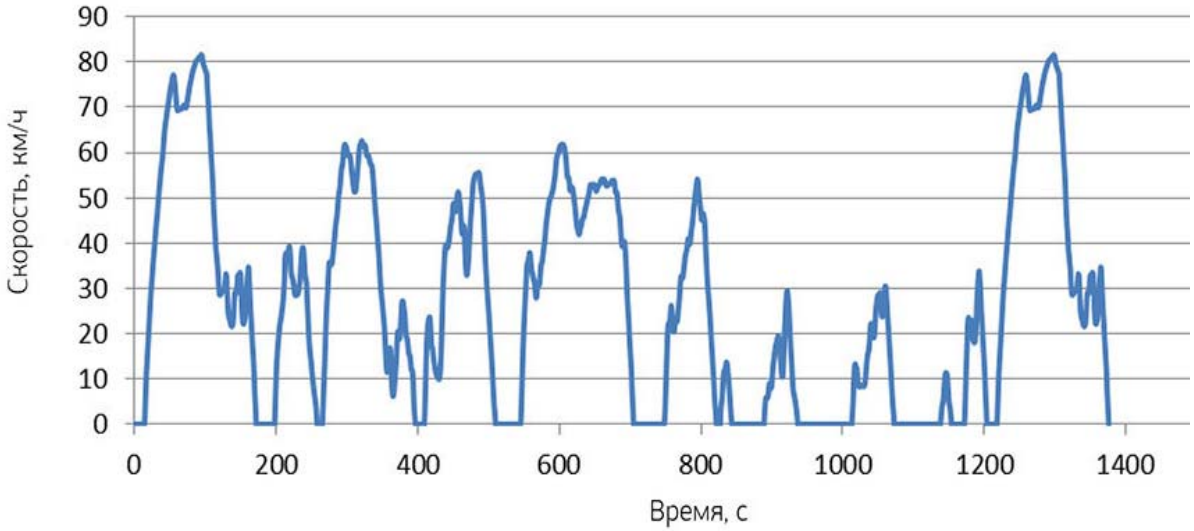


Рис. 2. Японский ездовой цикл

Тестовый 10-15 режимный цикл продолжительностью 660 с, имитирующий характерные условия движения транспорта в Токио, проводится один раз с пуском прогретого двигателя [2]. Причем, первые три цикла теста с максимальной скоростью движения 40 км/ч имеют 10 режимов, а последний цикл с максимальной скоростью движения 70 км/ч - 15 режимов [3]. Тест предполагает предварительное термотестирование на режиме холостого хода, которое проходит по следующей схеме: после 15 минут движения автомобиля со скоростью 60 км/ч в выпускном тракте двигателя измеряются концентрации углеводородов, окиси углерода и углекислого газа. После дальнейшего движения в течение 5 мин со скоростью 60 км/ч начинается 10-15 режимный тест. Анализ содержания токсичных компонентов в ОГ выполняется по методу CVS [2]: разбавленные отфильтрованным окружающим воздухом выхлопные газы собираются в один мешок. Массовые доли вредных веществ, содержащихся в собранных выхлопных газах, относят к пройденному пути, т.е. перечисляются в г/км.

Американский ездовой цикл. Более сложный ездовой цикл для испытаний легковых автомобилей используется в США. В нем практически нет установившихся режимов движения. Длина условного пути в таком цикле - 17,8 км, время его выполнения - 1877 с, максимальная скорость движения - 91,2 км/ч, средняя скорость движения - 34,1 км/час [2]. Согласно законодательству США производители автомобилей должны обеспечить расход топлива не выше 8,55 л на 100 км для легковых автомобилей и не более 11,6 л на 100 км для легких грузовых автомобилей. Указанный расход топлива измеряется при работе двигателя в испытательном ездовом цикле FTP 75 [3] (Federal Test Procedure - 55% времени) (рис.3) и тестовом цикле Highway (45% времени). Производители транспортных средств, не соответствующих этим нор-

мам, платят штраф государству, а покупатель облагается дополнительным налогом.

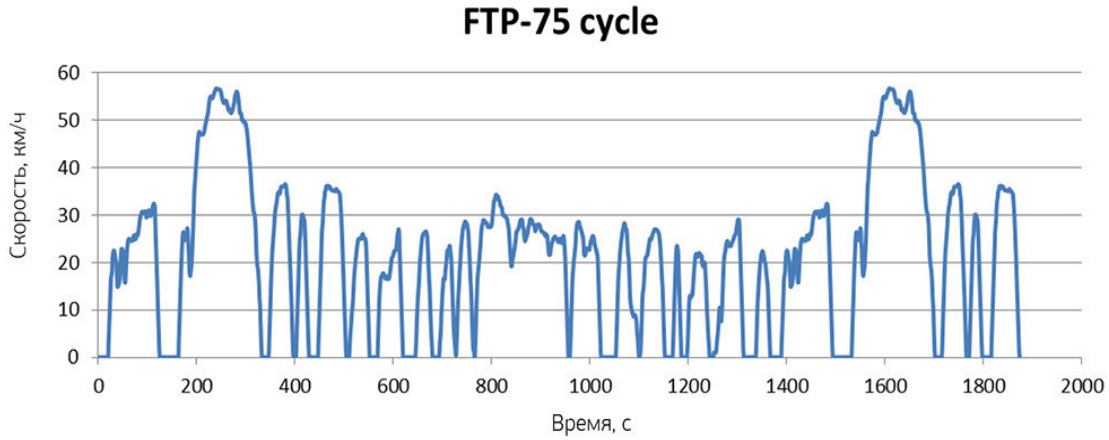


Рис. 3. Американский ездовой цикл

WLTP (WLTC) цикл. WLTC ездовой цикл (рис.4) [2] является всемирной процедурой выставления оценки экологической и топливной эффективности, применяющейся ко всем транспортным средствам вне зависимости от вида силового агрегата.

Основное отличие новой методики заключается в том, что замеры производятся не только в идеальных лабораторных условиях, недостижимых на практике, но и на реальных дорогах с учётом особенностей вождения.

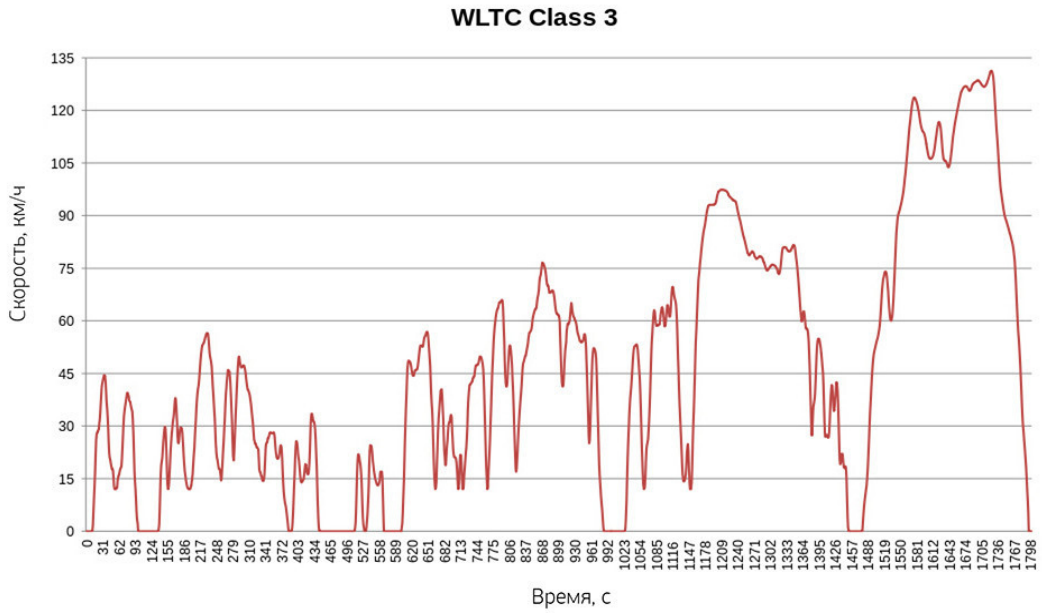


Рис. 4. WLTC ездовой цикл

Цикл WLTP на сегодняшний день является наиболее объективным, поскольку учитывает сведения, собранные по всему миру [2].

При проведении испытаний используется понятие скоростной характеристики и учитываются разные фазы вождения (торможение, ускорение, остановка, разгон и пр.) [2].

Проведение замеров происходит в течение 30 минут и на расстоянии 23,25 км.

Для расчётов применяется сложная и совершенная математическая модель, дающая возможность добиться результатов высокой точности. Для определения WLTP в городском цикле замеры делаются на скорости 56,5 км/ч и 76,6 км/ч, при движении по трассы - 97,4 км/ч и 131,3 км/ч [3].

В целом измерительный цикл WLTP имеет много нерешенных вопросов. Однако главная цель WLTP – приведение всех тестовых испытаний по расходу топлива и запасу хода к единому стандарту, что позволит сравнивать автомобили напрямую, без оговорок об измерительном тесте, в ходе которого будут получены определенные цифры.

Анализ международных ездовых циклов автомобиля позволяет сделать следующие выводы.

Современные ездовые циклы, первоначально разрабатывающиеся для оценки экологических характеристик автомобилей, не в полной мере отражают специфику движения современных транспортных средств в реальных условиях эксплуатации.

Европейский ездовой цикл имеет отдельные участки, на которых изменение скорости и ускорения описано линейными законами, чего нельзя сказать про остальные ездовые циклы. Плавные переходы между этими участками отсутствуют. Они соединяются под определенными углами, что в реальности невозможно. Американский, японский и WLTP циклы являются продолжительными и более сложными, по сравнению с европейским циклом.

Для дальнейших исследований был принят европейский ездовой цикл, так как, в отличие от других, позволяет полностью воспроизвести эксплуатационные условия управления автомобилем.

Список литературы

[1]. *Гусаков С.В.* Испытательный цикл NEDC и его соответствие современным условиям эксплуатации автомобилей с бензиновыми ДВС / С.В. Гусаков, В.А. Марков, Д.В. Михрячев // Автомобильная промышленность. – 2012. - №9. – С. 47-51.

[2]. *Антипов С.И.* Современные испытательные ездовые циклы и их актуальность при создании алгоритма работы системы управления автомобиля с КЭУ / С.И. Антипов, Ю.В. Дементьев // Наземные транспортные системы. – 2013. - №10. – С. 8-11.

[3]. *Златин П.А.* Электромобили и гибридные автомобили. – М.: Агроконсалт, 2004. – 416 с.

Зар Ни Лиин - аспирант КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: zarni.znl15@gmail.com

Чижевский Константин Владимирович - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: konstantin201997@yandex.ru

Сидоров Владимир Николаевич - заведующий кафедрой, доктор техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: sidorov-kaluga@yandex.ru

Алакин Виктор Михайлович - заместитель директора по инновациям, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: alakin@bmstu-kaluga.ru

М.А. Карпов, Н.Г. Сысенко, А.Г. Черенков, С.А. Голубина

АНАЛИЗ СОВРЕМЕННЫХ ПОДВЕСОК АВТОМОБИЛЕЙ

Подвеска автомобиля – система деталей, узлов и механизмов, соединяющих кузов автомобиля с дорогой. Современные автомобильные подвески являются достаточно сложными конструкциями, сочетающими механические, гидравлические, пневматические и электрические элементы, имеют электронные системы управления, обладают высокой комфортабельностью, управляемостью и безопасностью.

Существует большое число автомобильных подвесок, обеспечивающих надежную работу автомобиля в течении его эксплуатации. Наибольшее распространение в современном автомобилестроении получили такие типы подвесок: McPherson, двухрычажная, многорычажная, адаптивная, задняя зависимая, полузависимая, независимая.

Подвеска McPherson. Согласно литературным источникам [1-4] данный тип получил наибольшее распространение. Применяется на передней оси автомобиля. По своей конструкции подвеска МакФерсон является развитием подвески на двойных поперечных рычагах, в которой верхний поперечный рычаг заменен на амортизаторную стойку. Благодаря компактности конструкции подвеска McPherson широко используется на переднеприводных легковых автомобилях, так как позволяет поперечно разместить двигатель и коробку передач в подкапотном пространстве [4]. Вместе с тем, конструктивные особенности подвески приводят к значительному изменению развала колес. По этой причине данный тип подвески не применяется на спортивных автомобилях и автомобилях премиум-класса.

Двухрычажная подвеска. Двухрычажная подвеска может применяться на передней и задней оси автомобиля. Подвеска используется в качестве передней подвески на многих спортивных автомобилях, седанах представительского и бизнес класса, а также на болидах формулы один. Производиться и применяется на автоконцерне «Ford». Преимущества двухрычажной подвески – лучшая шумоизоляция и передача меньшей части нагрузок на кузов, относительная легкость ремонта. Недостатки: стоимость проектирования и обслуживания такой подвески выше, чем у Макферсона, настройка двухрычажной подвески – довольно сложная геометрическая задача. Дополнительные сложности возникают с применением двойных поперечных рычагов в задней подвеске [2].

Многорычажная подвеска. Многорычажная подвеска или по другом Multilink, является на сегодня самой распространенной среди тех, которые применяются на задней оси автомобиля. В меру прогресса, такой вид можно встретить на передней или задней оси машины, соответственно, как на переднеприводные, так и на заднеприводные. Такой тип подвески начали применять в атомобилях «Jaguar E-type» 1964г., затем на некоторых моделях «Audi». Преимуществом многорычажной подвески является держание угла

развала схождения колес, в момент работы многорычажная подвеска удерживает колесо в вертикальном положении при любой перегрузке, независимо от положения кузова. Плавность хода автомобиля, бесшумность работы всего механизма.

Адаптивная подвеска. Адаптивная подвеска бывает пневматической и гидравлической. В основе конструкции пневмоподвески лежат пневматический упругий элемент, установленный под каждым колесом [3]. Жидкостная адаптивная подвеска различается по принципу регулировки жесткости. Это может быть осуществлено с помощью электромагнитного клапана или применением специальной магнитно-реологической жидкости. Подобную подвеску выпускают: «General Motors – MagneRide» для автомобилей «Cadillac», «Chevrolet». Преимуществами адаптивной подвески являются: высокий уровень комфорта независимо от типа дорожного покрытия, особенно это применимо к пневмоподвескам. Хорошая управляемость на больших скоростях и в крутых виражах. Уменьшение нагрузки на несущие элементы кузова, снижение износа шин, уменьшение тормозного пути. Недостатки адаптивной подвески являются сложность её устройства и цена. Сложность электронной начинки может приводить к сбоям в работе. Надежность адаптивной подвески будет ниже, чем у традиционной.

Задняя зависимая схема подвески. Зависимая подвеска представляет собой единую жесткую ось, которая соединяет правое и левое колеса [2]. Обычно балка соединяется с корпусом автомобиля с помощью двух упругих элементов. Такая конструкция проста, при этом она обеспечивает надежное соединение. Когда одна сторона машины наезжает на неровность, то наклоняется весь автомобиль. Такой тип подвесков применялся в автомобилях «Жигули». Однако недостатки зависимой подвески на этом не заканчиваются. Кроме зависимости колес друг от друга, распространение такой подвески в современных легковых автомобилях было сведено к нулю из-за больших неподрессоренных масс, а также необходимости сильно поднимать пол автомобиля для обеспечения полноценной артикуляции подвески, особенно в случае с ведущим мостом.

Полузависимая подвеска. Полунезависимая подвеска состоит из двух продольных рычагов, которые соединяются между собой с помощью поперечной балки, то есть вся конструкция имеет вид буквы «П» [2]. Преимуществами являются легкость монтажа, высокий уровень жесткости в поперечном направлении, возможность изменения характеристик подвески при помощи геометрии поперечного сечения, компактные размеры и небольшой вес, низкая себестоимость. Недостатками данного типа является возможность установки только на заднем, не ведущем мосту и наличие отдельных требований к геометрии днища кузова.

Независимая подвеска. В независимой подвеске колеса одной оси не связаны друг с другом, и изменение положения одного колеса не оказывает влияния на другое. Такой вид подвески устанавливался на задние мосты автомобилей марок «Citroen», «Austin», а также на мотороллеры и небольшие

прицепы. Одним из основных преимуществ независимой является именно то, что при наезде одного колеса на неровность другое не меняет своего положения. Эта независимость работы подвесок на разных сторонах оси обеспечивает равномерное сцепление с поверхностью при прохождении неровностей. Недостатком данного типа является то, что параметры положения колеса (развал, схождение и ширина колеи) могут меняться при работе подвески, а также стоимость.

Таблица 1.

Характеристики подвесок

Подвеска	**Простота конструкции**	**Компактность**	**Управляемость**	**Дешево**
McPherson	Да	Да	Нет	Да
Двухрычажная	Да	Нет	Нет	Нет
Многорычажная	Нет	Нет	Да	Нет
Адаптивная	Нет	Нет	Да	Нет
Зависимая	Да	Нет	Нет	Да
Полузависимая	Да	Да	Нет	Да
Независимая	Нет	Нет	Да	Нет

Таким образом, исходя из проведенного анализа, можно сделать вывод, что в зависимости от области использования наиболее целесообразно использовать современные виды подвесок типа McPherson, полузависимой или независимой. Модернизацией существующих типов подвесок можно добиться уменьшения занимаемой подвеской подкапотного либо багажного пространства. Помимо всего перечисленного, автомобильная подвеска должна обладать приемлемой ценой, а также легко подвергаться ремонту и замене составляющих элементов.

Список литературы

[1]. *Алакин В.М.* Методы моделирования рабочих процессов передней подвески полноприводного автомобиля //Актуальные проблемы гуманитарных и естественных наук, 2016. – № 7-5. – С. 5-12.

[2]. *Буйкус К.В., Тихонович А.М.* Устройство автомобилей: учеб. пособие // Минск: РИПО, 2017. – 303 с.

[3]. *Извозчикова В.В., Хлынин И.А.* Модернизация легкового автомобиля пневматической подвеской // Новая наука: Проблемы и перспективы, 2017. – Т. 2. – № 3. – С. 133-137.

[4]. *Шинкоренко Е.А., Садковский Б.П., Пономарев А.И.* Исследование подвески типа Макферсон // Актуальные проблемы гуманитарных и естественных наук, 2015. – № 10-5. – С. 220-222.

Карпов Максим Алексеевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: karpovmaksim.ru@mail.ru

Сысенко Никита Григорьевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: nikita.sisenko@gmail.com

Черенков Александр Григорьевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: al.cherenckov2013@yandex.ru

Голубина Светлана Александровна - канд. техн. наук, старший преподаватель КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: asbina@yandex.ru.

И.А. Зенкина, Д.А. Мамышев

ВЫЧИСЛЕНИЕ УРАВНЕНИЯ ТРАЕКТОРИИ ДВИЖЕНИЯ ЗЕМЛИ

Рассматривается задача о нахождении уравнения траектории Земли вокруг Солнца.

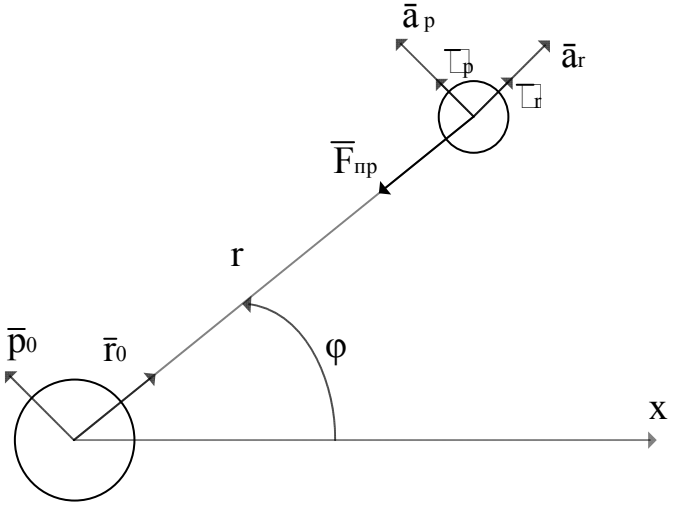


Рис. 1. Движение Земли вокруг Солнца

Запишем дифференциальное уравнение движения Земли вокруг Солнца под действием силы притяжения:

$$m\vec{a} = \vec{F}_{np},$$

где $F_{np} = K\dfrac{Mm}{r^2}$ – сила притяжения.

Составим уравнения движения Земли в полярной системе координат с центром в центре массы Солнца.

$$\begin{cases} m(\ddot{r} - r(\dot{\varphi})^2) = -K\dfrac{Mm}{r^2} \\ m(2\dot{r}\dot{\varphi} + r\ddot{\varphi}) = 0 \end{cases}, \qquad (1)$$

В качестве начальных условий примем следующие:
при

$$t = 0 \;\; \varphi = 0; \;\; \dot{\varphi} = \frac{v}{b}; \;\; r = b; \;\; \dot{r} = 0. \qquad (2)$$

Можно заметить, что

$$2\dot{r}\dot{\varphi} + 2\ddot{\varphi} = \frac{1}{r}\frac{d(r^2\dot{\varphi})}{dt}. \qquad (3)$$

Тогда из второго уравнения системы (1) с учетом (3) и начальных условий (2) получаем

$$\dot{\varphi} = \frac{vb}{r^2}. \qquad (4)$$

С учетом полученного выражения (4) первое уравнение системы (1) примет вид

$$\ddot{r} - \frac{v^2 b^2}{r^3} = -K\frac{M}{r^2}. \qquad (5)$$

Интегрируем его, используя начальные условия (2), и получаем выражение для производной радиальной координаты по времени

$$\dot{r} = \frac{1}{rb}\sqrt{2KMrb^2 - v^2b^4 + r^2(v^2b^2 - 2KMb)}. \qquad (6)$$

Для того, чтобы избавиться от времени, разделим выражение (6) на равенство (4) и получим следующее соотношение:

$$\frac{dr}{d\varphi} = \frac{r\sqrt{2KMrb^2 - v^2b^4 + r^2(v^2b^2 - 2KMb)}}{vb^2}. \qquad (7)$$

Задача сводится к решению дифференциального уравнения

$$\frac{dr}{r\sqrt{2KMrb^2 - v^2b^4 + r^2(v^2b^2 - 2KMb)}} = \frac{d\varphi}{vb^2}, \qquad (8)$$

которое решается с помощью замены переменной $r = \frac{1}{z}$.

Произведя интегрирование и подставив начальные условия, получаем уравнение

$$r = b\sqrt{\frac{v}{KM - (v^2b - KM)\cos(\varphi)}}. \qquad (9)$$

Это и есть уравнение траектории движения Земли вокруг Солнца.

Список литературы

[1]. *Пономарев К.К.* Составление дифференциальных уравнений. – Минск: «Вышэйшая школа», 1973. – 560 с.

Зенкина Ирина Александровна - доцент кафедры «Колесные машины и прикладная механика», канд. физ.-мат. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: nizenkin@yandex.ru

Мамышев Дмитрий Андреевич - студент КФ МГТУ им. Н. Э. Баумана. E-mail: mamysheff2013@yandex.ru

В.Н. Винокуров

КРАЕВАЯ ЗАДАЧА ДЛЯ ПОДПЯТНИКА С ГАЗОВОЙ СМАЗКОЙ

На рис. 1 схематично представлен подпятник с газовой смазкой. Газ под давлением $p_н$ подводится к нижней поверхности пористого дросселя и, пройдя сквозь его поры, попадает в рабочий зазор высотой h. Из рабочего зазора газ вытекает в окружающую среду с давлением p_0.

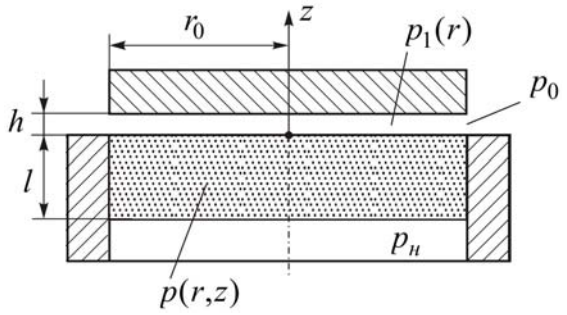


Рис. 1. Газовый подпятник с пористым дросселем

В изотропном дросселе, при условии изотермического процесса и наличии симметрии относительно осевой координаты, давление газа в цилиндрических координатах , φ, z подчиняется уравнению [1]

$$\frac{\partial}{\partial r}\left(r\frac{\partial p^2}{\partial r}\right)+\frac{\partial}{\partial z}\left(r\frac{\partial p^2}{\partial z}\right)=0. \qquad (1)$$

Ведём безразмерные переменные по правилу: $R=r/r_0$ – безразмерная радиальная координата; $P=p/p_0$ – безразмерное давление в дросселе; $U=P^2$ – квадрат безразмерного давления; $P_н=p_н/p_0$ – безразмерное давление наддува; $Z=z/l$ – безразмерная осевая координата в дросселе. Тогда уравнение (1) можно записать в виде

$$\frac{1}{R}\frac{\partial U}{\partial R}+\frac{\partial^2 U}{\partial R^2}+\frac{r_0^2}{l^2}\frac{\partial^2 U}{\partial Z^2}=0. \qquad (2)$$

Сформулируем граничные условия для уравнения (2).

На поверхности наддува давление известно:

$$U\big|_{Z=-1}=P_н^2. \qquad (3)$$

Радиальные скорости v_r частиц газа равны нулю при $r=0$ из условия симметрии относительно оси z, а при $r=r_0$ – из условия непроницаемости боковой стенки подпятника. Но, согласно закону Дарси [2],

$$v_r=-\frac{\sigma}{\mu}\frac{\partial p}{\partial r},$$

где σ – коэффициент проницаемости пористого материала, а μ – динамический коэффициент вязкости газа. Следовательно,

$$\left.\frac{\partial U}{\partial R}\right|_{R=0} = \left.\frac{\partial U}{\partial R}\right|_{R=1} = 0. \qquad (4)$$

Ещё одно граничное условие получается согласованием расходов газа протекающего через дроссель и рабочий зазор. Если в рабочем зазоре выделить элементарный параллелепипед, то по закону сохранения массы газа в нём можно получить уравнение

$$\frac{1}{r}\frac{\partial p_1^2}{\partial r} + \frac{\partial^2 p_1^2}{\partial r^2} - \left.\frac{12\sigma}{h^3}\frac{\partial p^2}{\partial z}\right|_{z=0} = 0, \qquad (5)$$

где через p_1 обозначено давление в рабочем зазоре.

Последнее уравнение получено при условии отсутствии скольжения частиц газа на пористой стенке дросселя, обращенной к рабочему зазору, что является предметом для дискуссий.

В безразмерных переменных уравнение (5) приводится к виду

$$\frac{1}{R}\frac{\partial U_1}{\partial R} + \frac{\partial^2 U_1}{\partial R^2} - \Lambda\left.\frac{\partial U}{\partial Z}\right|_{Z=0} = 0, \qquad 6)$$

где $\Lambda = 12\sigma r_0^2 \Big/ \left(h^3 l\right)$ – безразмерный параметр подпятника.

Так как давление в тонком смазочном газовом слое полагается постоянным по толщине слоя, и равным давлению на поверхности пористого дросселя, обращённой к рабочему зазору, $U_1 = U\big|_{Z=0}$, то уравнение (6) может быть представлено, также, в виде

$$\left.\left(\frac{1}{R}\frac{\partial U}{\partial R}\right)\right|_{Z=0} + \left.\frac{\partial^2 U}{\partial R^2}\right|_{Z=0} - \Lambda\left.\frac{\partial U}{\partial Z}\right|_{Z=0} = 0, \qquad 7)$$

по которому оно может быть истолковано как одно из граничных условий уравнения (2).

На выходе из рабочего зазора квадрат безразмерного давления газа равен единице:

$$U\big|_{Z=0,R=1} = 1. \qquad (8)$$

Уравнение (2) совместно с условиями (3), (4), (7), (8) составляют краевую задачу для симметричного подпятника с изотропным пористым дросселем.

Список литературы

[1]. *Винокуров В.Н., Емельянов А.В.* Теория течения газа в анизотропных пористых дросселях подшипников с газовой смазкой // Проблемы машиностроения и надёжности машин. – 2012. – №2. – С. 57–60.

[2]. *Коллинз Р.* Течения жидкостей через пористые материалы. М.: Мир, 1964. – 350 с.

Винокуров Виктор Николаевич - доцент, канд. физ.-мат. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: bbn01@mail.ru

Тинт Наинг Вин, В.М. Алакин

ОБОСНОВАНИЕ ЧАСТНОЙ МЕТОДИКИ ОПРЕДЕЛЕНИЯ ЦЕНТРА ТЯЖЕСТИ АВТОМОБИЛЯ

Исследование управляемости и дорожной устойчивости автомобиля обычно начинают с распределения масс и расчета координат центра тяжести снаряженного и груженого автомобиля по его длине и высоте. Поэтому на первом этапе был выполнен обзор методов расчета координат центра тяжести автомобиля и рассмотрена возможность применения основных вариантов для частного варианта исследования сил инерции и определения нагрузки на неподрессоренную часть автомобиля**.** В результате обзора методов установлено, что на этапе проектирования автомобиля обычно применяют классическую расчетно – графическую методику определения центра тяжести. Она заключается в выборе массы агрегатов, нагрузки и в определении их геометрического расположения относительно координат автомобиля в виде расстояния центров агрегатов от края автомобиля. Учитывая эти параметры, нахождение центра тяжести выполняется по формуле[1]:

Определение центра тяжести автомобиля полной массы:

$$L_{ЦМ_{полной.массы}} = \frac{\sum L_{агрегатов}.m_{агрегатов}}{m_{полной.массы}}. \quad (1)$$

Определение центра тяжести автомобиля снаряженной массы:

$$L_{ЦМ_{снар.массы}} = \frac{\sum L_{агрегатов}.m_{агрегатов}}{m_{снар.массы}}, \quad (2)$$

где $L_{агрегатов}$ – расстояние от опорной точки до агрегата.

$$X_{ЦМ_{снар.массы}} = \frac{\sum X_{агрегатов}.m_{агрегатов}}{m_{снар.массы}}, \quad (3)$$

$$Y_{ЦМ_{снар.массы}} = \frac{\sum Y_{агрегатов}.m_{агрегатов}}{m_{снар.массы}}, \quad (4)$$

где: $X_{агрегатов}$ и $X_{агрегатов}$ – расстояние от опорной точки до агрегата, по оси X и Y.

При выполнении исследований по модернизации серийных автомобилей применяют расчетно-лабораторные методы определения центра тяжести. Расчетный метод для конкретной модели автомобиля заключается в выборе распределения нагрузки на передний и задний мост снаряженного и груженого автомобиля, а также общее размеры конструкции и колесной базы.

В этом случае продольные координаты центра тяжести для порожнего и груженого автомобиля определяют по формуле [2]:

Для порожнего автомобиля:

$$a = L \cdot \frac{G_2}{G_0}, b = L - a, \quad (5)$$

где G_0 – Собственная масса машины, G_2 – нагрузка на заднюю ось, L– База машины.

Для груженого автомобиля:

$$a = L \cdot \frac{G_2}{G_a}, b = L - a, \quad (6)$$

где G_a – полная масса машины, G_2 – нагрузка на заднюю ось, L– База машины.

Высоту центра тяжести принимаем на основании габаритной схемы порожнего автомобиля

$$h = 0,4H, \quad (7)$$

Для груженого автомобиля с учетом размещения пассажиров в салоне и груза в багажнике:

$$h = 0,5H, \quad (8)$$

где Н – высота автомобиля.

Лабораторный метод выполняется в следующем порядке [3]:

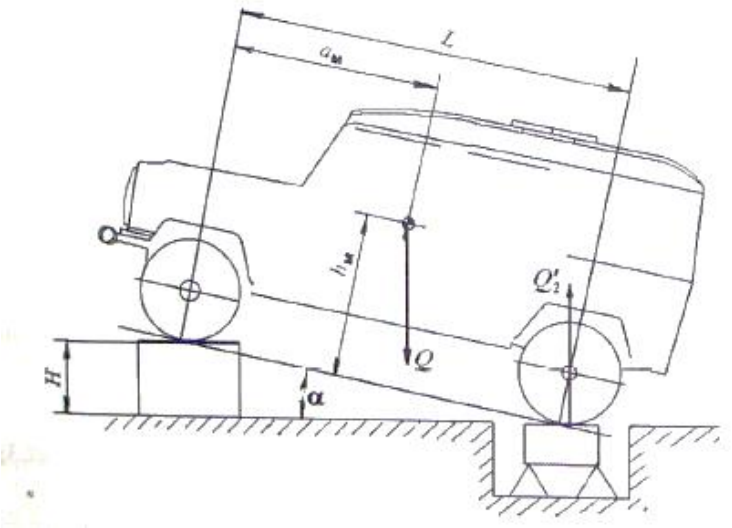


Рис. 1. Схема определение высоты центра масс с помощью весов

1.Массу автомобиля Q определяют после установки на платформу весов.

2.Определение массы, создающей нагрузку на колеса левого и правого бортов колесной машины, проводят в следующем порядке:

— устанавливают на платформе весов все колеса левого борта и измеряют массу Q',создающую нагрузку на колеса этого борта;

— устанавливают на платформе весов все колеса правого борта машины и измеряют массу Q'',создающую нагрузку на колеса правого борта;

Расстояние от центра масс до оси переднего a_M моста определяют расчетным путем по данным, полученным при обмерах и взвешивании машины, по формулам[3]:

Для двухосных машин:

$$a_M = \frac{Q_2 L}{Q}, \qquad (9)$$

где Q – масса машины; Q_2 – масса, приходящаяся на вторую ось, L – расстояние от оси переднего моста до оси заднего моста.

Высоту центра масс машины определяют расчетным путем по данным, полученным в результате взвешивания в горизонтальном и наклонном положении[3].

$$h_M = r_K + \frac{(Q_2' - Q_2)L}{Q tg\alpha_{np}}, \qquad (10)$$

где r_K – статический радиус колеса.

На основании анализа методик для решения задачи научного исследования предложена частная методика определения центра тяжести путем совмещения элементов расчетной и лабораторной методик. Суть частной методики заключается в расчете нагрузки на передний и задний мост серийного автомобиля при его установке под углом α (на рис.1) 2,69 град. На втором этапе частной методики определили высоту центра тяжести h_M по формуле (10) взятой из лабораторной методики. В результате расчета полной массы автомобиля получили значение высоты центра масс h_M равное 1370 мм. Для проверки результатов и адекватности предложенной методики выполнили дополнительный расчет h_M по формуле (7,8) и получили значение 1398 мм. В результате оценки значений установили, что расхождение составляет не более 5%. Поэтому частную методику можно принять как достоверную.

Список литературы

[1]. *Определение* центра масс автомобиля [Электронный ресурс]. – Режим доступа: https://diplomconsult.ru/preview/3568627/

[2]. *Рыжков С.В*. АВТОМОБИЛИ: Методические указания к выполнению курсового проекта для специальности 190601 "Автомобили и автомобильное хозяйство" — М.: Издательство РГСУ, 2009.

[3]. *Вержбицкий А.Н*. Показатели масс автомобилей: метод указания к выполнению лабораторных работ и домашнего задания по курсам «Основы научных исследований и испытаний автомобилей» и «Основы научных исследований и испытаний колесных машин» - М.: Издательство МГТУ им. Н. Э. Баумана. —2009. – С.12–15.

Тинт Наинг Вин - аспирант КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: tintnaingwin1990@gmail.com

Алакин Виктор Михайлович - заместитель директора по инновациям, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: alakin@bmstu-kaluga.ru

С.С. Остроумов

СОВЕРШЕНСТВОВАНИЕ КАРТОФЕЛЕУБОРОЧНЫХ МАШИН В НАПРАВЛЕНИИ СНИЖЕНИЯ ПОВРЕЖДАЕМОСТИ КЛУБНЕЙ КАРТОФЕЛЯ

Теоретические основы картофелеуборочной техники были разработаны в ведущих НИИ: ВИСХОМе, ВИМе, НИИКХ и других, такими учёными, как Алакин В.М., Горячкин В.П., Верещагин Н.И., Виноградов В.И., Грищенко Ф.В., Дорохов А.П., Ельцов Е.И., Кутепов Б.П., Колчин Н.Н., Кузьмин А.В., Мацепуро М.Е., Петров Г.Д., Пшеченков К.А., Сорокин А.А., Угланов М.Б., Шабуров Н.В. и другими.

При комбайновом способе уборки различают три варианта: прямое комбайнирование, раздельная (двухфазная) комбайновая уборка (подбор комбайнами валков, заранее уложенных на поверхность поля картофелекопателями) и уборка комбинированным способом.

Как выяснилось, при уборке повреждается в среднем 40 % клубней по массе. Если принять общее количество повреждений за 100 %, то из этого следует, что только на перепадах повреждается 67,5 %, а на перепадах и сепарирующих органах вместе повреждается уже 95 % клубней.

Таким образом, из всех рабочих органов комбайна наиболее опасны (с точки зрения механических повреждений клубней) сепарирующие органы. Поэтому мы рассмотрим их подробнее.

Прутковые элеваторы среди первичных сепараторов наносят самые незначительные повреждения. Это связано с тем, что полотно элеватора не является жесткой конструкцией, как грохоты или пайлеры (валковые грохоты), а может прогибаться при возникновении значительных усилий, что предотвращает в значительной мере клубни от повреждений. В целом же на данном этапе развития картофелеуборочной техники повреждения, наносимые элеваторами, составляют на копателях 0,8-5,5 %, на комбайнах – 1,6-14 %.

Анализ опытных данных подтверждает то, что основным фактором, определяющим внутренние повреждения клубней, является нормальная составляющая скорости при соударении клубня с полотном. Поэтому для элеватора с ударным встряхивателем внутренние повреждения клубней мало зависят от его линейной скорости, но прямо пропорциональны частоте вращения вала встряхивателя и радиусу его кривошипа (рис. 1) [1].

Для пруткового элеватора с эллиптическим встряхивателем наблюдается прямая зависимость повреждений клубней от линейной скорости полотна (рис. 2), что объясняется имеющейся связью между нормальной составляющей скорости полотна элеватора и его линейной скоростью.

Однако, прутковые сепараторы лучше предназначены для работы в условиях легкопросеиваимых почв: песчаные и супесчаные, а также легкие и средние суглинки. А для более тяжелых суглинков и в условиях повышенной влажности лучше применять роторные сепарирующие рабочие органы, кото-

рые при хорошем крошении почвенного пласта меньше повреждают клубни (4-5%) [2].

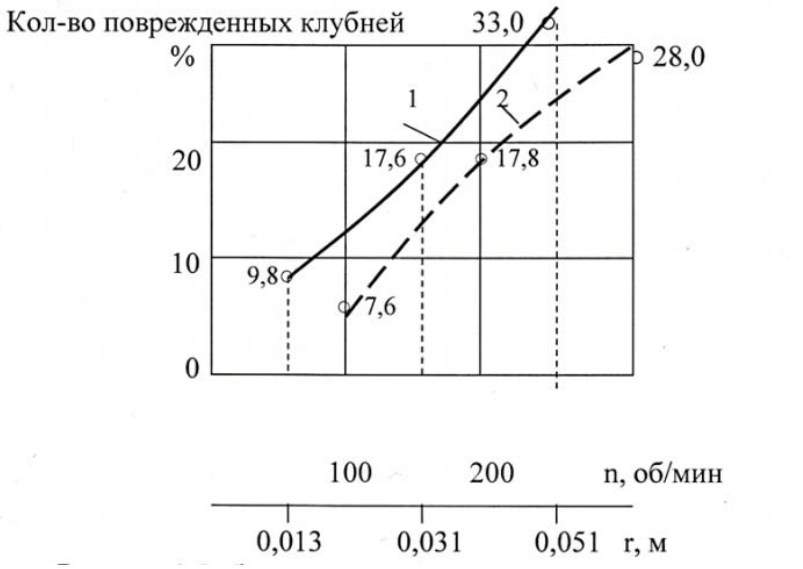


Рис. 1. Зависимость внутренних повреждений клубней
от параметров встряхивателя:
1 – от радиуса кривошипа при n = 200 об/мин и $v_э$ = 1,5 м/с;
2 – от частоты вращения вала при r = 0,031 м, a = 0,025 м, $v_э$ = 1,5 м/с.

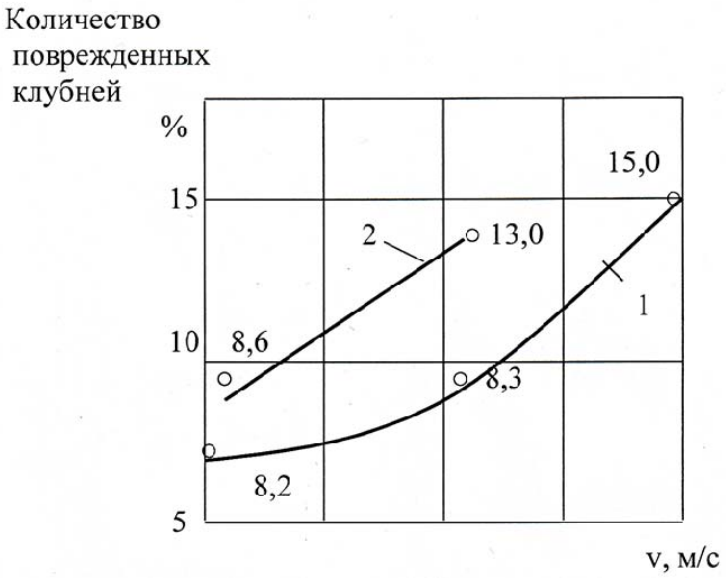


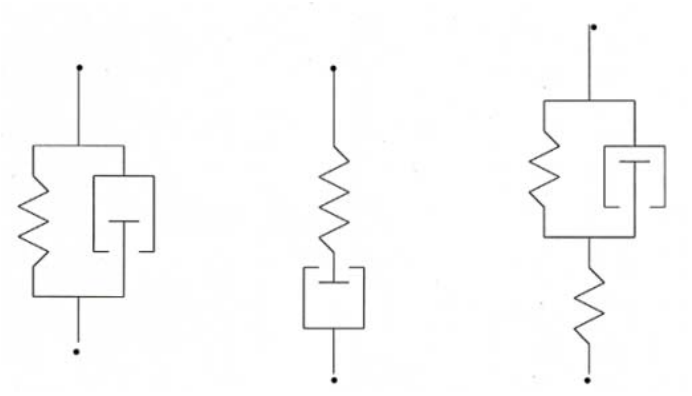
Рис. 2. Зависимость внутренних повреждений клубней от
линейной скорости полотна элеватора с эллиптическим встряхивателем:
1 – полотно с обрезиненными прутками;
2 – полотно с металлическими прутками

Но, прежде чем перейти к рассмотрению конструкции рабочих органов, необходимо проанализировать повреждения клубней. Исследования показали, что из всех видов повреждений клубней наиболее опасны внутренние повреждения мякоти, которые возникают при динамических воздействиях и

могут привести к большим потерям при хранении картофеля. Таким образом, необходимо исследовать поведение мякоти клубня при ударе.

Для проведения математического анализа и прочностных расчетов мякоть клубня необходимо заменить одной из моделей твердого тела. Так, зная, что стенки клеток мякоти клубня проявляют высокую степень упругости и гибкости, цитоплазма проявляет как упругие, так и вязкие свойства, а также то, что крахмальные зерна, входящие в состав клубней, содержат различные полимеры, можно предположить, что мякоти клубней соответствует такая же математическая модель, как и для других высоких полимеров вязкоупругих материалов[3].

В настоящее время известны три вида моделей вязкоупругих материалов (рис. 3).



а *б* *в*

Рис. 3. Модели упруго-вязких сред
а- модель Кельвина-Фойгта;
б - модель Максвелла; *в* - обобщенная модель

Анализ результатов исследования процессов пластической деформации и релаксации образцов, вырезанных из мякоти клубней, и характер протекания описанных процессов указывает на то, что исследуемые образцы обладают как упругими, так и упругопластическими свойствами. Подобное протекание процессов пластической деформации характерно для твердых тел, описываемых моделью твердого тела Зинера (обобщенной моделью), которая состоит из абсолютно упругой части и упругопластической, соединенных последовательно (рис. 3, *в*). При этом K_2 - коэффициент упругости упругой части твердого тела; K_1 - коэффициент упругости упругопластической части тела; а η_1 - коэффициент вязкости упругопластической части тела.

Деформация мякоти клубня, в соответствии с вышеуказанным, является суммой упругой и упругопластической деформаций:

$$\varepsilon = \varepsilon_{yn} + \varepsilon_y, \qquad (1)$$

Деформация упругого элемента равна:

$$\varepsilon_y = \frac{\sigma}{K_2}, \qquad (2)$$

Деформация упругопластической части:

$$\varepsilon_{уп} = \frac{\sigma}{K_1}\left(1 - e^{-\frac{K_1}{\eta_1}t}\right), \quad (3)$$

Следовательно, деформация всего тела будет:

$$\varepsilon = \frac{\sigma}{K_2} + \frac{\sigma}{K_1}\left(1 - e^{-\frac{K_1}{\eta_1}t}\right), \quad (4)$$

Однако проведенные нами опыты по определению времени удара клубня о плоскость, показали, что время удара t колеблется в пределах от 0,0075 до 0,0081 с в зависимости от массы клубня. Подставляя эти значения времени в уравнение (4) мы получим, что e в степени будет стремиться к единице и, следовательно, деформация упругопластической части будет стремиться к нулю, то есть клубень можно заменить моделью только упругой части[4]:

$$\varepsilon_y = \frac{\sigma}{K_2}, \quad (5)$$

Таким образом, мы приходим к линейной модели абсолютно упругого тела, подчиняющегося закону Гука.

Список литературы

[1]. *Лачуга Ю.Ф., Горбачев И.В., Измайлов А.Ю. и др.* Система машин и технологий для комплексной механизации и автоматизации сельскохозяйственного производства на период до 2020 года. Т. 1. Растениеводство. М.:ВИМ, 2012.304 с.

[2]. *Резников Л.А., Ещенко В. Т., Дьяченко Г.Н., Сокол Н.А.* Основы проектирования и расчет сельскохозяйственных машин. М.: Агропромиздат, 1991. С.428-446.

[3]. *Ксеневич И.П., Варламов Г.П., Колчин Н.Н. и др.* Машиностроение. Энциклопедия. Сельскохозяйственные машины и оборудование. Т.IV. М.: Машиностроение, 2002. С.288-298.

[4]. *Туболев С.С., Шеломенцев С.И., Пшеченков К.А., Зейрук В.Н.* Машинные технологии и техника для производства картофеля. М., Агроспас, 2010. С. 176-188.

Остроумов Сергей Сергеевич - канд. техн. наук, преподаватель, «Государственное автономное профессиональное образовательное учреждение Иркутской области». E-mail: kalugasbi@yandex.ru

М.А. Карпов, В.Н. Сидоров

СПОСОБЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПРИ ТОРМОЖЕНИИ АВТОМОБИЛЯ

Понятие «торможение автомобиля» определяет свойство автомобиля снижать скорость движения по желанию водителя, при необходимости быстро останавливаться, а также удерживать на уклоне во время стоянки. Торможение автомобиля имеет большое значение для безопасности движения и зависит от его тормозных качеств и способов торможения. Ошибка водителя при торможении может привести к ДТП.

Умение грамотно тормозить включает в себя:

- сохранение прямолинейного направления движения при торможении;
- использование максимального сцепления колес с дорогой;
- торможение двигателем с одновременным переключением на пониженную передачу;
- остановка при отказе тормозов.

По назначению различают служебное, экстренное и аварийное торможение.

Служебное торможение (с интенсивностью замедления менее 3 м/с2) не связано с дефицитом времени для замедления или остановки автомобиля и в нормальных условиях движения является наиболее приемлемым, так как осуществляется в комфортной зоне отрицательных ускорений.

Экстренное торможение используется в критических ситуациях, связанных с дефицитом времени и расстояния. Оно реализует самое интенсивное замедление с учетом тормозных свойств автомобиля, а также возможностей водителя применить традиционные или нетрадиционные приемы в зависимости от коэффициента сцепления шин с дорогой и других внешних условий.

Аварийное торможение применяется при выходе из строя или отказе рабочей тормозной системы и во всех других случаях, когда эта система не позволяет добиться необходимого эффекта.

Для повышения безопасности движения при торможении автомобиля при выполнении приведенных выше видов торможения применяют различные способы торможения.

Импульсное торможение автомобиля. К импульсному торможению относят два способа торможения - прерывистый и ступенчатый.

Прерывистое торможение - периодическое нажатие на педаль тормоза и полное её отпускание. Основной причиной, вынуждающей временно прекратить действие тормозных механизмов, является блокировка колес. Такой способ применяется на неровной дороге и там, где чередуются участки с разными коэффициентами сцепления, например, асфальт со льдом, снегом и грязью. Эффективность прерывистого способа при экстренном торможении недостаточна, так как временное прекращение действия тормозов влияет на увеличение тормозного пути автомобиля.

Для экстренного торможения характерен ступенчатый способ, который внешне напоминает прерывистый, но в отличие от прерывистого не имеет пассивной фазы, связанной с полным прекращением действия тормозных механизмов. Для него характерно последовательное увеличение каждого последующего усилия на тормозной педали, а также времени его приложения.

Появление в автомобиле ABS, ESP и других систем помощи водителю при торможении меняет представления о том, что нужно делать во время экстренного торможения. Для владельцев автомобилей, не оборудованных ABS, лучше всего подходит прерывистый способ торможения.

Интенсивность экстренного торможения ограничивается возможностями водителя (владением техническими приемами и способностью сохранять устойчивость и управляемость автомобиля), автомобиля (эффективностью тормозных систем, качеством шин) и внешними условиями (коэффициентом сцепления шин с дорогой, рельефом местности).

Контроль за выполнением торможения на грани блокирования колес осуществляется с помощью так называемого **мышечного чувства**. У разных водителей имеются значительные различия в возможностях корректировки мышечных усилий при экстренном торможении. Другим осложняющим фактором является **механизм страха**, который может затормозить проявление даже автоматизированных двигательных навыков и нарушить координацию движений.

В большинстве случаев применение экстренного торможения связано с эффектом полного или частичного кратковременного блокирования колес. Чаще всего блокирование возникает на задних колесах автомобиля, так как при торможении нагрузка в автомобиле перераспределяется по осям: передние колеса загружаются, а задние разгружаются. Поэтому многие автомобили имеют специальные регуляторы тормозных сил, ослабляющие действие задних тормозов на ненагруженном автомобиле.

Прием **«газ-тормоз»** чрезвычайно эффективен на автомобилях с передним приводом и позволяет сохранить управляемость передних колес при интенсивном торможении рабочим тормозом, избежать блокирования управляемых колес, увеличить тормозное усилие. Торможение выполняется левой ногой, во время торможения правая нога продолжает дросселирование - открытый дроссель.

Торможение двигателем и переключение передач. Торможение двигателем не дает большого эффекта замедления в чистом виде, поэтому часто игнорируется водителями. Однако его значимость существенна при управлении автомобилем в условиях низкого коэффициента сцепления и позволяет повысить устойчивость и управляемость автомобиля, его стабильность при экстренных маневрах.

Безопасное управление автомобилем требует, чтобы любой прием торможения выполнялся комбинированным способом, т.е. при включенной передаче. Торможение на нейтральной передаче в нормальных условиях следует расценивать как легкомысленное действие, а в сложных условиях - как

опасное. У некоторых начинающих водителей выработан рефлекс: начиная тормозить, обязательно выключать сцепление. В основе такой привычки лежит ученическая боязнь заглушить двигатель. Но двигатель глохнет при частоте вращения вала менее 500-700 об/мин. Этому режиму на прямой передаче соответствует скорость 13-15 км/ч, поэтому выключать сцепление следует практически перед самой остановкой автомобиля.

Прием «**перегазовка»** выполняется для уравнивания окружных скоростей вращения шестерен, входящих в зацепление. Такой прием помогает избежать рывка автомобиля и не спровоцировать занос на скользкой дороге и, кроме того, уменьшает износ синхронизаторов и увеличивает срок службы КПП. При этом правая стопа водителя осуществляет активное торможение рабочим тормозом, поэтому для выполнения перегазовки необходимо временно прекратить активное торможение или выполнить перегазовку носком (пяткой) правой стопы, не прерывая торможения.

Перегазовка при служебном торможении выполняется за три цикла: выключение повышающей передачи; пауза в нейтральном положении и перегазовка; включение понижающей передачи.

Экстренное торможение требует последовательного переключения передач вниз от прямой передачи до 2-й. Первая передача может включаться в аварийном режиме при отказе рабочей тормозной системы. В этом случае желательно сократить время на перегазовку и изменить структуру приема. Повышение частоты вращения коленчатого вала двигателя достигается не отдельным нажатием на педаль управления подачей топлива, а замедленным выключением сцепления при открытом дросселе.

Для компенсации динамического удара, возникающего при включении понижающих передач, выполняется некоторая пробуксовка сцепления. При комбинированном торможении в случае необходимости экстренного замедления автомобиля переключение передач в нисходящем порядке осуществляется на максимальной частоте вращения коленчатого вала, а в отдельных случаях и на критической.

Способ переключения передачи может быть ударным или мягким. Последний способ гарантирует устойчивость автомобиля в сложных ситуациях движения, особенно при низком коэффициенте сцепления шин с дорогой, но требует высокого уровня мастерства.

Очень вредной является избирательность: на сухой дороге тормозить только рабочим тормозом, на скользкой - еще и мотором. Значительно безопаснее иметь выработанный навык смешанного торможения и применять его в любых условиях, чем создать себе стереотип «летнего» торможения и из-за имеющегося автоматизма применить его на льду или снегу.

Аварийное торможение может осуществляться стояночным тормозом, а также нетрадиционными способами, в том числе и контактным способом с использованием естественных и искусственных препятствий.

В аварийной ситуации, когда все возможности совершения экстренного маневра были исчерпаны и/или произошел отказ тормозной системы, боль-

шинство водителей из-за неумения и стресса прекращают управление. Однако пассивная безопасность конструкции современного автомобиля позволяет существенно снизить тяжесть последствий ДТП за счет деформации сминаемых частей кузова, таких как крылья, бампера, багажник.

При этом важно выбрать направление контакта, чтобы избежать удара «в лоб», поскольку из всех силовых элементов кузова лонжероны имеют максимальную продольную жесткость, вылета на полосу встречного движения и опрокидывания. Как водителю, так и пассажирам необходимо уметь быстро принимать безопасную позу для снижения последствий удара.

Возможные проблемы при торможении автомобиля: невозможно одновременно выполнить резкое торможение (на юз) и маневрирование, при торможении на дорожном полотне с неровностями желательно прекращение торможения при их преодолении, на длительном спуске возможен перегрев тормозов. Временное прекращение торможения позволяет сохранить оптимальный температурный режим рабочего тормоза автомобиля, а, следовательно, и его эффективность.

Изучение способов торможение автомобилем является актуальной задачей среди начинающих автолюбителей. Очень много аварий связано с незнанием правильности торможения, характеристик торможения.

Необходимо помнить, что все перечисленные способы торможения автомобиля необходимо отрабатывать на специальных площадках.

Список литературы

[1]. *Анопченко В.Г.* Практикум по теории движения автомобиля: учебное пособие. – Красноярск: Сибирский федеральный университет, 2013. - 116 с.

[2]. *Буйкус К.В.*, *Тихонович А.М.* Устройство автомобилей: учебное пособие. – Минск: РИПО, 2017. - 304 с.

[3]. *Веюков Е.В.* Основы проектирования автомобильных дорог: учебное пособие для курсового проектирования. – Йошкар-Ола: ПГТУ, 2019. – 146 с.

Карпов Максим Алексеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: karpovmaksim.ru@mail.ru

Сидоров Владимир Николаевич - заведующий кафедрой, доктор техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: sidorov-kaluga@yandex.ru

СЕКЦИЯ 8.

ЗАЩИТА ИНФОРМАЦИИ

А.И. Самохина

АНАЛИЗ ВИДОВ ЭЛЕКТРОННОЙ ПОДПИСИ ДОКУМЕНТОВ

В настоящее время вопрос обеспечения целостности, конфиденциальности информации, а также установления или подтверждения авторства документов, создаваемых, хранимых и передаваемых в электронном виде, играет огромную роль. Одним из методов, защиты информации в данной области является электронно-цифровая подпись.

В настоящее время электронная подпись используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью.

В соответствии со ст. 2 п. 1 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

В ст. 2 п. 11.1 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определено понятие электронный документ – это документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

ЭЦП — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

В России в электронном документообороте можно использовать три вида подписи.

В ст. 5 п. 1 Федерального закона № 63-ФЗ «Об электронной подписи» определены три вида ЭП: «Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее – неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее – квалифицированная электронная подпись)».

Простая электронная подпись, или ПЭП

Простая ЭЦП передается посредством применения паролей, кодов или других спецсредств, сам факт и порядок использования которых уже указывает на то, что подпись сформирована определенным лицом. Примером простой электронной подписи может служить отправленный для авторизации код доступа через СМС, запрашиваемые логин и пароль на сервере предоставления услуг администрирования, при входе в электронную почту и т. п.

В коммерческих целях простая ЭЦП применяется в основном:

- при проведении традиционных банковских операций;
- для авторизации на сервисах по предоставлению госуслуг;
- для подписания внутреннего электронного документа в документообороте компании.

Использование простой электронной подписи недопустимо при подписании документации, содержащей государственную тайну или иную особо охраняемую информацию.

Для легитимизации использования простой цифровой подписи участники документооборота или обмена информацией должны согласовать использование этого средства авторизации подписанта. Если такой вид подписи используется во внутреннем документообороте компании, необходимо принять специальный локальный акт, регламентирующий этот момент.

Зачастую для получения доступа к сервисам по оказанию административных (государственных) услуг необходимо предварительное посещение владельцем простой электронной подписи одного из регистрационных центров для подтверждения личности и привязки к данному лицу его ЭЦП.

Усиленная ЭЦП

Усиленной неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Усиленной квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с 63-ФЗ.

Неквалифицированная электронная подпись, или НЭП

Усиленная неквалифицированная электронная подпись (далее — НЭП) создается с помощью программ криптошифрования с использованием закрытого ключа электронной подписи. НЭП идентифицирует личность владельца,

а также позволяет проверить, вносили ли в файл изменения после его отправки.

Человек получает в удостоверяющем центре два ключа электронной подписи: закрытый и открытый. Закрытый ключ хранится на специальном ключевом носителе с пин-кодом или в компьютере пользователя — он известен только владельцу и его нужно держать в тайне. С помощью закрытого ключа владелец генерирует электронные подписи, которыми подписывает документы.

Открытый ключ электронной подписи доступен всем, с кем его обладатель ведет ЭДО. Он связан с закрытым ключом и позволяет всем получателям подписанного документа проверить подлинность ЭП.

То, что открытый ключ принадлежит владельцу закрытого ключа, прописывается в сертификате электронной подписи. Сертификат также выдается удостоверяющим центром. Но при использовании НЭП сертификат можно не создавать. Требования к структуре неквалифицированного сертификата не установлены в федеральном законе № 63-ФЗ “Об электронной подписи”.

НЭП можно использовать для внутреннего и внешнего ЭДО, если стороны предварительно договорились об этом.

Участникам ЭДО необходимо соблюдать дополнительные условия, чтобы электронные документы, заверенные НЭП, считались равнозначными бумажным с собственноручной подписью. Стороны обязаны заключить между собой соглашение о правилах использования НЭП и взаимном признании ее юридической силы.

Квалифицированная электронная подпись, или КЭП

Усиленная квалифицированная электронная подпись — самый регламентированный государством вид подписи. Так же, как и НЭП, она создается с помощью криптографических алгоритмов и базируется на инфраструктуре открытых ключей, но отличается от НЭП в следующем:

- Обязательно имеет квалифицированный сертификат в бумажном или электронном виде, структура которого определена приказом ФСБ России № 795 от 27.12.2011.
- Программное обеспечение для работы с КЭП сертифицировано ФСБ России.
- Выдавать КЭП может только удостоверяющий центр, который аккредитован Минкомсвязи России.

КЭП применяется, при необходимости сдавать отчетность в контролирующие органы, участвовать в качестве поставщика и заказчика в электронных торгах, работать с государственными информационными системами, обмениваться формализованными документами с ФНС, вести электронный документооборот внутри компании или с ее внешними контрагентами.

КЭП — это подпись, которая придает документам юридическую силу без дополнительных условий. Если организации ведут ЭДО, подписывая документы КЭП, их юридическая сила признается автоматически согласно федеральному закону № 63-ФЗ “Об электронной подписи”.

Можно сделать вывод, что ЭЦП может использоваться для подписания документов в любой сфере. В зависимости от формы подписываемых документов используются различные виды электронно-цифровой подписи.

Список литературы

[1] *Гаврилов М.В.* Информатика и информационные технологии URL: https://studme.org/54376/informatika/informatika_i_informatsionnye_tehnologii

[2] *Федеральный* закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ

[3] *Электронная* подпись (ЭЦП). URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C_(%D0%AD%D0%A6%D0%9F)#.D0.A2.D1.80.D0.B8_.D0.B2.D0.B8.D0.B4.D0.B0_.D1.8D.D0.BB.D0.B5.D0.BA.D1.82.D1.80.D0.BE.D0.BD.D0.BD.D0.BE.D0.B9_.D0.BF.D0.BE.D0.B4.D0.BF.D0.B8.D1.81.D0.B8

Самохина Анастасия Ильинична – студентка КФ МГТУ им. Н.Э. Баумана. E-mail: stasysamdance@gmail.com

А.Г. Гуденко

АНАЛИЗ МЕТОДОВ ЗАПУТЫВАНИЯ КОДОВ

Аннотация

В данной статье рассматриваются основные способы запутывания кода. Производится разбор наиболее часто используемых методов обфускации. Описаны возможные преобразования исходного кода в зависимости от использования различных методов запутывания кода.

Ключевые слова: обфускация, запутывание кода, виды обфускации.

Введение

В настоящее время разработка защиты для программного продукта становится одной из важнейших задач для большинства программистов, так как многие компании желают предотвратить несанкционированное распространение и использование своих продуктов. Существует большое количество способов защиты ПО, таких как шифрование, выполнение на стороне сервера и использование машинного кода, однако одним из самых простых и дешевых способов защиты является обфускация.

Обфускация — приведение программного кода к виду, затрудняющему восприятие алгоритмов работы и модификацию кода, но сохраняющему основной функционал программы.

Для осуществления обфускации можно запутать алгоритм работы программы, исходный код или ассемблерный код. Для запутывания ассемблерного кода можно использовать специализированные компиляторы, которые используют неочевидные возможности среды исполнения. Для запутывания кода можно воспользоваться специализированными программами, осуществляющим запутывание кода, которые называются обфускаторами

Виды обфускации

Различают следующие виды запутывания кода:

1. Лексическая обфускация

Данный способ заключается в приведении кода программы в сложно читаемый, трудный для изучения вид.

Лексическая обфускация включает:

- удаление комментариев или замена их на дезинформирующие
- удаление пробелов, отступов, переносов строк, которые помогают лучше воспринимать текст.
- замену имен переменных, массивов, функций, процедур и т.д., на произвольные наборы символов
- добавление различных мусорных операций, переменных, классов
- изменение расположения блоков программы.

Лексическая обфускация помогает легко сделать код программы трудночитаемым. Однако она относительно малоэффективна по сравнению с другими видами обфускации, и к тому же может применяться лишь к высокоуровневым языкам.

2. Обфускация данных

Данный вид обфускации связан с трансформацией структур данных. Считается, что он сложнее, вследствие чего является более продвинутым и часто используемым. Его делят на следующие группы:

Обфускация хранения. Состоит в трансформации типов и хранилищ данных. Например, создание и использование необычных типов данных, изменение представления существующих и т.д.

Обфускация соединения. При использовании данного способа обфускации происходит соединение независимых данных, или разделение зависимых.

Обфускация переупорядочивания. Состоит в изменении порядка расположения хранилищ данных, объявления переменных, переупорядочивании функций, массивов, полей в структурах и т.д.

3. Обфускация управления

Данный способ запутывания кода осуществляет изменение потока управления, то есть порядка исполнения кода.

Обфускация управления меняет естественный ход программы. Для этого используются действия, результат которых трудно предугадать. В самом простом случае этот способ подразумевает создание дополнительных блоков кода. В этих блоках отдельно выполняются вычисления, отдельно происходит наследование и т.д. В некоторых блоках могут содержаться ложные операции. В других ситуациях может создаваться карта замещений, с помощью которой меняется структура кода.

Обфускация управления использует следующие группы методов:

Вычислительная обфускация. Изменяет структуру потока управления. К этим изменениям относят:

- расширения условий циклов.
- Добавление кода, который никогда не будет выполняться.
- устранение вызовов стандартных библиотек.
- добавление мертвого кода в наиболее трудные для изучения участки кода.
- Распараллеливание кода.

Обфускация соединения. Определенные фрагменты кода программы разделяются , либо, наоборот, объединяются, чтобы затруднить понимание логической связи между ними.

Обфускация последовательности. Заключается в изменении переходов, циклов, выражений.

4. Превентивная обфускация

Данный вид обфускации предназначен для того, чтобы предотвратить, либо помешать злоумышленнику применять деобфускаторы, декомпиляторы и другие средства для анализа программного кода.

Превентивная обфускация использует недостатки, особенности, присутствующие в самых распространенных деобфускаторах часто используемых злоумышленниками.

Заключение

Обфускация не может полностью защитить программный код от злоумышленников. К тому же, она увеличивает время выполнения программы, объем программного кода, затрачиваемые ресурсы. Но, несмотря на все эти недостатки, обфускация позволяет разработчику выиграть время для того, чтобы получить возможность предотвратить несанкционированное распространение их продукта в первое время, что и является основной целью обфускации.

Список литературы

[1]. *Обфускация* и защита программных продуктов [Электронный ресурс] - http://citforum.ru/, 2004. URL: http://citforum.ru/security/articles/obfus/ (дата обращения 15.10.2019).

[2]. *Обфускация,* взгляд изнутри [Электронный ресурс] - http://sharcus.blogspot.com/, 2011. URL: http://sharcus.blogspot.com /2011/06/blog-post.html (дата обращения 16.10.2019).

[3]. *Обфускация,* программное обеспечение [Электронный ресурс] - Википедия – свободная энциклопедия, 2019. URL: https://ru.wikipedia.org/ wiki/Обфускация_(программное_обеспечение) (дата обращения 16.10.2019).

[4]. *Защита* приложения [Электронный ресурс] -https://geekbrains.ru/, 2015. URL: https://geekbrains.ru/posts/app_protection_part2 (дата обращения 16.10.2019).

[5]. *Обзор* существующих обфускаторов и их алгоритмов [Электронный ресурс] - http://masters.donntu.org/, 2015. URL: http://masters.donntu.org/ 2017/fknt/medgaus/library/article1.htm (дата обращения 16.10.2019).

Гуденко Алексей Геннадьевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: alexey199749@gmail.com

А.Н. Огарева, А.Б. Лачихина

АНАЛИЗ СРЕДСТВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕЧАТИ БАНКОВСКИХ ДОКУМЕНТОВ

На данный момент на многих предприятиях происходит цифровизация большинства процессов: электронный документооборот, цифровые подписи, онлайн-сервисы, все это является подтверждением данной тенденции. К сожалению, пока что полный отказ от бумажного документооборота невозможен, поэтому многие предприятия все еще подвержены риску, связанному с печатью документов. Для поиска решений данной ситуации необходимо обозначить основные проблемы, связанные с ней.

Первой проблемой, которую необходимо обозначить, являются излишние растраты на печать. Специалисты Gartner, к примеру, несколько лет назад провели исследование и пришли к выводу, что эти издержки составляют около 3% от бюджета компании, а на каждого сотрудника может тратиться 600-700 долларов в год. Отправка документов на принтеры генерирует 55% внутреннего сетевого трафика, а проблемы, связанные с печатью, становятся причиной до 60% звонков сотрудников в корпоративную техподдержку.

Второе – проблема нецелевого использования устройств для печати личных документов. Случаются ситуации, когда сотрудники начинают злоупотреблять служебными устройствами для печати личной информации, что может привести к серьезным убыткам компании в целом.

Третья, и одна из важнейших категорий возможных проблем, это проблема информационной безопасности - одним из основных каналов утечек информации остается печать конфиденциальных документов. Это может быть как разглашение конфиденциальной информации сотрудников и клиентов компании, так и распространение информации, составляющей корпоративную тайну среди конкурентов.

Недавнее исследование, проведенное International Data Corporation, продемонстрировало печальную статистику:

-В 35% случаев основным каналом утечки данных служили принтеры.

-Компании понесли убытки в размере 134 тысяч долларов в год.

-Только 26% организаций включают защиту принтеров и печатных документов в общую стратегию информационной безопасности.

Из представленных выше проблем ясно, что необходимо пользоваться средствами контроля печати на предприятии, обладающими следующими функциями:

1) Запись в журнал всех фактов печати с подробной информацией, такой как:

- пользователь, инициирующий печать;
- время печати;
- рабочее место печати;
- сам распечатанный файл и другая информация;

2) Контроль доступа к устройствам печати;

3) Сбор статистики и мониторинг печати (по отделам, филиалам и т.п.);

4) Анализ документа и решение – разрешена ли печать данного документа;

Руководитель может воспользоваться услугами аутсорсинговой компании для разработки комплексного решения именно для его предприятия, разработать данное приложения силами сотрудников или же воспользоваться готовыми решениями, предложенными на рынке.

На данный момент существует множество приложений, позволяющих выполнить ту или иную функцию, необходимую для защищенной печати на предприятии. Главным минусом является то, что, скорее всего, потребуется использовать не одно, а сразу несколько решений для обеспечения защиты, что не всегда рационально.

1) FollowMe от компании Ringdale

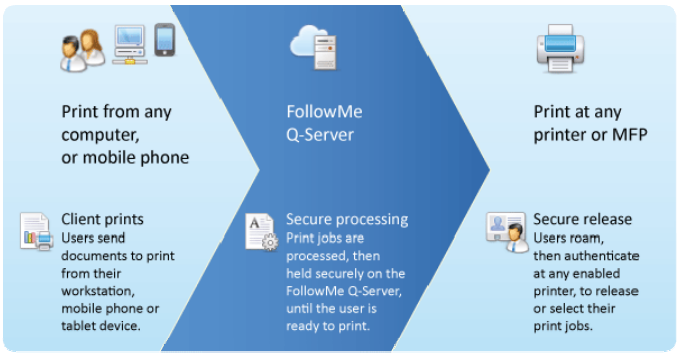


Рис. 1. FollowMe

Обеспечивает решение сразу нескольких необходимых задач, таких как учет и контроль доступа к устройствам. Учет использования всех принтеров и МФУ на предприятии, отслеживание активности отдельных пользователей или рабочих групп.

2) MegaTrack от компании Fontware

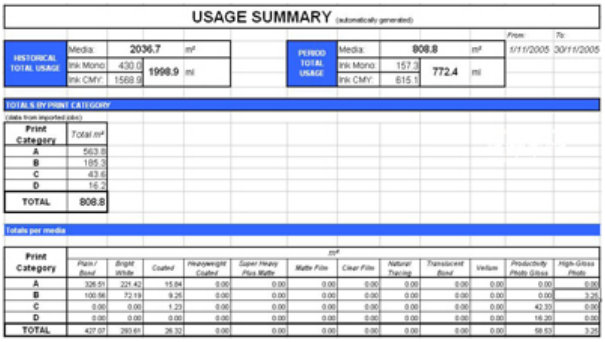


Рис. 2. MegaTrack

Приложение ведет мониторинг устройств печати и собирает статистику для последующего создания отчетов и анализа. Достоинство этого решения – возможность работать не только с сетевыми, но и локальными принтерами. В настройках каждого принтера можно ввести стоимость одного отпечатка, и

система будет создавать также экономические расчеты по каждому отделу или подразделению.

3) Pcounter от компании A.N.D. Technologies

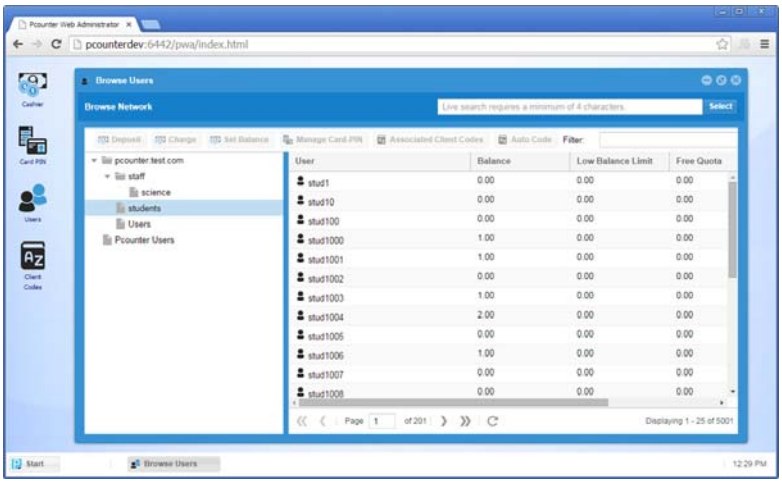


Рис. 3. Pcounter

Плюсом данного решения является простая интеграция в существующую инфраструктуру и последующее масштабирование. Система учитывает все задания печати, отправленные на устройство, собирает статистику его использования.

4) Print Manager Plus от компании Print Manager)

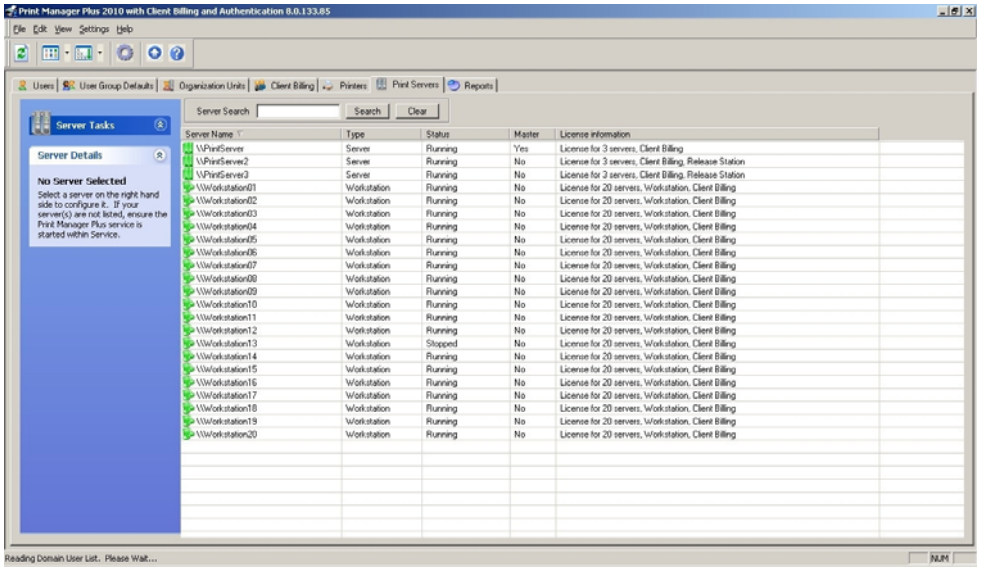


Рис. 4. Print Manager Plus

PMP позволяет и отследить, кто, что и на каком принтере печатал, и рассчитать стоимость печати для конкретного пользователя или отдела. Приложение позволяет проводить анализ состояния инфраструктуры печати.

Большинство рассмотренных выше решений поддерживают журналирование фактов печати, но не всегда в том объеме, котором необходимо организации. Так же они позволяют решить задачи контроля доступа к устройствам печати и вопросы мониторинга. Для решения проблемы анализа документа и решения о печати существует очень малое количество решений, в

большинстве случаев не подходящих под специфику конкретного предприятия.

Итак, можно заключить, что каждое предприятие в выборе средств для обеспечения безопасной печати должно отталкиваться от своей специфики и размера. Если проблема защищенной печати не стоит так остро, то имеет смысл использовать готовые решения. Если же проблема существует, то лучше использовать услуги аутсорсинговых компаний или сотрудников компании для разработки специализированного программного обеспечения, что обеспечит более комплексную и адаптированную защиту предприятия.

Список литературы

[1]. *Блог* компании Бизнес-Фабрика. Корпоративная печать: гораздо больше проблем, чем кажется. 29.07.2016 — [Электронный ресурс] — Режим доступа: URL: https://habr.com/ru/company/business_factory/blog/396345/ (дата обращения: 20.10.2019).

[2]. *Блог* компании Бизнес-Фабрика. Обзор решений для управления печатью. 12.08.2016 — [Электронный ресурс] — Режим доступа: URL: https://habr.com/ru/company/business_factory/blog/396813/ (дата обращения: 20.10.2019).

[3]. *Блог* компании Бизнес-Фабрика. Принтер — находка для шпиона. Как сделать печать в компании безопасным и экономичным процессом — [Электронный ресурс] — Режим доступа: URL: https://habr.com/ru/company/business_factory/blog/397471/ (дата обращения: 20.10.2019).

[4]. *Национальный* банковский журнал. Контролируем печать документов – угроза старая, но не устаревшая — [Электронный ресурс] — Режим доступа: URL: http://nbj.ru/publs/upgrade-modernizatsija-i-razvitie/2018/05/07/kontroliruem-pechat-dokumentov-ugroza-staraja-no-ne-ustarevshaja/index.html (дата обращения: 20.10.2019).

[5]. *Стахановец.* Не защищен принтер – не защищены данные — [Электронный ресурс] — Режим доступа: URL: https://stakhanovets.ru/blog/ne-zashhishhen-printer-ne-zashhishheny-dannye/ (дата обращения: 20.10.2019).

Огарева Антонина Николаевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: antonina.zlygosteva@gmail.com

Лачихина Анастасия Борисовна - доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasialach73@gmail.com

П.А. Селиванов, Ю.С. Белов

ВВЕДЕНИЕ В ПРОМЕЖУТОЧНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ОРИЕНТИРОВАННОЕ НА СООБЩЕНИЯ (MOM)

Введение

По мере того как программные системы продолжают распространяться в постоянно растущих масштабах, выходя за пределы географических и организационных границ, требования, предъявляемые к их коммуникационным инфраструктурам, будут возрастать в геометрической прогрессии. Современные системы работают в сложных средах с несколькими языками программирования, аппаратными платформами, операционными системами и требованиями к динамическим гибким развертываниям с надежностью 24/7, высокой пропускной способностью и безопасностью при сохранении высокого качества обслуживания (QoS). В этих средах традиционные механизмы прямого удаленного вызова процедур (RPC) быстро начинают не справляться с существующими проблемами.

MOM

Для того чтобы справиться с требованиями таких систем, появилась альтернатива механизму распределения RPC. Этот механизм, называемый Message-Oriented Middleware или MOM, обеспечивает связь между отдельными программными объектами. Оно является одним из краеугольных камней, на которых построены распределенные корпоративные системы. Это программное обеспечение может быть определено как любая промежуточная инфраструктура, которая предоставляет возможности обмена сообщениями.

Клиент системы MOM может отправлять и получать сообщения от других клиентов системы обмена сообщениями. Каждый клиент подключается к одному или нескольким серверам, которые выступают в качестве посредника при отправке и получении сообщений. MOM использует модель с одноранговыми отношениями между отдельными клиентами [1]. В этой модели каждый узел может отправлять и получать сообщения от других узлов клиента. Платформы MOM позволяют создавать гибкие связные системы; связная система (cohesion system) - это система, которая позволяет изменениям в одной части системы происходить без необходимости изменений в других частях системы.

Системы с промежуточным программным обеспечением, ориентированным на сообщения, обеспечивают распределенную связь на основе модели асинхронного взаимодействия. Эта неблокирующая модель позволяет решать многие ограничения, существующие в RPC. Участники системы не обязаны блокировать и ждать отправки сообщения, им разрешено продолжать обработку после отправки сообщения. Это позволяет доставлять сообщения, когда отправитель или получатель не активен или недоступен для ответа во время выполнения.

МОМ поддерживает доставку сообщений, которая может занять несколько минут, в отличие от таких механизмов, как RPC (RMI), которые доставляют в миллисекундах или секундах. При использовании МОМ отправляющее приложение не гарантирует, что его сообщение будет прочитано другим приложением, а также не дает гарантии о времени, в течение которого оно будет доставлено. Эти аспекты в основном определяются принимающим приложением.

МОМ вводит независимый слой между отправителями и получателями, который позволяет им использовать его в качестве посредника для обмена сообщениями. Основным преимуществом МОМ является слабая связь между участниками системы т.е. возможность связывать приложения без необходимости адаптировать исходную и целевую системы друг к другу.

В МОМ потеря сообщений из-за сбоя сети или системы предотвращается с помощью механизма сохранения и пересылки сообщений. Эта возможность вводит высокий уровень надежности в механизм распределения, хранения и пересылки предотвращает потерю сообщений, когда части системы недоступны или заняты. Определенный уровень надежности обычно настраивается, но системы обмена сообщениями с промежуточным программным обеспечением могут гарантировать, что сообщение будет доставлено, и что оно будет доставлено каждому предполагаемому получателю ровно один раз.

В дополнение к отделению взаимодействия подсистем, МОМ также отделяет характеристики производительности подсистем друг от друга. Подсистемы могут масштабироваться независимо, практически не нарушая работу других подсистем. Оно также позволяет системе справляться с непредсказуемыми всплесками активности в одной подсистеме, не затрагивая другие области системы. Модели обмена сообщениями МОМ содержат ряд естественных особенностей, которые обеспечивают простую и эффективную балансировку нагрузки, позволяя подсистеме принимать сообщение, когда она готова к этому, а не быть вынужденной принять его.

МОМ внедряет возможности высокой доступности в системы, обеспечивая непрерывную работу и более плавную обработку сбоев системы [2]. Оно не требует одновременной доступности всех подсистем. Сбой в одной из подсистем не приведет к возникновению цепочки сбоев во всей системе. МОМ также может улучшить время отклика системы из-за слабой связи между участниками. Это может сократить время завершения процесса и повысить общую чувствительность и доступность системы.

Сравнение МОМ и RPC

В зависимости от условий, в которых используется приложения, как МОМ, так и RPC имеют свои преимущества и недостатки. RPC обеспечивает более простой подход к обмену сообщениями, используя знакомую и простую модель синхронного взаимодействия. Однако механизм RPC страдает от негибкости и жесткой связи (потенциального геометрического роста интерфейсов) между взаимодействующими системами. Также проблематично масштабировать части системы и иметь дело с перебоями в обслуживании.

RPC предполагает, что все части системы будут доступны одновременно, если одна часть системы выйдет из строя или даже станет временно недоступной (отключение сети, обновление системы), тогда вся система может в результате остановиться.

Вызовы RPC требуют больше пропускной способности, чем аналогичное взаимодействие MOM. Модель RPC разработана на основе концепции одного клиента, взаимодействующего с одним сервером. Традиционный RPC не имеет встроенной поддержки связи "один ко многим". Преимуществом системы RPC является простота механизма и простота реализации. MOM упрощает процесс построения динамических гибких распределенных систем корпоративного класса.

Преимущество RPC перед MOM это гарантия последовательной обработки. С помощью синхронной модели RPC можно управлять порядком, в котором происходит обработка в системе. Например, в системе RPC вы можете быть уверены, что в любой момент времени все новые заказы, полученные системой, были добавлены в базу данных и что они были добавлены в том порядке, в котором они были получены. Однако при асинхронном подходе MOM это не может быть гарантировано, так как новые заказы могут существовать в очередях, ожидающих добавления в базу данных. Это может привести к временной неточности данных в базе данных[3]. RPC работает медленно, но последовательно, работа всегда выполняется в правильном порядке. Это важно для системы, которая требует, чтобы данные имели 100% временную целостность. Если этот тип целостности является более важным, чем производительность, вам нужно будет использовать модель RPC или разработать свою систему для проверки этих потенциальных временных неточностей.

Промежуточное программное обеспечение, ориентированное на сообщения, позволяет системе развиваться без резких изменений в приложении. Это обеспечивает инфраструктуру интеграции, которая приспосабливает функциональные изменения с течением времени без нарушения или ущерба для производительности и масштабируемости. Раздельный подход MOM дает возможность гибко интегрировать клиентов в систему и поддерживать большое количество потребителей/клиентов и анонимность производителя/потребителя. Коммерческие реализации обеспечивают высокую масштабируемость с поддержкой десятков тысяч клиентов, расширенную фильтрацию, легкую интеграцию.

Заключение

Метод RPC идеально подходит, если вам нужна строго типизированная или объектно-ориентированная система с жесткой связью, семантической проверкой во время компиляции и общей более простой реализацией системы.

Если распределенные системы будут с географически рассредоточенными развертываниями, с плохим подключением к сети и строгими требованиями к надежности, гибкости и масштабируемости, то MOM будет является идеальным решением.

Список литературы

[1]. *Бабичев С. Л.* Распределенные системы : учебное пособие для вузов / С. Л. Бабичев, К. А. Коньков. — Москва : Издательство Юрайт, 2019. — 507 с. — (Высшее образование). — ISBN 978-5-534-11380-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.urait.ru/bcode/445188 (дата обращения: 28.10.2019).

[2]. *Богатырев В.А.* Информационные системы и технологии. Теория надежности : учебное пособие для бакалавриата и магистратуры / В. А. Богатырев. — Москва : Издательство Юрайт, 2019. — 318 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-00475-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.urait.ru/bcode/433723 (дата обращения: 28.10.2019).

[3]. *Рыбальченко М.В.* Архитектура информационных систем : учебное пособие для вузов / М. В. Рыбальченко. — Москва : Издательство Юрайт, 2019. — 91 с. — (Университеты России). — ISBN 978-5-534-01159-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.urait.ru/bcode/437686 (дата обращения: 28.10.2019).

Селиванов Павел Александрович - студент, магистрант, ЗАО Калуга Астрал. E-mail: stejls@mail.ru

Белов Юрий Сергеевич - доцент, канд. физ.-мат. наук КФ МГТУ им. Н.Э. Баумана. E-mail: iu4-kf@mail.ru

Е.Ю. Шестопалов, А.В. Бурмистров, А.Б. Лачихина

ВИДЫ АТАК НА НЕЙРОННЫЕ СЕТИ

В последнее время технология машинного обучения, а именно глубокое обучение с использование глубоких нейросетей демонстрирует выдающиеся результаты во многих областях. Благодаря значительным успехам в машинном зрении и обработке естественного языка глубокие нейронные сети стали применяться во множестве областей, например, медицине [1], финансовой сфере [2], транспорте [3] и других. Однако, несмотря на свою высокую эффективность, глубокие нейронные сети уязвимы к состязательным атакам (adversarial attacks). Они заключаются в незначительном изменении данных, поступающих на вход нейросети (часто незаметным для человека), которое приводит к ошибке.

Данные атаки подразделяются на несколько подклассов [4].

По степени доступа злоумышленника к атакуемой нейросети:

- Типа черный ящик (black box);
- Типа белый ящик (white box).

В первом случае атакующий не имеет информации об архитектуре нейросети, ее параметрах, функции ошибки и способе обучения. Его взаимодействие с ней сводится к подаче данных на вход и получения предсказания. Все выводы о внутреннем строении делаются опосредованно.

Во втором случае у нападающего есть доступ непосредственно к самой нейросети и вся информация о ней.

Также такие атаки подразделяются по цели:

- Целевые (targeted);
- Нецелевые (non-targeted).

В случае целевой состязательной атаки злоумышленнику важно заставить нейросеть отнести модифицированные им входные данные к определенному классу. В случае нецелевой атаки ему важен лишь факт ошибки.

Так как к состязательным атакам уязвимы нейросети в целом, то данные атаки могут быть проведены в любой области. В данной работе рассмотрены две наиболее изученные области применения глубоких нейронный сетей – машинное зрение (computer vision) и обработка естественного языка (natural language processing).

Состязательные атаки на нейросети в задачах машинного зрения сводятся к добавлению к входному изображению шума, заставляющего ошибиться нейросеть, который часто незаметен для человека. Отличие атак заключается в методах получения данного шума, а также количестве изменяемых пикселей.

Виды состязательных атак в области машинного зрения [5]:

- Box-constrained L-BFGS
- Fast Gradient Sign Method (FGSM)
- Basic & Least-Likely-Class Iterative Methods
- Jacobian-based Saliency Map Attack (JSMA)

- One Pixel Attack
- Carlini and Wagner Attacks (C&W)
- DeepFool
- Universal Adversarial Perturbations
- UPSET
- ANGRI
- Houdini
- ATNs

В случае состязательных атак на нейросети в задачах обработки естественного языка изменение входной информации отличается от такового в машинном зрении. Исследователи используют не только добавление шума, но и замену и удаление слов. Также изменение входных данных осложнено тем фактом, что замена, добавление или удаление одного слова может сильно изменить смысл предложения.

Виды состязательных атак в области обработки естественного языка [6]:

- Fast Gradient Sign Method (FGSM)
- Jacobian-based Saliency Map Attack (JSMA)
- Carlini and Wagner Attacks (C&W)
- Direction-based
- Attention-based
- Reprogramming
- Concatenation Adversaries
- Edit Adversaries
- Paraphrase-based Adversaries
- GAN-based Adversaries
- Substitution

Несмотря на большое разнообразие состязательных атак на нейронные сети в разных областях, известные на данный момент методы защиты одинаковые. Наиболее распространенными являются состязательное обучение (adversarial training), фильтрация (distillation) и использование подавителей шумов (noise denoisers) [5,6].

Состязательное обучение заключается в добавлении в тренировочные данные состязательных примеров. Так модель учится давать корректные ответы на модифицированных данных. Недостатком данного метода является тот факт, что модель становится более устойчивой только к тем видам атак, которые были представлены при обучении.

Фильтрация заключается в обучении двух нейросетей. Первую обучают на имеющихся строгих метках данных. Вторую – на выходных данных первой, что делает входы второй нейросети более гладкими, чем у первой. Данный прием позволяет сделать нейросеть более устойчивой к модификации входных данных, однако, он менее эффективен, чем предыдущий.

Подавители шумов представляют собой отдельные нейросети, которые пытаются обнаружить во входных данных добавленный злоумышленником вредоносный шум, с целью дальнейшего его исключения. Преимуществом

такого метода является возможность повышения защищенности нейросети за счет простого добавления этого компонента без необходимости переучивать существующую нейросеть или обучения новой.

Таким образом, на данный момент технология глубокого обучения уязвима к атакам. Состязательные атаки представляют большую угрозу для технологии глубокого обучении, так как существующие методы противодействия не обеспечивают достаточного уровня защиты. Это является существенной проблемой, потому что нейросети активно внедряются в различные сферы жизни общества из-за их высокой эффективности. Однако высокая активность исследователей в данной области вселяет уверенность, что будут найдены способы обеспечить достойный уровень защиты.

Список литературы

[1]. *Курников Д.С., Петров С.А.* Использование нейронных сетей в экономике // Juvenis scientia. 2017. №6. URL: https://cyberleninka.ru/article/n/ispolzovanie-neyronnyh-setey-v-ekonomike (дата обращения: 16.10.2019).

[2]. *Akhtar N., Mian A.* (2018) Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey // arXiv.org URL: https://arxiv.org/pdf/1801.00553.pdf (дата обращения: 17.10.2019)

[3]. *Huang S., Papernot N., Goodfellow I., Duan Y., Abbeel P.* (2017) Adversarial Attacks on Neural Network Policies // arXiv.org URL: https://arxiv.org/pdf/1702.02284.pdf (дата обращения: 17.10.2019)

[4]. *Grigorescu S., Trasnea B., Cocias T., Macesanu G.* (2019) A Survey of Deep Learning Techniques for Autonomous Driving // arXiv.org URL: https://arxiv.org/pdf/1910.07738.pdf (дата обращения: 16.10.2019)

[5]. *Litjens G., Kooi T., Bejnordi B. E., Adiyoso Setio A.A., Ciompi F., Ghafoorian M., Jeroen A.W.M. van der Laak, B. van Ginneken, I. Sánchez C. A* (2017) Survey on Deep Learning in Medical Image Analysis // arXiv.org URL: https://arxiv.org/pdf/1702.05747.pdf (дата обращения: 16.10.2019)

[6]. *Zhang W.E., Z. Sheng Q., Alhazmi A., Li Ch*. (2019) Adversarial Attacks on Deep Learning Models in Natural Language Processing: A Survey // arXiv.org URL: https://arxiv.org/pdf/1901.06796.pdf (дата обращения: 17.10.2019)

Шестопалов Егор Юрьевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: shestopalovegor@gmail.com

Бурмистров Александр Викторович - ассистент кафедры «Защита информации» КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: burmistrov@bmstu.ru

Лачихина Анастасия Борисовна - доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasialach73@gmail.com

С.В. Степаненко

ВИДЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ

Создание резервных копий данных на регулярной основе остается важной частью обеспечения информационной безопасности, несмотря на то, что хранилища данных становятся все более надежными и устойчивыми. Существуют различные способы копирования информации, позволяющие её восстановить в случае возникновения инцидентов [1]:

– Полное копирование;
– Инкрементальное копирование;
– Дифференциальное копирование.

В табл. 1 приведены данные, которые будут сохраняться при различных видах копирования.

Таблица 1.

Сравнение видов резервного копирования

Номер резервной копии	Полное копирование	Инкрементальное копирование	Дифференциальное копирование
1	Полная копия	Полная копия	Полная копия
2	Полная копия	Изменившиеся со времени создания копии №1 данные	Изменившиеся со времени создания копии №1 данные
3	Полная копия	Изменившиеся со времени создания копии №2 данные	Изменившиеся со времени создания копии №1 данные

Основным видом является полное резервное копирование. Этот вид резервного копирования сохраняет полную копию всех данных на другой носитель. Основным преимуществом данного вида является минимальное время на восстановления данных. Недостатки заключаются в том, что оно занимает больше времени, чем другие виды, и требует больше места для хранения.

Инкрементальное резервное копирование подразумевает копирование только тех данных, которые были изменены с момента последней операции резервного копирования любого вида. Инструмент резервного копирования считывает метку времени в файлах и сравнивает ее с меткой времени последней резервной копии, после этого он записывает дату и время выполнения операции, чтобы в дальнейшем отслеживать измененные файлы. Преимущество инкрементального резервного копирования заключается в том, что при нем копируется меньший объем данных. Таким образом, данная операция будет выполняться быстрее и потребуют носителя информации с меньшим объемом.

Операция дифференциального резервного копирования при первом применении аналогична инкрементальному. Но при каждом следующем создании резервной копии будет продолжаться копирование всех данных, измененных с момента предыдущего полного резервного копирования [2]. Таким образом, для дифференциальных резервных копий требуется больше места и времени, чем для инкрементальных, но меньше, чем для полных.

Применение различных видов резервного копирования. На практике зачастую используется один из следующих подходов к резервному копированию:

- Полное ежедневное копирование;
- Полное еженедельное копирование и инкрементальное ежедневное;
- Полное еженедельное копирование и дифференциальное ежедневное.

В таблице 2 приведены требования к объему носителя для трех типичных стратегий резервного копирования [3]. Эти расчеты предполагают 20 ТБ общих данных, при этом 5% данных изменяются ежедневно, а общий объем хранилища за период не увеличивается.

Таблица 2.

Сравнение подходов к созданию резервных копий данных

Подход к резервному копированию	Необходимый размер носителей для хранения резервных копий за месяц	Необходимые файлы для восстановления данных
Полное ежедневное копирование	440 ТБ	Последняя резервная копия
Полное еженедельное копирование и дифференциальное ежедневное	156 ТБ	Последняя полная резервная копия и последняя дифференциальная копия
Полное еженедельное копирование и инкрементальное ежедневное	120 ТБ	Последняя полная копия и все инкрементальные копии

В соответствии с приведенными данными можно сделать следующие выводы.

Ежедневное полное резервное копирование требует больше места, однако доступно больше копий данных. В результате реализации этого подхода система имеет более высокую устойчивость к угрозам информационной безопасности, обеспечивается наименьшее время для восстановления.

В качестве альтернативы, еженедельное полное резервное копирование в сочетании с ежедневным инкрементальным использует наименьшее количество дискового пространства. Но такой подход может значительно увеличить

время восстановления и требует, чтобы каждая копия была правильной: сбой в одной из них может повлиять на все восстановление.

Запуск еженедельного полного резервного копирования и ежедневного дифференциального является компромиссным: меньший размер резервных копий по сравнению с первым подходом, более быстрое и надежное восстановление данных по сравнению со вторым.

Список литературы

[1] *George Crump.* The 7 critical backup strategy best practices to keep data safe, 2019. URL: https://searchdatabackup.techtarget.com/feature/The-7-critical-backup-strategy-best-practices-to-keep-data-safe (дата обращения 21.10.2019)

[2] *Савин И.В.* Дифференциальное резервное копирование. Преимущества и недостатки. Современные инновации, 2018, №5, с. 14-16.

[3] *Russ Fellows, Paul Crocetti.* Types of backup explained: Full, incremental, differential and mirror, 2019. URL: https://searchdatabackup.techtarget.com/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type (дата обращения 21.10.2019)

Степаненко Станислав Витальевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: st.v.stepanenko@gmail.com

К.Н. Солдатов

ДИАГНОСТИКА ФУНКЦИОНИРОВАНИЯ ПРЕДПРИЯТИЯ ПО ОТКЛОНЕНИЯМ В ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Современные предприятия и организации в различных сферах деятельности включают в себя информационные системы (ИС), обеспечивающие централизованное управление, автоматизацию процессов, мониторинг показателей работы и т.д. Каждая ИС обладает собственной структурой и моделью, выбранной или созданной в соответствии с областью применения и набором решаемых задач. Большинство систем включает в себя анализ функционирования всего предприятия, по результатам которого может быть отмечено снижение показателей, в связи с чем потребуется проведение мероприятий по выявлению и устранению причин.

Неотъемлемой частью любой системы являются данные, получаемые в ходе эксплуатации системы или из внешних источников. Вся информация хранящаяся и обрабатываемая в системе может использоваться для мониторинга, который позволяет проводить оценку работы по показателям эффективности и выявлять различного рода отклонения в производственных и бизнес-процессах организации. Дополнительно может проводиться анализ в смежных областях, что дает возможность отслеживать современные тенденции и получать актуальную информацию, играющую важную роль при принятии управленческих решений.

ИС масштаба предприятия работают с большими объемами постоянно накапливающихся многомерных данных, которые могут содержать скрытые закономерности. Для анализа такой информации эффективно применяются методы Data mining (интеллектуальный анализ данных) [1]. Данная технология направлена на поиск в больших объемах данных неочевидных и практически полезных закономерностей. Этот подход может применяться в различных областях для решения ряда задач таких как классификация, кластеризация, прогнозирование, поиск ассоциаций и т.д. [2].

Одной из задач Data mining является определение отклонений, что можно использовать для обнаружения нехарактерных значений в потоке рабочих данных. Данная задача заключается в поиске редких, нетипичных объектов или наблюдений, которые не соответствуют логике поведения анализируемого бизнес-процесса, или модели описывающей его данные. Статистические показатели, как правило, имеют случайный характер, но для каждого производственного процесса заданы определенные пределы, выходя за которые можно зафиксировать изменения в функционировании системы. Получаемые результаты анализируются для выявления наиболее значимых отклонений, при наличии которых проводятся дополнительные исследования с целью выявления их причин.

Как уже отмечалось, большие объемы данных могут содержать скрытые связи, которые могут быть выявлены с помощью подходов Data mining в рамках задачи поиска закономерностей. Это одна из распространенных задач в области анализа информации, она позволяет сопоставлять исходные данных и отклонения, полученные за определенные интервалы времени, выводя таким образом ассоциативные правила [3]. При этом точность правил и вероятность их выявления увеличивается прямо пропорционально объему данных и величине анализируемого периода. Полученные связи в виде правил достаточно легко проанализировать и определить факторы влияющие на отклонения показателей. Полученная таким образом информация может быть использована руководящими лицами при принятия управленческих решений.

В качестве примера можно привести предприятие по производству автомобилей, на котором производится сбор, агрегация и анализ данных: поставщики комплектующих деталей, параметры производственных процессов, количество выпускаемой продукции, уровень продаж в различных регионах, показатели автомобилей в период их эксплуатации и т.д. На основании информации, получаемой из сервисных центров, было зафиксировано увеличение числа неисправностей определенного узла автомобиля. Анализ данных за период выпуска автомобилей, для которых отмечены изменения, позволил определить, что был изменен поставщик деталей, что и явилось причиной участившихся поломок. Обладая данной информацией руководители могут принять решение о выборе более надежного поставщика для повышения качества выпускаемой продукции и предотвращения потенциального снижения спроса на данные марки автомобилей, вызванного участившимися случаями поломок.

В процессе функционирования предприятия могут возникать отклонения, влияющие на его работу и результаты. Большинство используемых ИС включают в себя процедуры анализа данных, что способствует обнаружению значимых изменений. При наличии больших объемов данных могут применяться методы Data mining, что позволяет обнаружить скрытые закономерности, связывающие изменения с их причинами. Получаемые формальные правила так же дают возможность выявить положительные тенденции, поддержание которых может способствовать повышению производительности.

Список литературы

[1]. *Силен Д., Мейсман А., Али М.* Основы Data Science и Big Data. Python и наука о данных. Санкт-Петербург, Питер, 2018, 336 с.

[2]. *Брюс П., Брюс Э.* Практическая статистика для специалистов Data Science. 50 важнейших понятий. Санкт-Петербург, БХВ-Петербург, 2018, 304 с.

[3]. *Ерисов В.Д., Пекова Е.А.* Применение средств интеллектуального анализа данных (data mining) для исследования экономических показателей. Международный студенческий научный вестник, 2019, №4, с. 8-16.

Солдатов Константин Николаевич - аспирант КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: Konstantin_Nikolaevich_91@mail.ru

П.Ю. Малахов

ЗАРУБЕЖНЫЙ ОПЫТ ФОРМИРОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Отправной точкой для формирования культуры информационной безопасности в развитых странах стали рекомендации Организации экономического сотрудничества и развития (ОЭСР) («Руководящие принципы по безопасности информационных систем и сетей: «На пути к культуре безопасности»), принятые в 2002 году. Эти рекомендации стали основой для Резолюции Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности», принятой в декабре 2002 года.

ОЭСР – это группа стран-единомышленников, приверженных принципам рыночной экономики и демократического плюрализма. Базы данных ОЭСР охватывают следующие области: системы национальных счетов, экономические показатели, торговлю, занятость, миграцию, образование, энергетику, здравоохранение и экологию.

Фактически рекомендации ОЭСР явились первым из известных документов, посвященных проблеме формирования в обществе культуры информационной безопасности. В 2003 и 2004 годах ОЭСР опросила правительства стран-участниц организации на тему реализации руководящих принципов ОЭСР для безопасности информационных систем и сетей: «На пути к культуре безопасности». По результатам опроса было выяснено, что почти все правительства стран-участниц ОЭСР завершили разработку своих национальных стратегий формирования культуры безопасности информационных систем и сетей. Подавляющая часть стран, принявших участие в опросе, сообщила о мерах, направленных на повышение осведомленности граждан по вопросам информационной безопасности, в том числе об инициативах, адресованных конкретным категориям населения: широкой общественности, предпринимателям малого и среднего бизнеса, молодым пользователям и новичкам в освоении информационных технологий.

Страны мира по-разному развиты в сфере информационных технологий, поэтому даже для решения похожих вопросов они применяют различные подходы. Международные стандарты будут определять лишь основные векторы по вопросам информационной безопасности. Каждая национальная культура будет иметь свои особенности. Анализ результатов опроса стран-участниц ОЭСР позволил выявить наиболее распространенные меры по формированию у граждан культуры информационной безопасности и способы ведения информационнопросветительской и пропагандистской работы с населением (см. табл. 1).

Таблица 1.

Меры по повышению осведомленности граждан в вопросе информационной безопасности

Методы повышения осведомленности граждан в странах ОЭСР.	
Страны	**Метод**
1	**2**
США	Создание национальной системы кибероповещения пользователей
Австрия, Нидерланды	Внедрение системы электронных государственных услуг
Австралия, Финляндия, Франция, ФРГ, Япония, Корея, Нидерланды, Португалия, Испания, Швеция, Великобритания, США	Организация сайтов и порталов по вопросам информационной безопасности
ФРГ, Японии, Нидерланды, Швеция, Великобритания, США	Организация сайтов, ориентированных на пользователей без опыта работы с ИКТ и Интернетом
Испания	Организация сайта «Центр раннего оповещения о вирусах и компьютерной безопасности» для пользователей Интернета
Чехия	Реализация национальной программы компьютерной грамотности
Австралия, Чехия, Франция, ФРГ, Венгрия, Япония, Корея, Мексика, Нидерланды, Португалия, США	Проведение рабочих совещаний, семинаров, обучения, конференций по информационной безопасности и публикация соответствующих трудов и исследований
Финляндия, Корея, Нидерланды, США	Привлечение средств массовой информации к информационно-пропагандистской деятельности в области информационной безопасности
Дания, ФРГ, Испания	Организация информационно-просветительских кампаний
Канада, США, Норвегия	Организация сайтов и информационных ресурсов для повышения осведомленности граждан в области информационной безопасности
Венгрия, ФРГ, Дания, США, Финляндия, Франция	Подготовка и распространение бесплатных информационных материалов, правил, рекомендаций, методологии, передовых практик и руководств по информационной безопасности
ФРГ	Участие в ассоциациях, федерациях, обществах по профилю информационной безопасности

Таблица 2(окончание)

1	2
Италия	Создание комитета для повышения осведомленности по вопросам информационной безопасности
США	Создание «горячих» линий для консультаций по вопросам информационной безопасности
Корея	Организация конкурсов по безопасности информационных систем и сетей для широкой общественности
Австралия	Организация серии встреч в разных городах по вопросам информационной безопасности
Япония	Онлайновые технические консультации для пользователей Интернета
Австрия	Внедрение услуг онлайн-банкинга с мобильными электронными подписями

В итоге можно сказать, что странами ОЭСР для формирования культуры информационной безопасности были выбраны следующие принципы: осведомление и расширение прав для населения в плане информационной безопасности, ответственность за управление риском цифровой безопасности со стороны государства и населения, управление рисками цифровой безопасности в соответствии с правами человека.

Список литературы

[1]. *Малюк А.А. , Полянская О.Ю.* Зарубежный опыт формирования в обществе культуры информационной безопасности. - Национальный исследовательский ядерный университет «МИФИ», Проект № 15-03-00248 – 2016.

[2]. *Кошелев Н.В.* ОЭСР (Организация экономического сотрудничества и развития). – 2019.

Малахов Павел Юрьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: pavel.mologec@gmail.com

С.С. Щеголихин

ИССЛЕДОВАНИЕ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Проблема обеспечения безопасности документооборота существовала всегда, и за прошедшие столетия были найдены способы, которые смогли обеспечить достоверность документа. Сам лист бумаги позволяет убедиться в целостности документа, поэтому в большинстве стран, включая Россию, законодательные акты и судебные решения хранятся в виде бумажных папок с документами в архивах. Проблемы подтверждения достоверности документа на бумаге решаются путем проставления штампов, печатей, личных подписей, а в особых случаях могут применяться водяные знаки.

Использование электронных документов появилось относительно недавно. Появление доступа к сети интернет полностью изменило положение, оно предоставило множество возможностей для передачи данных

Электронный документооборот (ЭДО) — это совокупность автоматизированных процессов в работе с документами, представленными в электронном виде без использования бумажных носителей.[1] Технологии ЭДО часто используются организациями для автоматизации их повседневных бизнес-процессов. Современный документооборот не обязательно связан с одной организацией, а может охватывать сразу несколько организаций.

Защита не для документа

Любой элемент системы ЭДО — документ, может быть файлом внутри системы, а может быть записью в БД. Когда говорят о защищенном ЭДО, то чаще всего подразумевают защиту документов, а именно защиту информации, которая находится в них.

По этому поводу есть небольшое заблуждение, потому что речь идет именно о защите системы, а не только о защите данных, которые в ней находятся.

Как защищать

Любая система электронного документооборота должна предусматривать механизмы защиты от угроз:

- обеспечение сохранности документов
- обеспечение подлинности документов
- протоколирование действий пользователей

Обеспечение сохранности документов

Система ЭДО должна обеспечивать сохранность документов от порчи и потери, а также иметь возможность их восстановления. По статистике 40% случаев потери важной информации приходятся на причины сбоя аппаратуры, стихийные бедствия и т.д. 35 % случаев происходят по вине пользователей и 25% приходится на действия злоумышленников. По результатам опроса, который был проведен в 2006 году аналитической компанией Deloitte-

Touch, было выявлено, что почти половина всех компаний сталкивались с потерей данных за последние 12 месяцев. Около 30% таких случаев привели к серьезным финансовым потерям.

Современные системы электронного документооборота имеют собственные подсистемы резервного копирования. Например, отказоустойчивый кластер Master-Slave на PostgreSQL.[2]

Обеспечение подлинности документов

Сегодня основным и практически единственным предлагаемым на рынке решением для обеспечения подлинности документа является электронной подписи (ЭП). Основной принцип работы ЭЦП основан на технологиях шифрования с ассиметричным ключом. Т.е. ключи для шифрования и расшифровки данных отличаются.

О «закрытом» и «открытом» ключах : «закрытый» и «открытый» ключи используются в асимметричной криптографии, с которой:

- открытый и закрытый ключи работают парами, и один открытый ключ соответствует одному уникальному закрытому ключу;
- данные, зашифрованные открытым ключом, могут быть расшифрованы только с помощью соответствующего закрытого ключа и наоборот;
- закрытый ключ хранится в секрете шифратором, а открытый ключ является открытым.

С помощью ЭП можно безопасно передавать документы, не боясь за то, что кто-то попытается изменить их. При проверке документа ЭП показывает, что документ был подписан именно отправителем, а также подтверждается тот факт, что документ не был изменен. Следовательно, подписать документ может именно обладатель «закрытого» ключа. Проверить подлинность документа можно с помощью «открытого» ключа.

Современные системы ЭДО имеют встроенные в свои системы, собственноручно разработанные приложения для работы с ЭП, как, например «Астрал.Онлайн». Такой тесной интеграции с ЭП немало способствовал и выход федерального закона “об электронной подписи” (№63–ФЗ от 06.04.2011г.)[3], в котором электронная цифровая подпись была признана имеющий юридическую силу наряду с собственноручной подписью. Согласно законам РФ, свою систему электронной подписи может разрабатывать только компания, имеющая на это соответствующую лицензию ФСБ.

Протоколирование действий пользователей

Это немаловажный пункт в защите электронного документооборота.

В целях безопасности и для соответствия последним правовым нормам любая система электронного документооборота должна вести контрольные журналы, которые отслеживают, кто и к какому документу получил доступ и когда, и какие изменения были внесены при каждом доступе. Действия должен быть проверен ответственным лицом. Усовершенствованные системы электронного документооборота обычно включают функцию трассировки, которая хранит все операции, выполненные с документом.[4]

Его правильная реализация в системе позволит отследить все неправомерные действия и найти виновника, а при оперативном вмешательстве даже пресечь попытку неправомерных или наносящих вред действий. Такая возможность обязательно должна присутствовать в самой СЭД. Кроме того, дополнительно можно воспользоваться решениями сторонних разработчиков и партнеров, чьи продукты интегрированы с СЭД. Говоря о партнерских решениях, прежде всего речь идет о СУБД и хранилищах данных, любой подобный продукт крупных разработчиков, таких как Microsoft или Oracle, наделен этими средствами. Также не стоит забывать о возможностях операционных систем по протоколированию действий пользователей и решениях сторонних разработчиков в этой области.

Зачем доверять электронному документообороту

С помощью ЭДО вы можете с уверенностью заменить свои шкафы с документами на что-то более безопасное: централизованное хранилище, где вы можете хранить, управлять и направлять всю важную деловую информацию. Вы можете хранить свою систему ЭДО локально или хранить ее в облаке. В любом случае это безопасно.

ЭДО помогает обеспечить безопасность документов и совместимость бизнеса с внешними и внутренними правилами ведения бизнеса. Возможность аудита документов имеет решающее значение для обеспечения безопасной и бесперебойной работы, а благодаря ЭДО есть четкий журнал каждого действия, касающегося любого документа. Существует возможность сканировать существующие бумажные документы или импортировать существующие цифровые файлы, а также создавать новые цифровые формы, которые обеспечивают выполнение бизнес-логики и автоматизированный сбор данных, гарантируя, что информация будет доставлена правильно с первого раза.

Список литературы

[1]. *https*://www.audit-it.ru/terms/agreements/edo_elektronnyy_dokumentooborot

[2]. *https*://habr.com/ru/post/188096/

[3]. *http*://www.consultant.ru/document/cons_doc_LAW_112701/

[4]. *https*://www.docpath.com/art-secure-document-management-system/

Щеголихин Сергей Станиславович - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: sergey.schegolihin@gmail.com

А.А. Шабанов

К ВОПРОСУ РАЗРАБОТКИ КРИТЕРИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ ПРИНИМАЕМЫХ В ФИЛИАЛАХ КРУПНЫХ КОМПАНИЙ НА ПРИМЕРЕ ПРЕДПРИЯТИЙ АВТОМОБИЛЕСТРОИТЕЛЬНОГО КЛАСТЕРА КАЛУЖСКОЙ ОБЛАСТИ

Аннотация. Приводится классификация корпораций. Описываются особенности предприятий автомобилестроительного кластера принадлежащих транснациональным корпорациям. Описывается стандартизация управленческого решения. Вводится экономический критерий эффективности управленческого решения. Объясняется эффективность использования разработанного критерия в условиях глобальных корпораций, имеющих большое количество филиалов в разных странах.

По одной из классификаций все корпорации разделяются на национальные и транснациональные, а транснациональные, в свою очередь, на интернациональные, многонациональные (мультинациональные) и глобальные корпорации. Все эти четыре вида корпораций отражают в действительности этапы их развития: от национальной к интернациональной компании, от интернациональной к многонациональной и от последней к глобальной корпорации [1]. Одной из задач глобальных корпораций является обеспечение успешного и прогнозируемого функционирования филиалов в различных точках мира без вмешательства из центра, т.е. избегая так называемого «ручного управления».

Предприятия автомобильного кластера Калужской области принадлежат к типу глобальных корпораций. Такие корпорации интегрирует воедино хозяйственную деятельность, осуществляемую в разных странах. Подобная компания проектирует изделие или схему оказания услуг применительно к определенному сегменту мирового рынка либо в разных странах производит составные части одного изделия [1].

Как правило, практически все предприятия автомобилестроительного кластера принадлежат компаниям, представляющим транснациональные корпорации (ТНК). Большое влияние на расширение практики создания таких предприятий оказывает соответствующая правительственная политика стран-импортеров, в которых при создании таких предприятий предоставляются различные льготы. Практически все предприятия автомобилестроительного кластера Калужской области в настоящее время частично или полностью принадлежат иностранному капиталу.

Для привлечения необходимых капиталов развивающиеся страны вводят ряд льгот для иностранных компаний, строящих в них предприятия, в частности, отменяют полностью или частично таможенные пошлины и налоги на ввоз оборудования и материалов для таких предприятий. Наряду с этим ограничивается импорт готовой продукции, аналогичной той, которую будут вы-

пускать создаваемые предприятия, также для подобных предприятий часто устанавливаются налоговые льготы на определенный период работы [2].

В работе предприятия автомобилестроительного кластера большую роль играет человеческий фактор, что также влияет на процесс управления. Так как в силу специфики рынка труда, в отличие от западных государств, где широкое применение имеют различные полностью роботизированные и автоматизированные системы, в России, на данный момент, многие операции все еще выполняются вручную оператором, хотя и с частым применением автоматизированных систем.

Другой особенностью предприятий автомобилестроительного кластера является найм персонала часто без достаточного бэкграунда в данной области. Однако за счет применения отработанных программ обучения и наставничества через короткое время компания получает достаточно квалифицированного в своей области специалиста, способного успешно выполнять требуемые задачи. Для автомобилестроительных предприятий принадлежащих ТНК, большое значение имеет работа в команде. Результаты исследований говорят о том, что если выполнение задачи требует разносторонних навыков, разных мнений и опыта, то команда работает с большей эффективностью, чем отдельный человек. Недостаток начальной квалификации агента также может быть успешно компенсирован эффективным обучением как на его собственном, так и чужом опыте (что имеет место при командной работе) [3].

На автомобилестроительных предприятиях транснациональных компаний большое внимание уделяется стандартизации рабочих процессов, регламентированию как можно большего количества действий исполнителя, для достижения требуемого результата вне зависимости от начальной квалификации сотрудника. Подобную стандартизацию можно применить и в вопросе согласования управленческого решения, оно должно находиться в пределах, определенных по критерию эффективности.

Задача состоит в стандартизации управленческого решения и его по возможности количественном выражении. Повышение уровня стандартизации управленческих решений позволяет повысить прогнозируемость результатов достигаемых филиалом. В условиях большого количества предприятий-филиалов в разных странах с разными уровнями подготовки менеджеров прогнозируемость результатов предприятий на местах, является важной задачей для центральной штаб-квартиры. Не обязательно выбираемое менеджером из альтернатив решение будет наилучшим, но оно должно быть достаточно эффективным и, за счет близости к корпоративному стандарту принятия решений прогнозируемым для центра.

Используя терминологию управления в организационных системах [3] штаб-квартира компании является центром, менеджмент филиала является агентом, а объектом являются управляемые менеджментом технические и социально-экономические системы предприятия.

Управленческое решение может быть признано эффективным и согласованным вышестоящей инстанцией, если его стоимость будет находиться в

определенных заранее центром пределах. Пределы выражаются минимальной и максимальной разрешенной стоимостью производимого объектом действия, наступающего после принятия агентом решения. Пределы устанавливаются центром на основе анализа подобных действий на уже существующих предприятиях компании. Следует отметить, что организационная структура предприятий автомобилестроительного кластера занимающихся одинаковой деятельностью, но расположенных в разных странах, практически ничем друг от друга не отличается. За счет большого количества очень похожих предприятий, успешно существующих в течение длительного времени, можно получить достаточно большую выборку решений и проанализировать их эффективность.

Вводя верхний и нижний пределы, центр заранее страхует себя от принятия неверного решения агентом. Например, если агент считает нужным закупить более дешевое оборудование, только что вышедшей на рынок фирмы. В этом случае есть вероятность, что компания сэкономит и получит работоспособное решение, затратив меньшие финансовые ресурсы, однако с другой стороны есть риск, что данное решение окажется «сырым» и не обеспечит в долгосрочной перспективе успех компании. Учитывая, что корпорация имеет десятки филиалов по всему миру, уследить за каждым очень сложно, да и в этом нет необходимости. Вводя критерий минимальной разрешенной стоимости компания заранее страхует себя от принятия совсем «дешевого» решения, которое может быть в отдельном случае было бы очень эффективным, но принимая во внимание эффект масштаба, - наличие большого количества филиалов в разных странах и менеджмент с разным менталитетом и уровнем подготовки, вряд ли было бы эффективным во всех случаях.

Максимальная разрешенная стоимость в свою очередь является страховкой компании от слишком больших потерь в случае принятия неправильного решения, в том числе в результате злоупотребления агента. Данный вариант возможен, в том числе, и из-за достаточно высокого уровня коррупции, имеющего место в ряде развивающихся стран. Максимальная разрешенная стоимость – эта та величина финансовых затрат, которыми компания готова рисковать при принятии агентом того или иного управленческого решения. В идеале стоимость подобных возможных неудачных решений может быть заранее заложена в стоимость продукции, чтобы предотвратить непрогнозируемые потери.

На этапе согласования решение проходит количественную оценку на основании принятых в каждом отдельном рассматриваемом вопросе пределов – максимальной и минимальной разрешенной стоимости. Применение вышеописанного экономического критерия выбора удовлетворительного варианта решения позволит любому менеджеру, вне зависимости от квалификации и опыта работы принять рациональное и приемлемое для компании решение.

Список литературы

[1]. *Шагурин С.В., Шимко П.Д.* Экономика транснационального предприятия: Учебное пособие. – СПб.: СПбГПУ, 2008. – 335 с.

[2]. *Гольдштейн Г.Я.* Основы менеджмента: Учебное пособие, изд 2-е, дополненное и переработанное. – Таганрог: Изд-во ТРТУ, 2003.

[3]. *Новиков Д.А.* Теория управления организационными системами. 3-е изд., испр. и дополн. – М.: Издательство физико-математической литературы, 2012. – 604 с.

Шабанов Алексей Александрович - руководитель технологической группы АО БВТ БАРЬЕР РУС. E-mail: shabanov.aa86@gmail.com

А.А. Чураков Е.А. Черепков

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ГРАЖДАН

Деятельность любой российской компании, сегодня связана с хранением и обработкой персональных данных различных категорий, к защите которых законодательством РФ выдвигается ряд требований. [1] Для их выполнения руководство компании, прежде всего, сталкивается с необходимостью формирования модели угроз персональным данным и разработки на ее основе системы защиты персональных данных, в состав которой должно входить средство криптографической защиты информации. Основным инструментом для этого служит средство криптографической защиты информации (СКЗИ), внедренному в систему защиты персональных данных, к которой выдвигаются следующие требования:

- Криптографическое средство должно штатно функционировать совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к нему требований. [2]
- Для обеспечения безопасности персональных данных при их обработке должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства. [2]

Внедрение криптосредств в системы защиты персональных данных

Внедрение криптосредства того или иного класса с систему защиты обуславливается категорией нарушителя (субъекта атаки), которая определяется оператором в модели угроз. Выделяется 6 основных типов нарушителей: Н1, Н2, Н3, Н4, Н5, Н6. Каждый следующий тип имеет более обширные возможности, нарушитель каждого следующего типа наследует возможности предыдущего. Криптографическое средство, в зависимости от обеспечиваемого им уровня защиты, может быть отнесено к одному из шести классов (КС1, КС2, КС3, КВ1, КВ2, КА1). Информационная система персональных данных (ИСПДн) также разделяются на 6 классов, в зависимости от наивысшей категории нарушителя. АК1- если наивысшая категория нарушителя Н1, АК2- если Н2, АК3 — если Н3, АК4 — если Н4, АК5 — если Н5, АК6 — если Н6. Соответственно распределены средства криптозащиты: АК1 — КС1, АК2 — КС2, АК3 — КС3, АК4 — КВ1, АК5 — КВ2, АК6 — КА1. Таким образом, средства криптографической защиты сегодня эффективно используются различными компаниями и организациями для защиты персональных данных российских граждан и являются одной из наиболее важных составляющих в системах защиты персональных данных.

На сегодняшний день для эффективного применения в корпоративной среде, программа для шифрования должна обеспечивать:

- шифрование данных на удаленном сервере;
- поддержку асимметричной криптографии;
- прозрачное шифрование;

• шифрование сетевых папок;

• возможность разграничения прав доступа к конфиденциальной информации между сотрудниками компании;

• возможность хранения сотрудниками закрытых ключей на внешних носителях информации (токенах).

Применение СКЗИ

Однако, при использовании СКЗИ, следует учитывать несколько аспектов. Во-первых, это стойкость криптографических алгоритмов и протоколов. Стандартизованные по ГОСТ алгоритмы и рекомендованные протоколы гарантируют обеспечение соответствующей криптографической стойкости. По мнению специалистов [3], лобовые атаки на сертифицированные алгоритмы и попытки их взлома можно в принципе исключить как угрозу на данном этапе. И пока еще нет достаточных вычислительных мощностей, чтобы решить заложенные в криптографические алгоритмы математические задачи. При этом криптографическая наука совершенствуется одновременно с IT-сферой.

Во-вторых, безопасность использования криптографии зависит от надежности реализации СКЗИ. Система лицензирования разработчиков СКЗИ и система оценки компетентными экспертами созданных СКЗИ гарантируют минимизацию рисков, связанных с потенциальными уязвимостями в самих СКЗИ. Риск, связанный с реализацией СКЗИ, существует, поскольку реализация может быть разной. Например, предустановленное в Windows ПО СКЗИ, его реализация основана на зарубежных криптоалгоритмах. Известно, что достаточно часто происходят успешные атаки на реализации западных криптографических алгоритмов, в том числе, используемые в России. Сертифицированные СКЗИ проверены экспертами, оценены их надежность, определены реализация (что в нем ничего не задокументированного нет), но также проверены и выработаны обязательные условия внедрения этого СКЗИ.

В-третьих, критически важно обеспечить безопасную эксплуатацию информационной системы с СКЗИ. Никакая система не может считаться защищенной, если ее неправильно эксплуатировать. В первую очередь злоумышленники ищут уязвимости в реализации информационной системы с СКЗИ и пытаются воспользоваться ошибками при эксплуатации СКЗИ. Поэтому требуется точно соблюдать установленный регламент при смене ключей, паролей к ключевым контейнерам, ограничивать доступ в помещения. Несоблюдение всех этих требований существенно повышает риски.

Еще один важный момент – прикладные системы, куда встроены СКЗИ. Их стойкость в плане информационной безопасности практически никем не регламентируется и их создание не контролируется. А там могут быть свои уязвимости. Учитывать эти векторы атак на конфиденциальную информацию тоже необходимо. В банковской сфере проводятся тематические исследования с получением заключения у экспертов ФСБ России. [4]

Для большинства компаний электронная почта является основным средством коммуникации между сотрудниками, именно поэтому очень важна и

защита корпоративной почты. Большинство почтовых клиентов, таких как «Outlook», «Thinderbird», «The Bat!» и др., позволяют настроить обмен зашифрованными сообщениями на основе сертификатов открытого и закрытого ключа (сертификаты в форматах X.509 и PKCS#12 соответственно) (алгоритмы RSA шифрования), создаваемых при помощи средств криптографической защиты.

Каждая компания обязана хранить данные его клиентов и защищать их, вследствие этого, сертифицированные криптографические средства стали неотъемлемой частью этих компаний. Они постоянно совершенствуются и не отстают от развития всей IT-сферы, что делает их надежными, и не позволяет злоумышленникам похитить данные.

Список литературы

[1] *Федеральный* закон "О персональных данных" от 27.07.2006 N 152-ФЗ URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 01.10.2019).

[2] *Методические* рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности – Утверждены руководством 8 Центра ФСБ России, 31 марта 2015 года, № 149/7/2/6-432 URL: http://www.consultant.ru/document/cons_doc_LAW_185051/ (дата обращения 01.10.2019).

[3] *Криптография* как зеркало российской экономики URL: https://safe-surf.ru/specialists/article/5235/610386/ (дата обращения 01.10.2019).

[4] *Перечень* средств защиты информации, сертифицированных ФСБ России. URL: http://clsz.fsb.ru/certification.htm (дата обращения 01.10.2019).

Чураков Александр Александрович - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: jumandj@yandex.ru

Черепков Евгений Александрович - преподаватель КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: e.cherepkov@yandex.ru

С.Е. Липатова, Е.А. Черепков, Ю.С. Белов

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ДАННЫХ НА ОСНОВЕ ТЕХНОЛОГИИ BLOCKCHAIN

Введение. В современном мире происходит всё большее развитие технологий, способных не просто значительно упростить жизнь пользователям, но и готовых обеспечить максимальную степень защиты данных. Одной из таких технологий является технология Blockchain, ставшая на этапе появления основой криптовалют.

Создание технологии Blockchain. Первые идеи создания Blockchain были описаны еще в 1991 году учеными-исследователями Стюартом Хабером и У. Скоттом Шторнеттом, внедрившими вычислительно-практическое решение для цифровых документов со штампом времени во избежание подделок документов. Система, описанная ими, использовала криптографическую закрепленную цепочку блоков для хранения документов с отметкой времени. В 1992 году в разработку с целью повышения эффективности были включены деревья Меркла. Система стала оптимальнее, сумела объединить несколько документов в один блок. Однако данная технология не заполучила должного внимания, и патент на нее был упущен в 2004 году. Спустя четыре года была создана сеть Bitcoin, основой которого стала нынешняя технология Blockchain [1].

В настоящее время Blockchain является цифровой и распределенной бухгалтерской книгой операций, записанной и реплицированной в реальное время через сеть компьютеров или узлов. Каждая транзакция должна быть криптографически проверена с помощью механизма консенсуса, выполняемого узлами, прежде чем она будет окончательно добавлена в качестве нового «блока» в конце «цепочки». Нет необходимости в центральном органе для утверждения транзакции, поэтому Blockchain иногда называют одноранговым механизмом доверия [2]. Каждый из узлов хранит полную, обновленную (актуальную) версию Blockchain. Таким образом, одноранговая сеть (рис.1) более надежна, нежели серверная (рис.2).

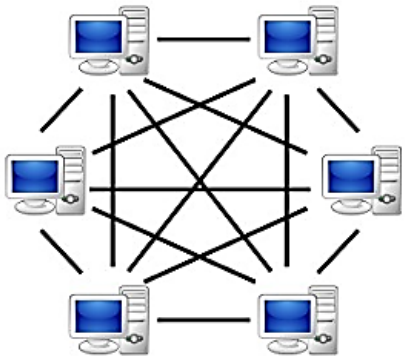


Рис. 1. Одноранговая сеть

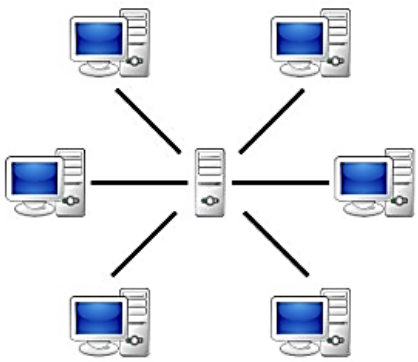


Рис.2. Серверная структура

Использование одноранговой сети с точки зрения безопасности имеет определенные преимущества, ведь нам не надо полагаться на безопасность одного сервера, чтобы знать, что Blockchain защищен. К тому же, при попытке взлома придется одновременно взломать тысячи компьютеров, а не один сервер, и всегда есть уверенность, что Blockchain никогда не исчезнет, потому что для этого его надо будет уничтожить всем узлам.

Механизм консенсуса. Однако для обеспечения безопасности транзакций использования одноранговой сети недостаточно. Например, как узнать, что все транзакции в Blockchain верны? Как узнать, что в блоках нет недействительных транзакций? И если есть разные версии Blockchain, откуда мы узнаем, которые из них являются истинными?

Все эти опасения весьма изобретательно решаются консенсусным механизмом, использование которого стало возможным, в первую очередь, благодаря одноранговой сети. Механизм консенсуса отвечает за поддержание целостности и безопасности распределенных систем, что особенно важно при работе криптовалютной сети. Но почему?

Публичные Blockchain построены как распределенные системы, и поскольку они не полагаются на центральные органы, распределенные узлы должны согласовывать валидацию транзакции. Именно здесь вступают в силу алгоритмы консенсуса, уверяющие, что соблюдаются правила протокола, и гарантирующие, что все транзакции происходят доверенным способом, поэтому монеты могут быть потрачены только один раз. Важно не путать понятия «протокол» и «алгоритм»: под протоколом подразумеваются первичные правила Blockchain, а под алгоритмом - механизм, с помощью которого они будут выполняться.

Таким образом, протокол будет определять способы взаимодействия узлов и передачи данных между ними, а так же требования к успешной проверке (валидации) блока. С другой стороны, алгоритм консенсуса отвечает за проверку балансов и подписей, подтверждение транзакций и фактическое выполнение проверки блоков, и все это зависит от консенсуса сети. В случае попытки одновременной записи нескольких блоков в Blockchain, все консенсусные протоколы решают эту проблему с помощью простого правила: выигрывают самые длинные цепочки. При этом основной цепочке не будет нанесен ущерб.

Существует несколько типов алгоритмов консенсуса, среди которых наиболее известны Proof of Work (PoW) и Proof of Stake **(**PoS). У каждого есть свои преимущества и недостатки при попытке сбалансирования безопасности с функциональностью и масштабируемостью. Алгоритм консенсуса Proof of Work считается одним из лучших решений Проблем Византийских Генералов, что позволило создать криптосистему Bitcoin как систему их решения с устойчивостью к атакам, таким как атака 51% (атака большинства). Таким образом, согласие на текущее состояние Blockchain, имеет большое значение для правильной работы цифровой экономической системы.

Защищённость технологии Blockchain обеспечивается так же и криптографическими ключами, рассчитывающимися специальными хэш-алгоритмами. Ключ обладает значимыми свойствами: владея ключом, нельзя узнать исходный набор данных и найти другой набор данных, дающий такой же ключ, нереально.

Применение технологии. Существует три уровня использования Blockchain:

- хранение цифровых записей;
- обмен цифровыми активами;
- запись и выполнение смарт-контрактов [2].

Данные уровни использую операции хранения и обмена данных, представленных в цифровом виде. В связи с этим важно обеспечить безопасность информации, а так же организовать транзакции таким образом, чтобы значительно сократить возможность стороннего вмешательства, способного вызвать ошибки и мошенничество. В связи с этим преимуществом технологии Blockchain является возможность выполнения одноранговых транзакции без доверенных сторонних посредников, тем самым сокращая время клиринга и расчетов и связанные с этим расходы.

Важно упомянуть и о смарт-контрактах – цифровых кодах, позволяющих автоматически выполнять определенные действия на основе договорных условий, утвержденных всеми сторонами. Они включают в себя и «умные» договоры аренды и кредита, включающие в себя арендные платежи и право собственности на активы в случае дефолта соответственно. Таким образом, смарт-контракты могут не только выполнять повторяющиеся бизнес-операции, но и потенциально могут помочь уменьшить конкретные значения по умолчанию. Записанные в Blockchain смарт-контракты являются неизменяемым, поэтому требуют высококачественный код, способный значительно снизить риск ошибок и мошенничества [2]. Например, двум деловым сторонам, участвующим в сделке, не потребуется вести собственный учет транзакции, и вместо этого они будут использовать Blockchain в качестве единственного источника правды. Это способствует повышению доверия между участниками транзакций, что становится всё сложнее и дороже в условиях роста глобализации и оцифровки данных. К тому же, с целью контроля транзакций непосредственная реализация технологии Blockchain классифицируется на два типа: публичный (любой человек моет подтвердить транзакцию) и разрешенный (доступен только предварительно одобренным сторонам).

Таким образом, «Умные контракты» с внешними сторонами, включенные в Blockchain, могут быть частично или полностью выполнены и реализованы с минимальным человеческим взаимодействием, что позволяет повысить эффективность. Прозрачность в событиях, которые обеспечивает Blockchain - выполнение видимых действий во всем расширенном предприятии - может оказать существенное влияние на эффективность ERM (с англ. - управление рисками предприятия) [3].

Развитие Blockchain в сферах общественной жизни. Blockchain играет важную роль не только в криптовалютных сетях и экономическом взаимодействии сторон. В наше время данная технология стала настолько распространенной, что нашла применение в телекоммуникациях, медиа, развлечениях, медицине и других сферах жизни общества. Так, Blockchain может помочь компаниям повысить безопасность пользователей, устройств, контента и учетных записей. Транзакции, хранящиеся в цепочке блоков, зашифрованы, с отметкой времени и синхронизированы по всей сети. Аналогично, идентификационные данные действующих сторон и устройств криптографически уникальны и зарегистрированы в Blockchain. В сфере здравоохранения вопрос управления информацией очень актуален. Медицинские работники ежедневно работают с данными, которые требуют осторожного обращения, анонимности, верной передачи информации. Это также требует особых правил касательно предоставления доступа к медицинским данным, особого алгоритма управления правами, разработку единых стандартов при внесении и работе с большим объемом информации [3]. Именно поэтому многие компании и разработчики предлагают решения на основе технологии Blockchain для работы с большими объемами распределенной информации.

Заключение. Развитие технологии Blockchain является перспективным направлением разработки. Обеспечивая защиту данных на высоком уровне, технология способна не просто уменьшить количество споров, случаев мошенничества, защитить активы и управлять их происхождением, сократить расходы и модернизировать учет и платежи, но и стать основой для действительно сетевой цифровой экономики. В будущем она может быть применена для цифровой идентификации, автоматизации IoT, сетевых услуг следующего поколения и комплексного управления правами на контент, лицензионными платежами и рекламой, а на более высоком уровне Blockchain может предложить целым сетям возможность реагировать на события и более эффективно управлять собой. Технология постепенно внедряется в различные сферы, становясь для современного общества обыденностью, способной значительно упростить жизнь людей, повысить качество жизни населения.

Список литературы

[1] *История* Blockchain. URL: https://www.binance.vision/ru/blockchain/history-of-blockchain (дата обращения 23.10.2019).

[2] *Piscini E., Cotteleer M., Holdowsky J.* Blockchain: A technical primer. URL: https://www2.deloitte.com/us/en/insights/topics/emerging-technologies/blockchain-technical-primer.html?icid=dcom_promo_featured|us;en (дата обращения 24.10.2019).

[3] *Kinsella D., Kambil A., Dr. Sanjoy Sen, Singh C.P. Resetting the front line of defens*e. URL: https://www2.deloitte.com/us/en/insights/topics/risk-management/extended-enterprise-risk-management.html (дата обращения 27.10.2019).

Липатова Софья Евгеньевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: sonya_lipatova@list.ru

Черепков Евгений Александрович - преподаватель КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: e.cherepkov@yandex.ru

Белов Юрий Сергеевич - доцент, канд. физ.-мат. наук КФ МГТУ им. Н.Э. Баумана. E-mail: iu4-kf@mail.ru

С.А. Медведева, П.В. Фролов, Мазин А.В., Е.В. Вершинин

ОБЗОР ИССЛЕДОВАНИЙ ПО АНАЛИЗУ СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ МЕТОДОВ

В настоящее время большое значение имеют задачи исследования и разработки методов обеспечения информационной безопасности. Активно решаются задачи, связанные с защитой от компьютерных угроз и атак, для борьбы с которыми постоянно совершенствуются существующие и создаются новые системы обнаружения вторжений (СОВ, Intrusion Detection System – IDS).

Все подобные системы имеют сложную структуру и основаны на специальных алгоритмах (методах), позволяющие идентифицировать различные атаки на информационную систему (ИС). Каждая система использует различные методы обнаружения.

Все исследования в рамках данной темы направлены на поиск наиболее эффективного способа работы подобных систем. Как правило, исследуется архитектура систем и применяемые алгоритмы. Для оценки алгоритмов, в свою очередь, выделяют различные численные показатели эффективности.

Существует большое число классификаций систем обнаружения вторжений. И в разных работах можно встретить разные принципы разделения систем на группы. Наиболее распространенная классификация встречается в работе Шелухина О.И. [1]. Автор делит системы на две группы:

1. системы для мониторинга конкретного узла в сети;
2. системы, производящие мониторинг всей сети.

Системы первой группы, как правило, собирают информацию из журналов регистрации ОС и приложений (веб-сервисов, СУБД и т.д.).

Системы второй группы собирают информацию из сетевого трафика. Такие системы производят мониторинг сетевого трафика в режиме реального времени.

Кроме того, в данной работе можно встретить другие классификации СОВ. Как и все программное обеспечение (ПО), IDS можно классифицировать по архитектуре. Система может быть централизованной, т. е. располагаться на одной рабочей машине, и распределенной, т. е. состоящей из нескольких элементов, которые могут быть разнесены по сети и обладать определенной зоной ответственности.

Также Шелухин О.И. разделяет системы по способу реагирования на аномалию: пассивные, которые ведут запись в журнал и оповещают администратора, и активные, которые кроме всего прочего могут отклонять аномальный трафик.

Кроме того, в работе встречаются следующие классификации.

По подходу обнаружения вторжений:

1. обнаружение аномалий;
2. обнаружение злоупотреблений.

По источнику данных:

1. записи о транзакциях, выполняемых в системе;

2. сетевые пакеты;

3. анализ состояния системы (ядро, службы, файлы).

Как правило, большинство систем являются активными, распределенными и анализируют весь сегмент сети. Но основной частью каждой системы является метод (алгоритм) обнаружения аномалий.

Климов С.М. в своей работе [2] разделяет алгоритмы на две основные группы:

1. методы анализа сигнатур;

2. методы обнаружения аномальных отклонений.

Методы анализа сигнатур предназначены для обнаружения известных атак и основаны на контроле программ и данных в критически важной информационной системе (КВИС).

Методы обнаружения аномальных отклонений предназначены для обнаружения неизвестных атак. Принцип их действия состоит в том, что выявляется аномальное поведение КВИС отличное от типичного и на основании этого факта принимается решение о возможном наличии атаки.

В различных источниках, предлагающих подходы по решению задач информационной безопасности, описывается применение разных методов обнаружения. К примеру, в работе Тишиной Н.А. [3] предлагается обнаружение вторжений на основе вейвлет-анализа сетевого трафика. В работе Арустамова С.А. [4] предлагается применить байесовский метод. Каменев А.В. в своей работе [5] использует модель иммунной системы.

Описываемые выше алгоритмы, а также другие, незатронутые в данной работе, имеют свои преимущества и недостатки. Каждый из методов лучше или хуже подходит для идентификации определенного типа атак.

Стоит заметить, что во всех предлагаемых решениях для обнаружения угроз применяется один конкретный метод, т. е. один метод применяется к отдельной последовательности пакетов, к которой не применяется больше никакой из других методов обнаружения.

Исследуя данные подходы можно сделать следующие выводы:

- Предлагаемые решения не могут учесть все признаки вторжений, соответствующие разным уровням эталонной модели ISO/OSI и различным сетевым протоколам. Это следует из того, что различные типы атак могут проходить на разных уровнях сетевой модели.
- Большинство методов не исключают возможности ложного срабатывания системы, и большинство из них используют готовые шаблоны для обнаружения аномалий. Кроме того, они не предполагают возможности идентификации новых видов атак.
- Также стоит заметить, что, применяя отдельный метод для обнаружения вторжений, нет никаких гарантий, что действительно применяемый метод подходит для атак данного типа. Существует большое количество видов атак, и все они отличаются по различным характеристикам: длительности, способу, масштабности и пр.

В одной из работ на данную тематику Браницким А.А. [6] предлагается использование комбинации нейронных, иммунных и нейронечетких классификаторов. Данный подход предполагает решение ряда указанных недостатков, однако в работе не учитывается применение этих подходов для различных уровней модели ISO/OSI, что является существенным минусом.

Таким образом, можно сделать вывод о перспективных направлениях исследования моделирования системы, которая бы позволяла избавиться от большинства перечисленных недостатков.

Моделируемая система должна быстро и эффективно обрабатывать входную последовательность данных, используя преимущества каждого метода обнаружения.

Для получения более объективных результатов анализа сетевого трафика следует пытаться применить для различных уровней пакетов данных комбинацию методов анализа, т. е. не стоит останавливаться на одном конкретном методе, производящем мониторинг на определенном уровне модели. Данный подход поможет в проблеме, при которой нельзя классифицировать несколько разных типов атак.

Кроме того, исследуемый подход поможет снизить вероятность ложных срабатываний при анализе сети, так как можно комбинировать и анализировать информацию, полученную в результате работы различных алгоритмов на нескольких уровнях модели сети.

В существующих работах не проводятся исследования о возможности обнаружения неизвестных атак. Такую возможность можно предусмотреть при применении самообучающихся алгоритмов.

Список литературы

[1] *Шелухин О.И., Сакалема Д.Ж., Филинова А.С.* Обнаружение вторжений в компьютерные сети (сетевые аномалии). Москва, Горячая линия — Телеком, 2013, 220 с.

[2] *Климов С.М., Сычев М.П., Астрахов А.В.* Противодействие компьютерным атакам. Методические основы: Электронное учебное издание. - М.: МГТУ имени Н.Э. Баумана, 2013, 108с.

[3] *Тишина Н. А., Дворовой И. Г., Соловьев Н. А.*. Обнаружение вторжений на основе вейвлет-анализа сетевого трафика. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp?id=18861585 (дата обращения: 15.10.2019).

[4] *Арустамов С.А., Дайнеко В.Ю.* Применение динамической байесовской сети в системах обнаружения вторжений. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/v/primenenie-dinamicheskoy-bayesovskoy-seti-v-sistemah-obnaruzheniya-vtorzheniy (дата обращения: 23.10.2019).

[5] *Каменев А.В., Киселев А.А.* Обзор применения искусственных иммунных систем в системах обнаружения вторжений. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp?id=21415194 (дата обращения: 23.10.2019).

[6] *Браницкий А.А., Котенко И.В.* Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов.

[Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/obnaruzhenie-setevyh-atak-na-osnove-kompleksirovaniya-neyronnyh-immunnyh-i-neyronechetkih-klassifikatorov (дата обращения: 24.10.2019).

Медведева Светлана Александровна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: svetlana_medvedeva_1997@mail.ru

Фролов Павел Валерьевич - ассистент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: Han-92@mail.ru

Мазин Анатолий Викторович - заведующий кафедрой «Защита информации», доктор техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: mazinav@yandex.ru

Вершинин Евгений Владимирович - заведующий кафедрой «Системы обработки информации», кандидат физико-математических наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: yevgeniyv@mail.ru

М.Д. Гущина

ОБЗОР МЕТОДОВ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА

Современному человеку свойственно оперировать информацией во всех ее проявлениях и форматах. Одним из них является работа с электронными файлами.

Отказ от бумажных носителей носит все более глобальный характер, т.к. позволяет в значительной степени экономить ресурсы, рационализировать затраты на ведение учета и упрощает хранение информации. Наряду с этим, все большее значение приобретают системы электронного документооборота, способные передавать большое количество электронных файлов конечному получателю.

Социальные сети, мессенджеры и электронная почта. Электронная почта уже достаточно давно позволяет обмениваться не только сообщениями, но и документами. Однако, в настоящее время она все более уступает свои позиции большинству социальных сетей и популярных мессенджеров, имеющих более обширный функционал.

Передача файлов и документов по таким каналам является простейшим документооборотом, однако, подходит для передачи лишь общедоступных документов и сведений.

Файлообменники. Для обычного обмена информацией вполне достаточно использовать простые файловые обменники, в том числе популярные сегодня облачные сервисы.

Работа таких сервисов заключается в том, чтобы предоставить пользователю возможность загружать на них файлы, доступ к которым можно получить по сгенерированной ссылке или напрямую поделиться ими с пользователями данного сервиса. [1]

Такие порталы позволяют оперативно управлять доступом к документам, однако не защищают от несанкционированного копирования и дальнейшего распространения. В данных каналах возможна частичная передача конфиденциальной информации.

Физическая передача электронных носителей. Этот вид передачи является наиболее безопасным, т.к. электронные файлы хранятся только на носителях. Существуют специальные методы защиты содержимого носителей, что позволяет предотвратить несанкционированный доступ при утере. [2]

В данном канале можно обмениваться информацией любого вида, однако, главный недостаток такого подхода – необходимость физического контакта отправителя и получателя.

Электронный документооборот на основе подписи сертификатами. Появление ассиметричного шифрования привело к созданию электронных сертификатов, предоставивших большой функционал в области электронного документооборота.

Цифровой сертификат – выпущенный удостоверяющим центром акт, подтверждающий принадлежность владельцу указанного открытого ключа или каких-либо атрибутов. Т.е. сертификат является электронным документом, подтверждающим личность. [3]

Требования к сертификатам, удостоверяющим центрам и процессам взаимодействия удостоверяющих центров, граждан и государства закреплены в законодательстве и имеют юридическую силу.

Выпустив сертификат, пользователь имеет два ключа шифрования – закрытый (известный лишь ему) и открытый (известный участникам документооборота). Зашифровав файлы или документы своим закрытым ключом, владелец сертификата отправляет зашифрованные данные получателю. Приняв данные, получатель расшифровывает их, используя открытый ключ отправителя, тем самым подтверждается, что полученные данные принадлежат отправителю, т.к. только он имеет закрытый ключ. [4]

Таким образом, процесс документооборота с использованием цифровых сертификатов выполняет сразу несколько функций: защита конфиденциальной информации и удостоверение отправителя. В настоящее время существует большое количество сервисов, позволяющее автоматизировать все описанные процессы.

Однако, открытый ключ не является чем-то секретным и его довольно легко получить. Например, он может остаться от предыдущих документооборотов или может быть опубликован удостоверяющим центром или самим владельцем. В данном случае ставится под сомнение выполнение функции защиты конфиденциальной информации. Для решения данной проблемы необходимо либо выпускать сертификат для каждого документооборота, либо строго контролировать публикацию открытого ключа.

Данный канал передачи подходит для обмена конфиденциальной информацией, однако, для работы с информацией ограниченного доступа требуется соблюдать дополнительные меры безопасности. В остальном, электронный документооборот с использованием цифровых сертификатов больше подходит для подтверждения личности отправителя и получателя. [5]

Электронный документооборот с использованием симметричного шифрования на основе выработанного общего ключа. Данный подход решает ограничение цифровых сертификатов на количество доступных ключей шифрования. Решение заключается в том, что для каждого документооборота его участники будут генерировать общий ключ на основе имеющихся у них сертификатов, а затем при помощи данного ключа зашифровывать симметричными алгоритмами документы и файлы, передавая их друг другу.

Таким образом, для каждого документооборота будет сгенерирован свой ключ шифрования, что полностью обезопасит передачу любых файлов и документов.

Заключение. Рассмотренные каналы обмена информацией широко распространены в современном мире, однако, использование каждого из них накладывает ограничения на передачу конфиденциальных данных.

Список литературы

[1] *Организация* и технология документационного обеспечения управления / сост. С.Е. Мишенин; – Кемерово: Кемеровский государственный университет, 2017. – 478 с.

[2] *Копылов Ю.Р.* Основы компьютерных цифровых технологий машиностроения: учебник / Ю.Р. Копылов. — Санкт-Петербург: Лань, 2019. — 496 с. — Электронно-библиотечная система «Лань»: [Электронный ресурс]. — URL: https://e.lanbook.com/book/125736 (дата обращения: 15.10.2019).

[3] *Порядина О.В.* Управление информационными ресурсами. Поволжский государственный технологический университет. – Йошкар-Ола: ПГТУ, 2015. – 52 с.: [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book&id=439328 (дата обращения: 16.10.2019).

[4] *Лопатин В.М.* Информатика для инженеров: учебное пособие / В.М. Лопатин. — Санкт-Петербург: Лань, 2019. — 172 с. — Электронно-библиотечная система «Лань»: [Электронный ресурс]. — URL: https://e.lanbook.com/book/115517 (дата обращения: 16.10.2019).

[5] *Конфиденциальное* делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Дёмушкин, Т.В. Кондрашова, А.Г. Фабричнов; 2-е. — Москва: Логос, 2017. — 500 с. Электронно-библиотечная система «Лань»: [Электронный ресурс]. — URL: https://e.lanbook.com/book/126123 (дата обращения: 17.10.2019).

Гущина Мария Дмитриевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: mgusina096@gmail.com

Н.А. Зоринов

ОБЗОР МЕТОДОВ СНИФФИНГА СЕТЕВОГО ТРАФИКА

Задача анализа сетевого трафика приобретает все большую актуальность в связи с развитием и внедрением новых сетевых технологий и, как следствие, увеличением объема данных, передаваемых по сети, а также появлением большого количества новых сетевых протоколов прикладного уровнях [1]. В качестве наиболее популярных областей практического применения можно выделить:

1. Анализ трафика с целью выявления проблем в работе сети (в том числе, несанкционированной активности).
2. Восстановление потоков данных («прослушивание»).
3. Предотвращение различного рода сетевых атак.
4. Сбор статистики.

Если говорить о комплексном решении задачи анализа сетевого трафика, то в первую очередь следует разделить ее на три в достаточной степени независимые подзадачи: перехват трафика, его хранение и анализ.

Система анализа должна обеспечивать захват всего трафика, а также предоставлять эффективные методы анализа и навигации по его результатам. Захват трафика осуществляется посредством снифферов.

Анализатор трафика (сниффер) – программа или устройство для перехвата и анализа сетевого трафика. В рамках конкретных продуктов могут быть реализованы дополнительные возможности, например, разбор заголовков сетевых протоколов, фильтрация по заданным критериям, восстановление сессий [2].

Сниффер может анализировать только то, что проходит через его сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются всем машинам, из-за этого возможно перехватывать чужую информацию. Использование коммутаторов (switch, switch-hub) и их грамотная конфигурация уже является защитой от прослушивания. Между сегментами информация передаётся через коммутаторы [3].

Перехват трафика может осуществляться:

1. Обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы).
2. Подключением сниффера в разрыв канала.
3. Ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер (Network tap).
4. Через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика.
5. Через атаку на канальном (MAC-spoofing) или сетевом уровне (IP-spoofing), приводящую к перенаправлению трафика жертвы или всего

трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

Анализ прошедшего через сниффер трафика позволяет:

1. Обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (снифферы здесь малоэффективны; как правило, для этих целей используют сбор разнообразной статистики серверами и активным сетевым оборудованием и её последующий анализ).

2. Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных снифферов – мониторов сетевой активности).

3. Локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами) [4].

Поскольку в сниффере анализ трафика происходит вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), то он подходит для анализа лишь небольших его объёмов [5].

CommView

CommView – это сетевой монитор и анализатор, разработанный для администраторов локальных сетей, специалистов по безопасности, сетевых программистов, домашних пользователей. CommView обладает множеством удобных для пользователя функций и сочетает в себе производительность и гибкость с простотой использования.

Это приложение захватывает каждый пакет в сети для отображения информации, такой как список пакетов и сетевых подключений, диаграммы распределения протоколов. Доступны функции анализа, сохранения, фильтрации, импорта и экспорта захваченных пакетов, просмотр и декодирование протоколов до самого нижнего уровня с полным анализом. Более 100 поддерживаемых протоколов. С помощью этой информации CommView позволяет определить проблемы с сетью и устранить неполадки программного и аппаратного обеспечения.

CommView включает в себя анализатор VoIP для углубленного анализа, записи и воспроизведения голосовых сообщений SIP и H.323. Для задач удаленного мониторинга существует дополнительное программное обеспечение: *Удаленный агент CommView*. Оно позволяет пользователям CommView перехватывать сетевой трафик на любом компьютере, на котором работает удаленный агент, независимо от физического местоположения компьютера.

Функции сниффера:

1. Поддержка сотен протоколов и добавление новых.
2. Просмотр подробной статистики IP-соединений: IP-адреса, порты, сеансы.

3. Доступные фильтры: по протоколу Ethernet, по протоколу IP, по MAC-адресу, по IP-адресу, по порту, по тексту, по процессу, расширенные логические правила, позволяющие создавать сложные формулы.

4. Генерация отчетов о трафике в режиме реального времени.

5. Форматы отчетов: HTML, CSV, текстовые файлы, растровые файлы.

6. Не кроссплатформенный: Windows.

7. Текущие данные могут быть считаны из Ethernet, Token Ring, IEEE 802.11.

8. Анализ VoIP.

9. Импорт и экспорт пакетов в форматах tcpdump (libpcap), Pcap NG, Network Instruments Observer, Network General Sniffer, Microsoft Network Monitor, WildPackets EtherPeek/AiroPeek.

10. Просмотр захваченных и декодированных пакетов в режиме реального времени.

11. Реконструирование сеанса TCP.

12. Поиск строк или шестнадцатеричных данных в содержимом захваченного пакета.

13. Настройка сигналов тревоги, которые могут уведомлять о важных событиях, таких как подозрительные пакеты, высокая пропускная способность, неизвестные адреса.

14. Создание собственных плагинов для декодирования любого протокола.

15. Обмен данными с пользовательским приложением через TCP/IP.

16. Экспорт любого IP-адреса в SmartWhois для поиска IP.

17. Захват петлевого трафика.

Wireshark

Wireshark – анализатор сетевых протоколов. Развитие Wireshark происходит благодаря добровольному вкладу сетевых экспертов по всему миру и является продолжением проекта, начатого Джеральдом Комбсом в 1998 году.

Функции сниффера:

1. Поддержка 3000 протоколов и добавление новых.

2. Просмотр подробной статистики IP-соединений: IP-адреса, порты, сеансы.

3. Самые мощные фильтры в отрасли.

4. Генерация отчетов о трафике в режиме реального времени.

5. Форматы отчетов: XML, CSV, PostScript, текстовые файлы.

6. Кроссплатформенный: Windows, Linux, macOS, Solaris, FreeBSD, NetBSD.

7. Текущие данные могут быть считаны из Ethernet, IEEE 802.11, Token Ring, PPP/HDLC, ATM, Bluetooth, USB, Frame Relay, FDDI.

8. Анализ VoIP.

9. Импорт и экспорт пакетов в форматах tcpdump (libpcap), Pcap NG, Network Instruments Observer, Network General Sniffer, Microsoft Network Monitor, WildPackets EtherPeek/TokenPeek/AiroPeek, Catapult DCT2000, iplog

Cisco Secure IDS, Sniffer Pro, NetXray, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime.

10. Просмотр захваченных и декодированных пакетов в режиме реального времени.

11. Поддержка расшифровки многих протоколов, включая IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP и WPA/WPA2.

Заключение

В статье были рассмотрены инструменты анализа сетевого трафика: Wireshark, CommView. Для каждого инструмента приведено описание архитектуры, а также основные достоинства и недостатки с точки зрения функциональности и удобства использования. Лидером является Wireshark, так как поддерживает разбор и распознавание более 1000 сетевых протоколов. CommView не обладают поддержкой такого количества протоколов. Кроме того, Wireshark предоставляет пользователю графический интерфейс. В Wireshark отсутствует возможность выполнения некоторого действия в случае обнаружения каких-либо паттернов в трафике. CommView предоставляют функциональность для данного сценария работы. Идеологически Wireshark является средством просмотра и сбора статистики, но не анализа. CommView позиционирует себя как систему обнаружения вторжений – отсюда архитектурное решение в пользу модели событий.

Ни один из них не позволяет эффективно анализировать сессии – каждый из инструментов способен лишь восстанавливать потоки протокола TCP, но не устанавливать связи, существующие между потоками в рамках работы приложений. Потому возникает необходимость в создании собственного сниффера, который бы обладал данной функциональностью.

Список литературы

[1] *Программно-аппаратные* средства обеспечения информационной безопасности: учебное пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов; под редакцией А.В. Душкина. — Москва: Горячая линия-Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5. — Текст: электронный // Электронно-библиотечная система «Лань». URL: https://e.lanbook.com/book/111053.

[2] *Скудис Э.* Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: учебное пособие / Э. Скудис. — Москва: ДМК Пресс, 2009. — 512 с. — ISBN 5-94074-170-3. — Текст \: электронный // Электронно-библиотечная система «Лань». URL: https://e.lanbook.com/book/1112.

[3] *Шелухин О.И.* Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинов; под редакцией О.И. Шелухина. — Москва: Горячая линия-Телеком, 2018. — 220 с. — ISBN 978-5-9912-0323-4. — Текст: электронный // Элек-

тронно-библиотечная система «Лань». URL: https://e.lanbook.com/book/111119.

[4] Шаньгин В.Ф. Информационная безопасность: учебное пособие / В.Ф. Шаньгин. — Москва: ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст: электронный // Электронно-библиотечная система «Лань». URL: https://e.lanbook.com/book/50578.

Зоринов Николай Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: zorinov.nikolai@yandex.ru

Я.И. Румякин

ОБЗОР ПОДХОДОВ И ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ РАСПРЕДЕЛЕННОГО УПРАВЛЕНИЯ ДОСТУПОМ МЕЖДУ ПРИЛОЖЕНИЯМИ

На настоящий момент времени в интернете размещено около миллиарда сайтов, при этом более чем на 15% из них в том или ином виде присутствуют механизмы регистрации и авторизации пользователей. Согласно подсчетам, среднестатистический пользователь имеет пару электронных адресов, несколько учетных записей в социальных сетях, пользуется некоторыми онлайн-магазинами, форумами и блогами. В совокупности, количество заводимых пользователем личных кабинетов на различных порталах достигает отметки в 10, а иногда и в 20 учетных записей. Кроме того, человеческий фактор играет не в пользу систем безопасности, т.к. в большинстве случаев люди склонны использовать одинаковые или мало различимые пароли и коды доступа на разных ресурсах. [1]

Наравне с этим, большие социальные сети, форумы, онлайн-магазины и прочие порталы стремятся усилить меры безопасности, при этом как можно сильнее упростив жизнь обычных пользователей. Для этого служат различные виды аутентификации, включая двухфакторную, использующую мобильные телефоны, коды восстановления, а также одноразовые пароли. Однако, такие подходы не обеспечивают решения еще одной проблемы – создания большого числа личных кабинетов. [2]

Для этого, сообщество инженеров разработало открытый стандарт OAuth, являющийся протоколом авторизации, позволяющим предоставлять третьим сторонам ограниченный доступ к защищенным ресурсам пользователя с учетом его согласия, не требуя при этом передачи сторонним приложениям логинов и паролей личных кабинетов. Крупные медиа-гиганты, интернет-компании и социальные сети стали активно развивать стандарт. Наряду с этим, произошло появление другого открытого стандарта – OpenId, позволяющего создавать децентрализованные системы аутентификации, предоставляющие пользователям разнообразных порталов возможности по созданию единой учетной записи для аутентификации на множестве различных никак не связанных друг с другом интернет-ресурсов. Далее развитие стандартов привело к появлению OAuth 2.0 и OpenId Connect – протоколов и стандартов, активно использующихся в настоящее время в мобильных приложениях, приложениях умных телевизоров, экосистемах умных домов и других ресурсах сети Интернет. [3]

На пути становления стандартом. Основной проблемой становления и развития стандартов являлось создание подхода, при котором пользователь бы чувствовал, что его личные данные находятся под надежной защитой и что без его ведома к ним никто не получит доступ. Ярким примером является проблема аутентификации и авторизации в личном кабинете – как не запра-

шивая логин и пароль пользователя уведомить систему к данным какого аккаунта она запрашивает доступ и имеет ли она на это право.

Решением данной проблемы явился старый подход с некоторыми доработками – необходимость доверия своим пользователям. Доверие заключается в том, что пользователь должен самостоятельно аутентифицироваться и авторизоваться на сервисе личных данных, а затем предоставить приложению некоторый идентификатор, используя который можно узнать, что это за пользователь и что можно получить от его имени. [4]

Протоколы OAuth 2.0 и OpenId Connect. Следует сразу указать на различие того, что протокол OpenId Connect – это протокол аутентификации, т.е. однозначно идентифицирующий, что за пользователь запрашивает доступ, а протокол OAuth 2.0 – это протокол авторизации, позволяющий получить от пользователя права на доступ к определенным ресурсам.

Протокол OAuth 2.0 является наследником протокола первой версии, появившегося в 2006 г. Отличием новой версии является простота. Протокол претерпел ряд изменений, сокративших количество необходимых запросов и упростивших схемы подписи пользовательских данных.

Протокол OpenId Connect также является развитием стека протоколов OpenId. Он является расширением протокола OAuth 2.0 и позволяет сторонним сервисам однозначно идентифицировать пользователя. Таким образом, приложения могут запрашивать и отсылать друг другу данные пользователей, зная при этом, что они оперируют данными одного и того же пользователя в рамках одного сервиса личных данных.

В настоящий момент времени, использование протокола OpenId Connect более предпочтительно, т.к. позволяет синхронизировать данные пользователей на различных сервисах, а также позволяет подготовиться к возможной интеграции данных сервисов. [5]

Суть протоколов состоит в том, чтобы отправить пользователя на сервис с личными данными (например, социальная сеть), запросив при этом доступ к определенному набору пользовательских данных или других ресурсов от его имени (1). Затем, пользователь должен авторизоваться на том сервисе, куда его отправили (2, 3), выбрав при этом к каким запрашиваемым ресурсам приложение получит доступ. После подтверждения пользователь отправится обратно в приложение со специальными идентификаторами (4). Схематичное описание представлено на рис. 1.

При помощи полученного идентификатора доступа, приложение может осуществлять запросы к другим приложениям, также использующим сервис авторизации, выдавший полученный идентификатор доступа. Следует уточнить, что при таком подходе, разница между протоколами сводится к тому, что при использовании OpenId Connect сервис авторизации также включает в идентификатор доступа уникальный идентификатор пользователя — это может быть логин, электронная почта или что-то другое, однозначно идентифицирующее авторизовавшегося пользователя учетной записи.

Рис. 1. Схема авторизации пользователя по протоколу OAuth 2.0

Такой тип аутентификации и авторизации с использованием протокола OpenIdConnect называется явным и является самым простейшим. Кроме него, существует еще несколько схем:

- Базовая авторизация – используется в том случае, если идентификатор необходим серверу приложения. При данном подходе сервис авторизации возвращает специальный код, передающийся серверу, который затем напрямую запрашивает идентификатор доступа.
- Гибридная авторизация – использует смешанный подход базовой авторизации на основе кода и простого получения идентификатора напрямую через явную авторизацию. [6]

Заключение. Рассмотренные протоколы широко применяются как различными порталами, агрегирующими данные пользователей, так и их клиентами. Использование данных протоколов позволяет отказаться от огромного числа учетных записей, заводимых на каждого отдельного пользователя, а также позволяет самим пользователям сосредоточиться на защите своего единственного аккаунта.

Для получения более подробной информации следует обратиться к спецификациям стандартов.

Список литературы

[1] *Москалев С.М.* Интернет-технологии и реклама в бизнесе / С.М. Москалев; Министерство сельского хозяйства РФ, Санкт-Петербургский государственный аграрный университет. – Санкт-Петербург: СПбГАУ, 2018. –

101 с.: ил. [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page =book&id=491717 (дата обращения: 07.10.2019).

[2] *Технология* разработки интернет ресурсов: курс лекций: авт.-сост. И.А. Журавлёва; Министерство науки и высшего образования Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». – Ставрополь: СКФУ, 2018. – 171 с.: ил. [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book&id=562579 (дата обращения: 11.10.2019).

[3] *Резниченко А.Д., Аббакумов А.А., Панфилов С.А.* Создание информационных систем на базе распределенных сетей сайтов. //Научно-технический вестник Поволжья. – 2015. – №3. – с. 205-209.

[4] *Новиков А.Ю., Кейно П.П., Хорошко Л.Л.* Разработка архитектуры интернет-сервиса организации научных мероприятий с автоматизацией документооборота. Прикладная Информатика - 2018 г. №4. с. 70-76. [Электронный ресурс]. – URL: https://e.lanbook.com/journal/2067 (дата обращения: 12.10.2019)

[5] *Поляков А.Н., Пойда А.А., Сорокин А.А.* и др. Разработка программных средств виртуальной интеграции распределенных источников данных для создания масштабных информационных инфраструктур профессионального назначения. //Автоматизированные системы и комплексы. – 2013. – №3(37). – с. 152-160.

[6] *Официальные* спецификации протокола OpenId Connect. [Электронный ресурс]. – URL: https://openid.net/specs/openid-connect-core-1_0.html (дата обращения 12.10.2019).

Румякин Ярослав Игоревич – студент КФ МГТУ им. Н.Э. Баумана. ЗАО Калуга Астрал. Email: yaroslow@yandex.ru

В.А. Бессонов

ОБЗОР СИСТЕМЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ ИЗМЕРЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОЙ НАСТРОЙКИ И ВМЕШАТЕЛЬСТВА

Современные средства измерения (СИ) содержат интеллектуальные модули, позволяющие им анализировать измеряемые параметры. Несанкционированное воздействие на эти модули приводят к искажению результатов измерений.

Согласно ГОСТ Р 8.654-2015, «Программное обеспечение средств измерений (ПО СИ)» – это программы (совокупность программ), предназначенные для использования в СИ и реализующие в том числе сбор, передачу, обработку, хранение и представление измерительной информации, а также программные модули и компоненты, необходимые для функционирования этих программ [1].

Угрозами информационной безопасности называются потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсам информационной системы. Все угрозы безопасности, направленные против программных и технических средств информационной системы, в конечном итоге оказывают влияние на безопасность информационных ресурсов и приводят к нарушению основных свойств хранимой и обрабатываемой информации. Как правило, угрозы информационной безопасности различаются по способу их реализации.

В соответствии с ГОСТ Р 8.883-2015 определена методика испытаний ПО СИ и его алгоритмов. Среди них для анализа системы защиты ПО необходимо выделить следующие методы испытаний [2]:

1. проверка разделения программного обеспечения;
2. проверка идентификационных данных (признаков) и методов идентификации программного обеспечения;
3. проверка структуры программного обеспечения;
4. оценка влияния программного обеспечения и его алгоритмов на метрологические характеристики средств измерений;
5. проверка защиты программного обеспечения и определение ее уровня.

Проверка разделения программного обеспечения. Разделение ПО СИ приводят в целях выделения в составе ПО СИ метрологически значимой части, т. е. той его части, которая подлежит испытаниям.

Метрологически не значимая часть ПО СИ испытаниям не подлежит. Ее модификация может быть выполнена без уведомления организаций, проводящих испытания, если изменение этой части не приводит к изменению идентификационных данных метрологически значимой части ПО СИ.

После испытаний ПО метрологически значимая часть ПО СИ не должна измениться. Любая модификация метрологически значимой части ПО СИ

приводит к изменению ею идентификационных данных и к необходимости проведения повторных испытаний, в частности испытаний с целью утверждения типа СИ, или внесению изменений в описание типа СИ в соответствии с административным регламентом.

Проверку идентификационных данных ПО и методов идентификации проводят в целях обеспечения идентификации ПО СИ при поверке СИ. Идентификация ПО СИ осуществляемая при поверке СИ представляет собой проверку соответствия ПО СИ тому, которое было зафиксировано (документировано) в описании типа СИ с последующим обеспечением защиты ПО от несанкционированного доступа во избежание искажений результатов измерений.

Под проверкой структуры ПО понимают:

1. проверку отсутствия недопустимого влияния на метрологически значимую часть ПО и данные, осуществляемого через интерфейс пользователя;

2. проверку отсутствия недопустимого влияния на метрологически значимую часть ПО и данные, осуществляемого через интерфейсы связи;

3. проверку правильности взаимодействия между метрологически значимой и незначимой частями ПО.

Проверку защиты ПО СИ и его алгоритмов проводят с целью установления наличия средств защиты метрологически значимой части ПО и измеренных данных и определения уровня защиты ПО от непреднамеренных и преднамеренных изменений. Под проверкой защиты ПО понимается:

1. проверка защиты метрологически значимой части ПО и измеренных данных от случайных или непреднамеренных изменений:

2. проверка защиты метрологически значимой части ПО и измеренных данных от преднамеренных изменений.

На основе анализа документации определяют наличие (отсутствие) средств защиты метрологически значимой части ПО и измеренных данных от изменения или удаления в случае возникновения непредсказуемых физических воздействий (например, наличие энергонезависимой памяти для хранения измеренных данных).

С помощью функциональных проверок, имитирующих непредсказуемые физические воздействия, убеждаются в действии средств защиты метрологически значимой части ПО и измеренных данных от изменения или удаления в случае возникновения непредсказуемых физических воздействий [3].

Для безопасного ПО СИ необходимо реализовать следующие программные модули, которые должны быть включены в программный комплекс СИ:

1. Модуль предотвращающий работу метрологически значимой части ПО СИ в случае несанкционированного изменения кода программного продукта;

2. Модуль автоматического идентификаци ПО СИ (вычисление контрольных сумм) каждых отдельных частей ПО СИ и ПО СИ в целом;

3. Интерфейс предоставляющий полученные идентификационные данные для каждой части ПО СИ и ПО СИ в целом;

4. Модуль автоматической очистки из памяти данных ПО СИ по завершению работ в запланированном или аварийном режиме;

5. При разработке ПО СИ исключить возможность сохранения промежуточных результатов работ в энергонезависящей памяти;

6. Обеспечить операторов ПО СИ только необходимым интерфейсом ввода команд управления;

7. Ограничить доступ операторам СИ к окружению, в котором функционирует ПО СИ.

Таблица 1

Уровни защиты ПО СИ от непреднамеренных и преднамеренных изменений

Уровень защиты	Описание
Низкий	Не используют никакие специальные средства защиты от преднамеренных изменений
Средний	Метрологически значимая часть ПО и измеренные данные защищены от преднамеренных изменений с помощью простых программных средств
Высокий	Метрологически значимая часть ПО СИ и измеренные данные достаточно защищены с помощью специальных средств защиты от преднамеренных изменений

Заключение. Программное обеспечение средств измерений имеют высокую важность в соблюдении ее целостности, так как любое непреднамеренное изменение может привести к искажению результатов измерений. Важно обеспечить защиту и не допустить нарушение таких параметров как конфиденциальность, целостность и точность результатов работы средств измерений от угроз, направленных на программное обеспечение средств измерений.

Список литературы

[1]. *ГОСТ* Р 8.654-2015 Государственная система обеспечения единства измерений (ГСИ). Требования к программному обеспечению средств измерений. Основные положения – М.: Стандартинформ, 2015.

[2]. *ГОСТ* Р 8.883-2015 Государственная система обеспечения единства измерений (ГСИ). Программное обеспечение средств измерений. Алгоритмы обработки, хранения, защиты и передачи измерительной информации. Методы испытаний – М.: Стандартинформ, 2015.

[3]. *Порядок* проведения испытаний стандартных образцов или средств измерений в целях утверждения типа (утвержден приказом Министерства промышленности и торговли Российской Федерации от 30 ноября 2013 г. № 1081) – М.: Стандартинформ, 2013.

Бессонов Валентин Андреевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: valentbesson@gmail.com

Ю.С. Носова

ОБЗОР УЯЗВИМОСТЕЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Сетевая инфраструктура представляет собой совокупность различного оборудования, а также программного обеспечения, которая формирует особую среду для эффективного процесса обмена данными.

Согласно ГОСТ Р 56545–2015, «уязвимость» – это недостаток (слабость) программного (программно–технического) средства или ИС в целом, который (которая) может быть использована для реализации угроз безопасности информации [1].

Недостаточная защита сетевой инфраструктуры является одной из главных проблем для специалистов по сетям и безопасности, поскольку она представляет собой критическую угрозу для эффективности и результативности организации при постоянно растущей скорости написания и распространения эксплойтов. Чрезвычайно важно заранее определить слабые места сетевой безопасности организации, прежде чем злоумышленник сможет их обнаружить и, как следствие, организует атаку [2].

Управление уязвимостями включает в себя регулярно повторяющийся процесс выявления, классификации и исправления недостатков.

Основными элементами IT-инфраструктуры являются локально-вычислительная сеть, сервера и рабочие места пользователей.

Уязвимости могут иметь следующие разумные причины:

1. Сложность: большие, сложные системы увеличивают возможность появления слабых мест в системе.

2. Использование одного и того же пароля в нескольких программах.

3. Просмотр веб-сайтов: автоматически установленные на компьютерных системах вредоносные шпионские или рекламные программы могут стать причиной уязвимости, поскольку компьютерные системы после посещения определенных веб-сайтов заражаются, позволяя злоумышленнику обладать собранной ценной информацией.

4. Ошибки программного обеспечения: ошибки программного обеспечения могут позволить злоумышленнику злоупотреблять предназначенным инструментом.

Рассмотрим некоторые уязвимости элементов сетевой инфраструктуры.

Уязвимости маршрутизаторов. К распространённым уязвимостям маршрутизаторов относят отсутствие проверки авторизации, что позволяет удаленным злоумышленникам выполнить команду ping через запрос GET для перечисления сетевых устройств или сбоя маршрутизатора.

Также существует возможность раскрытия информации посредством запросов на документ router_info.xml. При этом отобразится PIN-код, MAC-адрес, таблица маршрутизации, версия прошивки, время обновления, информация о локальной сети и информация о беспроводной сети устройства. Эти сведения могут помочь злоумышленнику организовать атаку на отказ в об-

служивании (Denial of Service) или атаку «Man in the middle» (человек посередине).

Отсутствие обновлений на сервере. Все, что требуется злоумышленнику или инсайдеру – это отсутствие обновлений на сервере, которое позволяет осуществить несанкционированный доступ в информационную среду организации. Следует сказать, что установка обновлений требует особой аккуратности, но их отсутствие может сделать сервер уязвимым.

Для решения данной проблемы необходимо следовать рекомендациям по обеспечению безопасности сети, обновив операционную систему и любое другое программное обеспечение, работающее на ней.

Слабые или стандартные пароли. Самая распространенная уязвимость — слабый пароль. Пароль является основным способом определения подлинности пользователя. Стандартный пароль или его отсутствие ставит под угрозу информационную безопасность, так как злоумышленник может использовать подбор пароля с помощью специальных программ или же с помощью знаний каких–либо фактах о владельце и получить неограниченный доступ к ресурсам рабочей станции или сервера.

Решение: регулярно менять и проверять слабые пароли и рассмотреть возможность использования инструмента управления паролями. Полезным будет реализовать блокировку нарушителя после определенного количества неудачных попыток входа в систему.

Неправильная настройка межсетевого экрана. Неправильная настройка или отсутствие межсетевого экрана открывает множество возможностей для сетевых атак рабочих станций и серверов извне. Межсетевой экран (англ. firewall) — это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Используя уязвимости неправильно настроенного межсетевого экрана злоумышленник может в рамках разрешенного протокола реализовать атаку.

Грамотная настройка политики безопасности может обеспечить надежную работу сервера и защиту конфиденциальной информации.

Отсутствие контроля над использованием внешних USB-накопителей. Мобильность и удобство съемных накопителей приводят к тому, что им часто доверяют личную и служебную информацию. Как следствие, количество атак с использованием USB-накопителей увеличилось. Главные угрозы, которые возникают, — кража, потеря, подмена и бесконтрольное использование. В результате происходит заражение систем вредоносными программами и утечка информации [3].

Для безопасного использования служебного USB-накопителя важно обеспечить возможность использования накопителя только на определенных компьютерах, чтобы исключить бесконтрольное подключение к неизвестным устройствам и настроить политику безопасности таким образом, чтобы для каждого пользователя установить соответствующие ограничения.

Заключение. В данной работе было рассмотрено понятие уязвимости с точки зрения информационной безопасности, в том числе описаны одни из

самых распространенных уязвимостей сетевой инфраструктуры. Поводя итоги данной статьи, отмечаем, что специалист по обеспечению безопасности обязан постоянно проводить работу по выявлению слабых мест в системе, следить за обновлением баз данных уязвимостей, а также своевременно устранять недостатки и устанавливать соответствующие меры в контролируемой им системе.

Список литературы

[1]. *ГОСТ* Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей». – М.: Стандартинформ, 2015.

[2]. *Электронный* ресурс: https://www.network-security-magazine.com

[3]. *Лукацкий А.В.* Обнаружение атак. – СПб.: Издательство «БВХ», 2001. – 624 с.

Носова Юлия Сергеевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: yuliya-nosova1996@yandex.ru

А.Р. Филатов, М.К. Савкин

ОБЩИЙ ПОДХОД К ТЕСТИРОВАНИЮ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕРВЕРНЫХ ПРИЛОЖЕНИЯХ

На сегодняшний день все большее распространение получают приложения, основанные на клиент-серверной архитектуре. Клиент-серверная архитектура – это вычислительная или сетевая архитектура, в которой нагрузка распределена между поставщиками услуг, называемыми серверами, и заказчиками услуг, называемыми клиентами. Фактически клиент и сервер — это программное обеспечение. Обычно эти программы расположены на разных вычислительных машинах и взаимодействуют между собой через вычислительную сеть посредством сетевых протоколов, но они могут быть расположены также и на одной машине. Программы-серверы ожидают от клиентских программ запросы и предоставляют им свои ресурсы в виде данных или сервисных функций. Перенос вычислительной нагрузки на серверную часть позволяет решить сразу несколько задач:

- уменьшение требований к вычислительным машинам клиентов;
- отсутствие дублирования кода;
- централизованное управление данными и вычислительными ресурсами.

Однако нужно учитывать, что сосредоточивание в одном месте данных и вычислительных ресурсов несет в себе опасность полной потери работоспособности системы при условии проведения успешной атаки.

Поскольку большинство серверов являются web-серверами или взаимодействует с ними, а протоколы и стандарты для различного рода взаимодействий между web-серверами и web-приложениями разработаны и описаны довольно подробно, то в данной статье будет рассмотрено применение и соблюдение требований, определенных в рамках существующих протоколов.

HTTP/HTTPS

HTTP — широко распространённый протокол передачи данных, изначально предназначенный для передачи гипертекстовых документов (то есть документов, которые могут содержать ссылки, позволяющие организовать переход к другим документам). Аббревиатура HTTP расшифровывается как HyperText Transfer Protocol, «протокол передачи гипертекста». В соответствии со спецификацией OSI, HTTP является протоколом прикладного (верхнего, 7-го) уровня. Актуальная и самая распространенная на данный момент версия протокола HTTP 1.1 (постепенно заменяемая на версию HTTP/2), описана в спецификации RFC 2616.

Также HTTP часто используется как протокол передачи информации для других протоколов прикладного уровня, таких как SOAP, XML-RPC и WebDAV. В таком случае говорят, что протокол HTTP используется как «транспорт».

API многих программных продуктов также подразумевает использование HTTP для передачи данных – сами данные при этом могут иметь любой формат, например, XML или JSON. Как правило, передача данных по протоколу HTTP осуществляется через TCP/IP-соединения. Серверное программное обеспечение при этом обычно использует TCP-порт 80 (если порт не указан явно, то обычно клиентское программное обеспечение по умолчанию использует именно 80-й порт для открываемых HTTP-соединений), хотя может использовать и любой другой.

HTTPS – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов SSL или TLS. В отличие от HTTP с TCP-портом 80, для HTTPS по умолчанию используется TCP-порт 443.

Исходя из спецификации протоколов можно вынести следующие рекомендации и места, на которые следует обратить при тестировании:

1. Сервер не должен поддерживать пользовательские HTTP методы – нестандартизированные пользовательские методы могут представлять потенциальную угрозу для сервера из-за отсутствия должного контроля при разработке этого метода и его выполнения.

2. Сервер не должен поддерживать TRACE, TRACK или CONNECT методы.

HTTP методы TRACE/TRACK используется для получения информации о том, что происходит с сообщением на промежуточных узлах. У сообщений с HTTP методом TRACE/TRACK есть конечный получатель, который определяется значением поля заголовка Max-Forwards: первый HTTP сервер, прокси-сервер или шлюз, получивший данное сообщение с значением Max-Forwards 0 является конечным получателем. Использование таких методов позволяет безошибочно отследить сообщение на всех узлах его пути.

HTTP метод CONNECT используется для преобразования HTTP соединения в прозрачный TCP/IP туннель. Используется для шифрования сообщений. Никто кроме самого приложения не должен иметь доступ к шифрованию сообщений.

3. Принудительное использование протокола HTTPS

Использование протокола с обязательным шифрованием сообщений повышает уровень информационной безопасности в приложении.

4. Наличие и правильная конфигурация следующих заголовков в HTTP/HTTPS сообщениях:

- Expect-CT – заголовок сообщает браузеру о том, то он должен выполнить дополнительные «фоновые проверки», чтобы убедиться, что SLL сертификат является подлинным
- Feature-Policy – заголовок позволяет определить, включена ли конкретная функция браузера на текущей странице
- Access-Control-Allow-Origin – с помощью заголовка приложение сообщает браузеру, что можно получать запросы из других источников

- Strict-Transport-Security – с помощь заголовка браузер принудительно активирует защищённое соединение через протокол HTTPS
- X-Frame-Options – заголовок описывает возможность встраивания браузером содержимого в текущую страницу. Позволяет настроить списки разрешенных источников встроенного содержимого.
- Content-Security-Policy и X-XSS-Protection – заголовки предоставляет утилиты для предотвращения множества атак: от XSS (межсайтовый скриптинг) до перехвата кликов (клик-джеккинга)

5. Не должно быть следующих заголовков в HTTP/HTTPS сообщениях, которые показываю версию ПО сервера: Server, X-Powered-By, X-AspNet-Version

6. Должны быть проверены гиперссылки, доступные пользователю, ведущие на сторонние ресурсы, структуры запросов и ответов для этих ресурсов, в т. ч. HTTP заголовки запросов.

7. При использовании HTTPS протокола предпочтение всегда должно отдаваться TSL протоколу шифрования. SSL протокола шифрования следует избегать.

Общие рекомендации

Все содержимое ресурса должно управляться отдельной системой управления содержимым. Разрешения на взаимодействие с приложением и ОС для такой системы должны быть минимальными. Если в такой системе используется кэширование, то чувствительная информация не должна храниться в кэше на стороне клиента. Проверка данных на клиенте и контроль работы системы являются обязательным.

Если web-приложение использует cookies (небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя), то они должны содержать минимум важной для обеспечения ИБ информации (пароли, логины и т. д.). Необходима проверка информации, помещаемой в cookies, контроль жизненного цикла cookies и выставляемые для cookies в течении их существования флаги.

Обязательное следование стандарту Payment Card Industry Data Security Standard (представляет собой совокупность детализированных требований по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций) при возможности оплаты через приложение.

Наличие файрволла для серверных приложений является одним из обязательных условий.

Последним, но достаточно важным, можно назвать рекомендацию по внедрению вознаграждения пользователей в системах за поиск и сообщение о найденных уязвимостях.

Подытожив все вышеперечисленное, можно сказать, что на данный момент существуют стандартизованные подходы к обеспечению ИБ для серверных приложений и соответственно на их основе можно проверять и оце-

нивать существующие системы. Очевидно, что с ростом количества угроз будет расти и список необходимых проверок.

Список литературы

[1] Артюхов А., Простым языком об HTTP, URL: https://habr.com/ru/post/215117/ (дата обращения 29.10.2019)

[2] Арсенальт К., Лучшие практики при защите web- приложений, URL: https://www.keycdn.com/blog/web-application-security-best-practices (дата обращения 29.10.2019)

[3] Надалин А., Как усилить защищенность веб-приложений при помощи HTTP заголовков, URL: https://habr.com/ru/company/edison/blog/434228/ (дата обращения 29.10.2019)

[4] PCI SECURITY STANDARDS URL: https://www.pcisecuritystandards.org/documents/PCI-Secure-Software-Standard-v1_0.pdf/ (дата обращения 29.10.2019)

Филатов Александр Романович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: afnotdead@yandex.ru

Савкин Михаил Константинович – ассистент кафедры «Защита информации» КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

А.Б. Лачихина, А.А. Серегин

ОРГАНИЗАЦИЯ И ПОДХОДЫ МОНИТОРИНГА ФИЗИЧЕСКОГО ПОДКЛЮЧЕНИЯ СЕТИ

Одной из основных задачей защиты системы является мониторинг состояния элементов сети, который отслеживается на разных уровнях системы.

На физическом уровне рассматриваются такие характеристики, как качество сигнала, модуляция, частота и т.п.

На канальном уровне применительно к Ethernet определяется обнаружение и коррекция ошибок, а измеряется количество кадров и коллизий.

На сетевом уровне отслеживается неполадки и заторы сети. Также на сетевом уровне устанавливается соединение, присваивается адрес сетевому узлу и происходит продвижение данных.

На прикладном уровне измеряется время отклика сети. Мониторинг осуществляется подключением к сети специальных устройств-анализаторов или встроенными средствами коммуникационных устройств и конечных узлов.

«Анализ сети — это процесс захвата сетевого трафика и его быстрого просмотра для определения того, что произошло с сетью» - Анжелла Оребаух. Различают два вида мониторинга сети: первый, маршрутизаторо-ориентированный, основан на особенностях работы маршрутизатора. Функции, которые встроены в сами маршрутизаторы и не требует установки дополнительного ПО, называются методами, основанными на маршрутизаторе. Второй, не ориентированный на маршрутизаторы. Не основанные на маршрутизаторах методы требуют установки стороннего ПО и предоставляют большую функциональность.

Методы мониторинга, которые основаны на маршрутизаторе — жёстко находятся (вшиты) в маршрутизаторах, и они имеют низкую гибкость.

Протокол сетевого мониторинга (SNMP**).** SNMP — протокол прикладного уровня, который входит в стек протоколов TCP/IP. Он позволяет администраторам руководить производительностью сети, находить и устранять сетевые неполадки, планировать рост сети. Также он собирает статистику по трафику функционирования агентов через пассивные датчики.

Существуют две версии: SNMPv1 и SNMPv2, он построен на SNMPv1 и усовершенствован функцией добавления операций с протоколами. Версия 3 (SNMPv3) находится на стадии рассмотрения и стандартизации.

Для протокола SNMP присущи три ключевых компонента:

- управляемые устройства (Managed Devices),
- агенты (Agents)
- системы управления сетью (Network Management Systems - NMSs).

Для анализа сети применяется анализатор протоколов или сетевой тестер — это специализированное устройство, направленное обработку и хранение определённой информации с различных уровней сети.

Специально для возможности внешнего наблюдения в ряде коммутаторов организуют отражение портов (port mirroring). Трафик одного из портов дублируется в специально выделенный порт, который предназначен для подключения внешнего анализатора. Однако возникают проблемы, так как пропускаемой входного порта чаще всего недостаточно для пропускания трафика обоих направлений (если порт анализатора имеет ту же скорость, что и наблюдаемые). Отражение не позволяет наблюдать за всеми портами сразу, из-за этого нет полной информации по устройству. Правда, иногда предоставляется возможность отражения группы портов на порт с большей скоростью.

Средства мониторинга, встроенные в сетевые устройства, позволяют наблюдать за всеми портами (узлами) сразу, правда, с меньшими возможностями анализа. В управляемые хабы и коммутаторы встраивают зонды удаленного мониторинга (RMON probe), информация от которых может предоставляться менеджерам. Функциональные возможности зондов заметно связаны с ценой управляемых устройств, поэтому многие модели аппаратуры реализуют только часть функций удаленного мониторинга групп RMON (рис. 1).

Рис. 1. Устройство RMON мониторинга

Фирма 3Com хочет перенести средства мониторинга и управления на клиентское ПО. Эта идея реализуется в технологии Dynamic Access. Средства мониторинга (dRMON Smart Agent) реализуются клиентским программным обеспечением узлов (на уровне драйверов сетевых карт и операционной системы) и требуют сравнительно небольшого усложнения аппаратных средств адаптеров. При этом возможности мониторинга могут значительно расширяться по сравнению с обычным RMON (протокол мониторинга компьютерных сетей).

Интеллект агентов RMON позволяет выполнять диагностику неисправностей и предупреждать о возможных перебоях или отказах. С помощью RMON технологии можно собрать данные о функционировании сети, а в

случае отклонений от заданных стандартов на сервер или клиентское ПО может прийти оповещение о неполадки или полном отказе оборудования. Собирая информацию, получаемую от агентов RMON, приложение может помочь устранить или подобрать план действий для устранения проблемы администратором сети.

Управление локальными сетями обычно осуществляется с одного управляющего компьютера. Протяжённость сетей и высокая стоимость сетевого оборудования вынуждает крупные компании распределять функции среди нескольких серверов, которые располагаются во многих странах мира. Такая конфигурация сети может быть предпочтительнее из-за ограниченного количества линий связи, а также из-за необходимости устойчивой работы сети.

Все это заставляет администратора международной сети задуматься о средствах управления и контроля работы сети, которые бы, во-первых, могли бы самостоятельно определять состояние сетевых устройств. И если и не ремонтировать их, то хотя бы диагностировать неисправности. Тем самым сотрудники технического отдела могли бы подготовиться к выезду и иметь необходимые информацию и инструменты. Во-вторых, необходимо оборудование, которое предупреждало бы о появляющихся проблемах и могло бы диагностировать в чем именно заключается проблема. Такая технология необходима чтобы избежать рисков полного отказа оборудования.

Список литературы

[1]. *Манакова И.П*. Как сделать анализ чужого сетевого трафика, / [электронный ресурс]. Режим доступа: URL: https://belbriz.ru/obschie-voprosy/kak-sdelat-analiz-chuzhogo-setevogo-trafika/

[2]. *Методы* мониторинга, основанные на маршрутизаторе / [Электронный ресурс]. Режим доступа: URL: https://studwood.ru/1270648/informatika/metody_monitoringa_osnovannye_marshrutizatore

[3]. *Пятифан* / Разработка методики анализа аномальности сетевого трафика на основе статистической обработки экспериментальных данных, / [Электронный ресурс]. Режим доступа: URL:http://5fan.ru/wievjob.php?id=88812

[4]. *Студопедия* /RMON (Remote Monitoring), / [Электронный ресурс]. Режим доступа: URL: https://studopedia.ru/5_96820_RMON-Remote-Monitoring.html

[5]. *OSP* – Гид по технологиям цифровой трансформации / RMON переходит в наступление, / [Электронный ресурс]. Режим доступа: URL: https://www.osp.ru/nets/1996/06/141763/

Лачихина Анастасия Борисовна - доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasialach73@gmail.com

Серегин Антон Александрович - студент, ЗАО НПФ «Сигма». E-mail: tige_25@mail.ru

Р.В. Габдуллин, Е.А. Черепков, Ю.С. Белов

ОЦЕНКА ЭФФЕКТИВНОСТИ МНОГОМЕРНОГО ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Введение. Линейный криптоанализ – одна из двух наиболее широко используемых атак на блочные шифры (наряду с дифференциальным криптоанализом). Открытие принадлежит Mitsuri Matsui. В 1993 году Matsui опубликовал атаку на DES (Data Encryption Standard), таким образом, представив первый экспериментальный криптоанализ шифра DES, о котором сообщалось в открытом сообществе [1]. Впоследствии были предложены различные варианты усовершенствования атаки, такие как использование многомерных аппроксимаций и включение нелинейных выражений.

Цель данной работы заключается в оценке эффективности многомерного линейного криптоанализа.

Краткие теоретические сведения. Линейный криптоанализ представляет собой статистическую атаку, которая использует двоичную линейную связь между открытым текстом, шифром и ключом.

Matsui представил два алгоритма, алгоритм 1 (Алг. 1) и алгоритм 2 (Алг. 2) для итерационных блочных шифров. Алг. 1 извлекает один бит информации о секретном ключе, Алг.2 может быть использован для нахождения нескольких битов ключа, полученных на последней итерации. Части предполагаемых ключей с последней итерации ранжируются, и ожидается, что верный ключ будет иметь самый высокий ранг. Тогда можно извлечь еще один бит информации о секретном ключе с помощью Алг. 1.

Многомерный линейный криптоанализ предполагает использование множественных линейных аппроксимаций, которые формируют линейное подпространство. Множество линейных аппроксимаций позволяют сделать линейную атаку более эффективной. Потенциально может быть восстановлено больше битов информации ключа и, возможно, с использованием меньшего количества данных. Но тогда также необходимы более трудоемкие статистические модели.

В качестве метода усовершенствования Алг. 1 и Алг. 2 будет рассмотрен следующий: логарифмическое отношение правдоподобия (ЛОП). Теория предсказывает, что для Алг. 1 и Алг. 2 ранжирование ключей, основанное на ЛОП, более эффективно, чем тесты с использованием χ^2 (или G-теста) [2].

Эффективность метода будет измеряться и сравниваться в теории и экспериментах с использованием концепции преимущества, введенной Сельчуком. Блочный шифр Serpent был разработан, чтобы противостоять линейному криптоанализу. Поэтому в качестве испытаний будет использоваться Serpent (с уменьшенным числом итераций) [3].

Основное теоретическое преимущество многомерного метода заключается в том, что статистическая модель может быть дана без допущения о статистической независимости линейных аппроксимаций.

Построение многомерной линейной аппроксимации. Пространство n-мерных двоичных векторов обозначается $\mathbb{F}_2^n$. Сумма по модулю 2 обозначается символом $\oplus$.

Скалярное произведение для $a=(a^1,\ldots,a^n), b=(b^1,\ldots,b^n)\in\mathbb{F}_2^n$ определяется как $a\cdot b=a^1b^1\oplus\cdots\oplus a^nb^n$. Тогда вектор a называется (линейной) маской b.

Функция $f:\mathbb{F}_2^n\mapsto\mathbb{F}_2$ называется булевой функцией. Линейная булева функция — это отображение $x\mapsto u\cdot x$, где $u\in\mathbb{F}_n$. Функция $f:\mathbb{F}_2^n\mapsto\mathbb{F}_2^m$ с $f=(f_1,\ldots,f_m)$, где f_i – булевы функции, называется векторной булевой функцией размерности m. А линейная Булева функция от $\mathbb{F}_2^n$ до $\mathbb{F}_2^m$ представлена $m\times n$ двоичной матрицей U. m строк U обозначаются $u_1,\ldots,u_m$, где каждое u_i является линейной маской.

Рассмотрим итерационный блочный шифр с размером блока n. Пусть x - открытый текст, а y - результат шифрования после R итераций. Обозначим через K вектор, состоящий из всех битов ключа, используемых в R итерациях, и через h длину K. Тогда блочный шифр — это векторная булева функция с входом $(x,k)\in\mathbb{F}_2^n\times\mathbb{F}_2^m$. А m-мерная линейная аппроксимация блочного шифра может рассматриваться как векторная Булева функция

$$\mathbb{F}_2^n\times\mathbb{F}_2^h\to\mathbb{F}_2^m,(x,K)\mapsto Ux\oplus Wy\oplus VK \qquad (1)$$

где U и W – есть $m\times n$ двоичные матрицы. Матрица V имеет также m строк и делит ключи на 2^m классов эквивалентности $g=VK, g\in\mathbb{F}_2^m$.

Ранжирование ключей. Набор предполагаемых ключей задан, и задача состоит в том, чтобы определить, какой ключ является правильным. Пусть ключи ищутся из набора $\mathbb{F}_2^l$ всех 2^l строк l битов. Алгоритм состоит из четырех фаз: *фазы подсчета, фазы анализа, фазы сортировки и фазы поиска* [4]. На этапе подсчета данные, например пары открытый текст – зашифрованный текст, собираются из шифра. На этапе анализа вещественная статистика T используется для вычисления метки $T(k)$ для всех ключей $k\in\mathbb{F}_2^l$.

На этапе сортировки ключи k сортируются, т. е. ранжируются в соответствии с их метками $T(k)$. Оптимально, чтобы правильный ключ, обозначенный k_0, находился в верхней части списка. В противном случае, на этапе поиска ключи в списке тестируются до тех пор, пока не будет найден k_0.

Исследование четырех-итерационного шифра Serpent. Ниже, на рис.1, представлены результаты тестирования ЛОП-метода для многомерного Алг. 1 на 4-7 итерациях Serpent. Путем выбора линейно независимых одномерных базовых аппроксимаций $u_i\cdot x\oplus w\cdot y, i=1,\ldots,m$, была построена линейная аппроксимацию вида (1) с $m=10$. Используемые маски w и $u_i, i=1,\ldots,m$, можно найти в [5].

На рис. 1 также показано, насколько лучше m-мерный ЛОП-метод по сравнению с биномиальным методом, где тот же набор m одномерных аппроксимаций и Алг. 1 используются для определения каждого бита предполагаемого класса ключей отдельно и независимо.

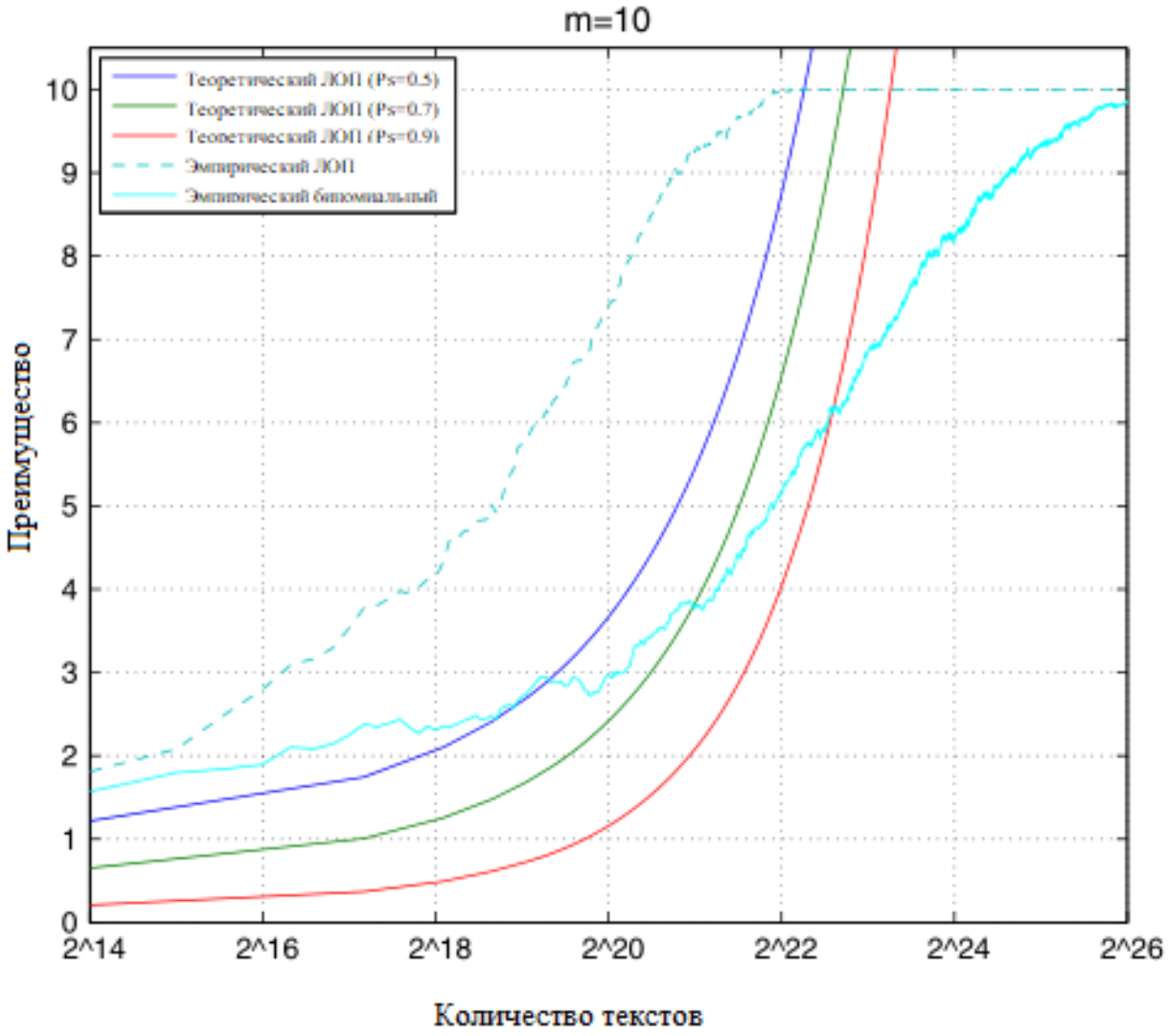


Рис. 1. Алг. 1: Теоретическое и эмпирическое преимущество в зависимости от сложности данных с использованием ЛОП-метода для четырех-итерационного Serpent при $m = 10$

Теперь рассмотрим шифр с $R+1$ итерациями. Пусть x-открытый текст, а z-зашифрованный текст после $R+1$ итераций. Пусть $(R+1)$ - я функция итерации и ключ итерации – f и $k \in \mathbb{F}_2^l$ соответственно. Тогда результат шифрования после R итераций равен $y = f^{-1}(z,k)$. Алгоритм 2 использует многомерную линейную аппроксимацию по R итерациям, заданную как (1) с распределением вероятности p. задача состоит в том, чтобы найти правильный ключ последней итерации k_0 и, возможно, кроме того, класс правильного ключа g_0 для ключа, используемого в первых R итерациях.

Теоретическое преимущество ЛОП-метода проиллюстрировано на фоне сложности данных на рис. 2 для различных m. Эмпирические преимущества для нескольких различных m показаны на рис. 3. Метод может быть усилен увеличением m, пока увеличение емкости $C(p)$ не станет незначительным по сравнению с увеличением m. Для четырех-итерационного Serpent это происходит при $m \approx 12$.

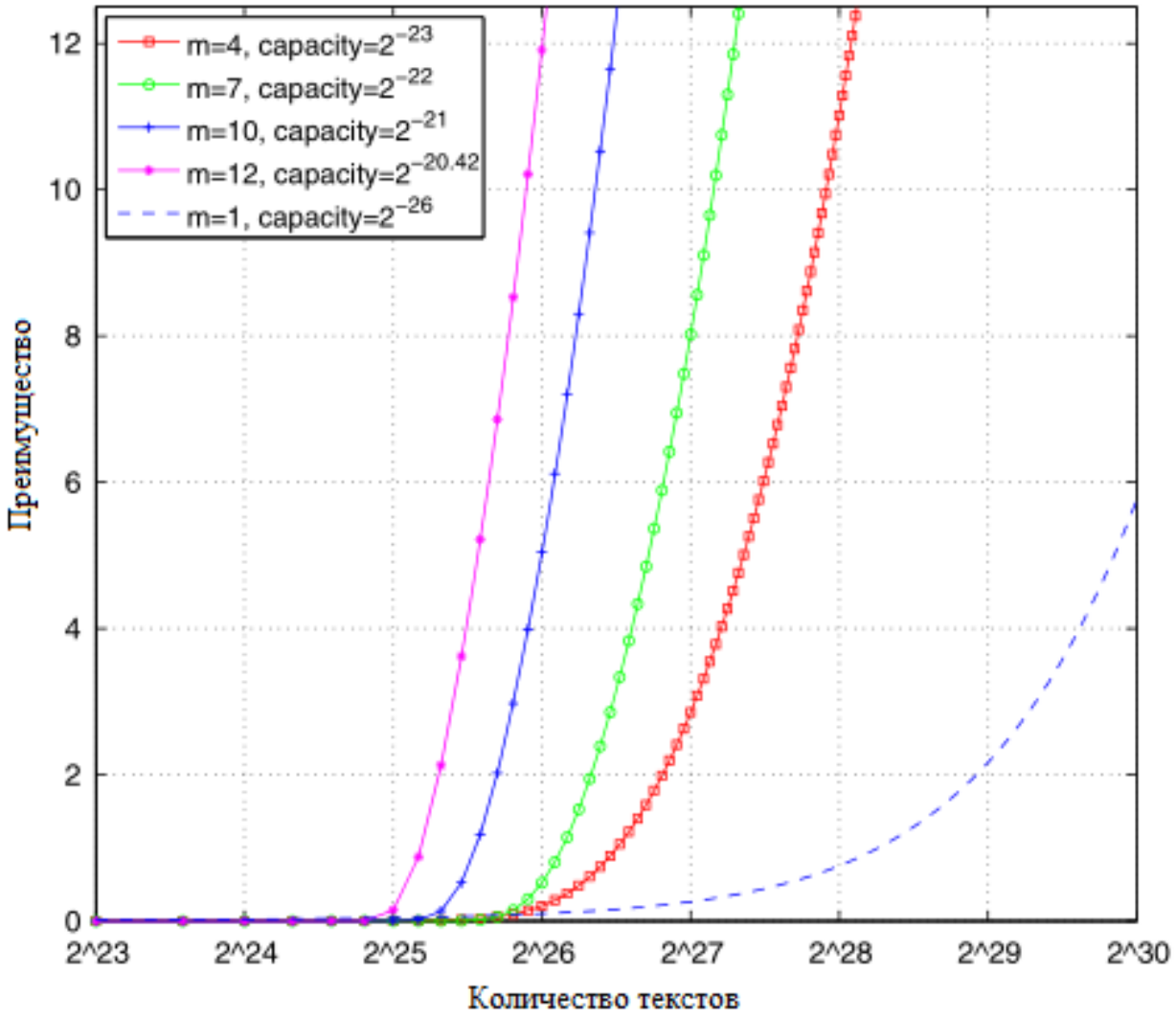


Рис. 2. Алг. 2: Теоретическое преимущество ЛОП-метода для различных m и $P_s = 0.95$

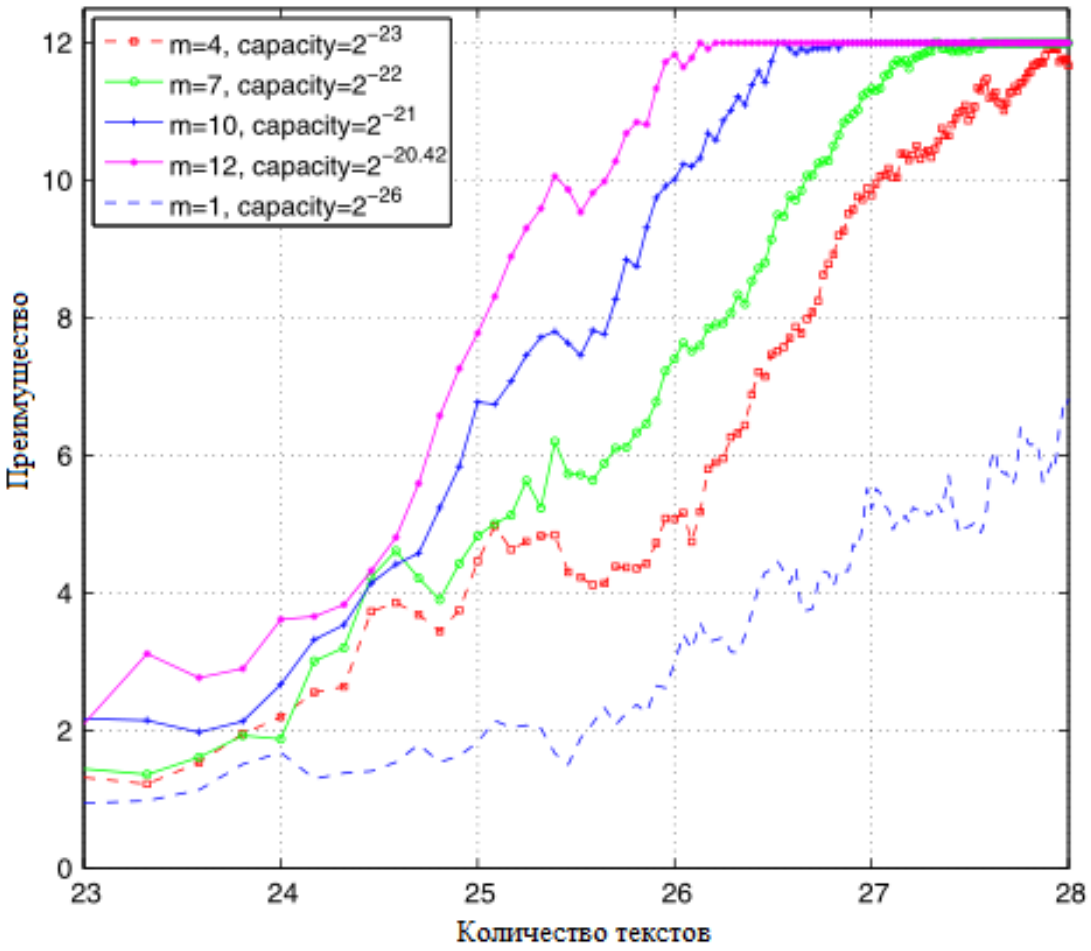


Рис. 3. Алг. 2: эмпирическое преимущество ЛОП-метода для различных m

Заключение. Таким образом, способ (логарифмическое отношение правдоподобия) расширения алгоритмов Matsui 1 и 2 до нескольких измерений позволяет значительно увеличить эффективность линейного криптоанализа, используя при этом меньшее количество данных.

Список литературы

[1] *Matsui M.* The First Experimental Cryptanalysis of the Data Encryption Standard. *Advances in Cryptology – CRYPTO '94*, 1994, vol. 839, pp. 1-11. Springer Link URL: https://link.springer.com. doi: https://doi.org/10.1007/3-540-48658-5_1 (Дата обращения 30.10.2019)

[2] *Hermelin M., Cho J. Y., Nyberg K.* Multidimensional Linear Cryptanalysis. *Journal of Cryptology*, 2019, vol. 32, no. 1, pp. 1-34. Springer Link URL: https://link.springer.com. doi: https://doi.org/10.1007/s00145-018-9308-x (дата обращения 20.10.2019).

[3] *Biham E., Anderson R., Knudsen L.* Serpent: a new block cipher proposal. *International Workshop on Fast Software Encryption*, 1998, vol. 1372, pp. 222–238. Springer Link URL: https://link.springer.com. doi: https://doi.org/10.1007/3-540-69710-1_15 (Дата обращения 27.10.2019)

[4] *Vaudenay S.* An experiment on DES statistical cryptanalysis. *CCS '96 Proceedings of the 3rd ACM conference on Computer and communications security*, 1996, pp.139–147. ACM URL: https://dl.acm.org. doi: https://doi.org/10.1145/238168.238206 (Дата обращения 27.10.2019)

[5] *Hermelin M., Cho J. Y., Nyberg K.* Multidimensional Linear Cryptanalysis of Reduced Round Serpent. *Information Security and Privacy, 2008* , vol. 5107, pp. 203-215. Springer Link URL: https://link.springer.com. doi: https://doi.org/10.1007/978-3-540-70500-0_15 (дата обращения 31.10.2019).

Габдуллин Равиль Василевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: gvg.ravil@gmail.com

Черепков Евгений Александрович - преподаватель КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: e.cherepkov@yandex.ru

Белов Юрий Сергеевич - доцент, канд. физ.-мат. наук КФ МГТУ им. Н.Э. Баумана. E-mail: iu4-kf@mail.ru

А.А. Гапутина

ПЕРЕХОД К СИСТЕМАМ БЕЗОПАСНОГО ОБМЕНА ФАЙЛАМИ НА ОСНОВЕ ТЕХНОЛОГИИ MFT

Ежедневно миллионы людей со всего мира используют сайты обмена файлами для отправки текстовых документов, программного обеспечения, образов, медиа-файлов и др. Но при использовании таких сайтов можно столкнуться с такими проблемами, как безопасность, потеря файлов, компрометация данных. Для конфиденциальных документов это является большим риском утечки важной информации и не может соответствовать должным образом требуемым мерам безопасности.

Среди основных требований для организации безопасного файлообмена можно выделить следующие:

- Авторизованный обмен файлами,
- Понятный на интуитивном уровне пользовательский интерфейс,
- Централизованная передача файлов, как в традиционных решениях (FTP, электронная почта), гарантия их конфиденциальности и контроль процессом обмена,
- Выполнение пунктов:
  - Соответствие локальным нормативным требованиям,
  - Аудит и администрирование используемой системы,
  - Комплексное отслеживание информации обо всех передаваемых файлах и операциях скачивания,
  - Групповая передача данных,
  - Управление пользователями и их правами.

Общедоступный файлообменник все эти задачи решить не сможет. Для устранения недостатков передачи файлов была изобретена управляемая передача файлов, или MFT.

О системах Managed File Transfer (MFT)

Управляемая передача файлов (англ. Managed File Transfer, MFT) – программное решение, реализованное для упрощения задач безопасной передачи файлов с одного компьютера на другой посредством сети (например, Интернет).

Существует множество систем MFT, которые предоставляют своим пользователям различные функциональные возможности для обмена файлами. Среди основных функций выделяют следующие:

- шифрование отправляемых файлов;
- проставление ЭП на передаваемых документах;
- журналирование и аудит проделанных операций и входов в систему;
- администрирование системы;
- возможность интеграции с различными ИС с помощью API;
- возможность аутентификации на основе LDAP, AD, Web SSO, X.509,
- поддержка нескольких протоколов передачи файлов.

На сегодняшнем рынке существуют различные программные продукты, которые обладают широкими функциональными возможностями и которые можно выбрать, исходя из нужд компании.

Serv-U MFT Server — это расширенная версия известного FTP-сервера Serv-U, который может управлять передачей файлов с использованием нескольких протоколов, таких как FTP, FTPS, SFTP и HTTP/S. Программное обеспечение позволяет использовать общий доступ к файлам и обеспечивает одноранговую передачу файлов с веб- и мобильных устройств. Он может интегрироваться с NAS / SAN и внешними серверами баз данных, что обеспечивает легкий доступ к хранилищу.

Globalscape EFT Cloud Services — это облачный безопасный и масштабируемый сервис обмена файлам. Организации любого размера могут использовать его для безопасного и легкого хранения данных в облаке, перемещения файлов по защищенной сети без каких-либо задержек. Консоль инструмента позволяет администраторам видеть все, что происходит в режиме реального времени, и позволяет им мгновенно создавать отчеты.

GoAnywhere MFT Standard дает возможность обмениваться файлами и данными по всей организации как внутренне, так и внешне. Эти задачи могут быть выполнены с помощью интеллектуального интерфейса. В течение всего процесса передачи файлов, все файлы остаются полностью зашифрованными. Инструмент предлагает неограниченную передачу файлов по электронной почте, комплексное шифрование, поддержку подключения к серверу и подробные отчеты аудита.

MOVEit MFT System предоставляет сетевым администраторам возможность управлять всеми действиями по передаче файлов в рамках своей организации с помощью единой консоли. Пользователи имеют возможность отправлять файлы друг другу, когда это необходимо, а администраторы могут отслеживать, где находятся файлы. MOVEit имеет меры безопасности и шифрования, чтобы защитить данные. Используя это программное обеспечение, можно гарантировать безопасность конфиденциальных корпоративных данных. Данная система включает в себя функцию обработки отказа. Это обеспечивает высокую надежность, предотвращая задержку и потерю данных.

Direct FTP — это в первую очередь FTP-клиент, но он предлагает множество возможностей для легкой передачи и загрузки файлов, а также функции редактирования. Инструмент оснащен интуитивно понятным интерфейсом. В отличие от большинства других инструментов FTP, Direct FTP предлагает встроенный редактор кода. Он имеет поддержку HTML, JavaScript и других распространенных типов кода.

MassTransit от Acronis – эта система разработана, чтобы помочь более крупным организациям безопасно и надежно обрабатывать большие нагрузки по передаче данных, без особых усилий и со скоростью, значительно превышающей скорость передачи файлов по стандартным протоколам передачи файлов. MassTransit может обрабатывать файлы размером более 100 Гб, и обеспечивает детальное отслеживание передачи файлов в режиме реального

времени. Программное обеспечение включает в себя административные функции, которые помогают автоматизировать процессы передачи файлов и управлять рабочими процессами.

Увеличение количества передаваемых файлов различных типов и размеров постепенно приводит к необходимости использования специализированных технологических продуктов для решения задачи безопасного управления файлообменом. Использование традиционных решений больше не позволяет удовлетворить все требования безопасности, а использование сторонних файлообменников и вовсе может привести к серьезным последствиям для компании. Системы MFT являются эффективным инструментом для решения задачи файлообмена и удовлетворяют большую часть потребностей современной организации.

Список литературы

[1] *Andy Hampshire.* Managed File Transfer Product Overview – 2017 / [электронный ресурс]. Режим доступа: URL: https://community.tibco.com/wiki/managed-file-transfer-product-overview

[2] *Renaud* Larue-Langlois. 10 Best Managed File Transfer (MFT) Tools and Software - 2018 / [электронный ресурс]. Режим доступа: URL: https://www.addictivetips.com/net-admin/managed-file-transfer-software/

[3] *Реализация* безопасного файлообмена с помощью систем управляемой передачи файлов. Часть 1 / [электронный ресурс]. Режим доступа: URL: https://powersecurity.org/ru/blog/managed-file-transfer-secure-file-exchange/

Гапутина Алина Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: alina.gaputina@yandex.ru

И.С. Скубаева

ПОДХОДЫ К МОНИТОРИНГУ ЗАПУЩЕННЫХ ПРОЦЕССОВ В ОС LINUX

Любая операционная система, в том числе основанная на базе Linux, во время своей работы использует службы и процессы. Управление операционной системой заключается в настройке множества служб, используя командную строку и разные сервисы, предназначенные для поддержки бесперебойной работы системы. Для корректной работы процессов необходимо поддерживать не только стандартные сервисы, но и специальные службы, предназначенные для обработки ввода, повышения производительности, ресурсов для разгрузки и т.д. Процессы также являются составляющими основных функций компьютера, следовательно, важно иметь достаточное количество ресурсов.

Сделать систему уязвимой может служба, которая использует ресурсы системы, работающая без контроля администратора. Чтобы избежать снижения уровня безопасности, необходимо знать, каким образом можно обнаружить и завершить в любой момент времени посторонний процесс или службу, выполняющуюся в системе [1].

Существует несколько способов обнаружения всех запущенных служб и процессов в операционной системе Linux, например, команды, помогающие найти и управлять процессами и службами.

Инструмент командной строки ‘service’

Команда «service» поставляется почти с каждым дистрибутивом Linux и может быть использована не только для запуска и остановки служб и процессов, но и для их мониторинга настоящее временя. После использования команды, предоставляется полный список служб.

Инструмент командной строки ‘top’

«top» является встроенным инструментом, используемым для получения данных о всех процессах и службах, выполняемых в настоящее время на компьютере. Он включен в дистрибутивы на основе Debian и RedHat и предлагает множество функций, которые помогут понять, что происходит на сервере [2].

HTOP

Htop очень похож на «top» с точки зрения его основных функций. Обычно он не включен в операционную систему по умолчанию, однако он доступен для большинства дистрибутивов Linux. Подобно top, htop позволяет пользователю просматривать подробную информацию о каждом процессе, а также следить за самой системой. Но htop позволяет намного более точно контролировать отображаемую информацию, а также предлагает набор утилит, которые могут быть применены к процессам.

Например, используя htop можно настроить приоритет выполнения процесса, и завершить его с указанным приоритетом. В данном инструменте

присутствует сортировка, упрощающая просмотр только важной информации. Htop имеет гистограмму, отображающую различные системные ресурсы, которая позволяет быстро отслеживать, сколько используется ресурсов процессора или ОЗУ.

Команда PS

PS является предустановленной функцией, используемой для отображения сведений о процессах. PS простой инструмент, предназначенный для быстрого получения результатов. С помощью одной простой команды можно получить подробный список запущенных процессов.

PS работает быстрее чем top, ориентирована на просмотр PID процесса и всей командной строки каждого процесса.

Описание выводимых столбцов.

- **C**. Отображает количество выполняемых операций в секунду.
- **TIME**. Общее процессорное время, затраченное на выполнение процесса.
- **%CPU**. Параметр указывает, какой процент процессорного времени был потрачен на выполнение процесса с момента его запуска.
- **STIME**. Время старта процесса.
- **RSS**. Объем физической памяти, занятой процессом, в килобайтах.
- **TRS**. Размер размещенной в физической памяти командной части программы.
- **%MEM**. Это значение указывает, какую долю (в процентах) от общего объема оперативной памяти компьютера составляет значение **RSS** [3].

Linux process explorer

Linux process explorer — компактное, но мощное графическое приложение для просмотра активных процессов (диспетчер задач) и мониторинга состояния системы (системный монитор).

Диспетчер задач Linux Process Explorer имеет удобный интерфейс и минимум настроек. Позволяет отображать в режиме реального времени состояние всех ресурсов системы - загрузку процессора, памяти, подкачки, использование сетевых соединений, а также даёт возможность просмотреть детальную информацию о любом из запущенных процессов [4].

mpstat

mpstat — встроенный инструмент, который отслеживает использование процессоров в системе. Наиболее часто используемая команда mpstat -P ALL — показывает развернутую статистику всех процессов системы.

Безопасность ОС напрямую зависит от выполняющихся служб и процессов, поэтому необходимо вести их постоянный мониторинг. В настоящее время существует множество приложений и программных средств, позволяющих облегчить работу администратора, но для обеспечения требуемого уровня безопасности, следует периодически использовать простые инструменты для администрирования ОС [5].

Список литературы

[1]. *Как* перечислить все запущенные службы в Linux с помощью командной строки / [электронный ресурс]. Режим доступа: URL: https://bestwebber.ru/kak-perechislit-vse-zapyshennye-slyjby-v-linux-s-pomoshu-komandnoi-stroki/

[2]. *Использование* ps для мониторинга процессов / [электронный ресурс]. Режим доступа: URL: https://wiki.dieg.info/ps

[3]. *Linux* Process Explorer / [электронный ресурс]. Режим доступа: URL: https://zenway.ru/page/procexp

[4]. *Мониторинг* Linux. Более 80 инструментов / [электронный ресурс]. Режим доступа: URL: weblampa.ru/nix/monitoring-linux.html

Скубаева Ирина Сергеевна - студентка КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: russia071@yandex.ru

И.Е. Рунов

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ЗАЩИТЫ БАЗ ДАННЫХ

К настоящему времени человечеством накоплено огромное количество информации об объектах и явлениях, хранящееся в электронном виде и используемое в БД, защита которых является ключевой проблемой в решении задач информационной безопасности в связи с возможностью многопользовательского доступа в локальных, корпоративных и глобальных сетях [1].

В конце двадцатого столетия число атак на базы данных было значительно ниже числа атак непосредственно на web-серверах компаний. Но за последние годы ситуация несколько изменилась. Всемирно известные хакерские организации — такие, как Black Hat (www.blackhat.com) и Defcon (www.defcon.org), начали проявлять все больший интерес к вопросам безопасности БД. Множество уязвимостей в защите БД публикуется в группах новостей — таких, как SecurityFocus (www.securityfocus.com). Добыча полноценной версии корпоративной системы управления базами данных (СУБД) и анализ на наличие уязвимостей в системе безопасности на сегодняшний день не представляют сложности для хакерского сообщества. Инсталляция современной СУБД доведена до элементарного уровня и может быть выполнена даже незатейливым пользователем, умеющим нажимать необходимые кнопки. Как показывает практика, большинство распространенных на рынке СУБД по умолчанию предрасположены к взлому. Естественно, это не означает, что они не могут быть сконфигурированы с надлежащим уровнем безопасности [2].

Обеспечение эффективной защиты информационных ресурсов предполагает соблюдение высоких критериев комплексности, как необходимого условия сохранения конфиденциальности критически важной информации практически в любых областях деятельности. Система безопасности баз данных представляет собой комплексное решение защиты информации.

Криптографические методы применяются лишь как часть такой комплексной защиты. В многоуровневой системе безопасности – это последний внутренний уровень защиты. Криптография используют как для шифрования данных в базе, закрытия аутентификационных данных пользователей, так и для организации невозможности отказа от совершенного действия (non-repudiation).

В зависимости от генерации и использования ключей на сегодняшний день существуют криптосистемы с открытым ключом и с использованием симметричного (закрытого) криптографического ключа.

Использование симметричного криптографического ключа означает, что для шифрации и дешифрации используется один ключ. Подобного рода системы подразумевают, что отправитель и получатель сообщения обладают идентичным ключом, который может быть передан по защищенному каналу

связи. Системы симметричного шифрования классифицируются на поточные алгоритмы шифрования, в которых алгоритмы шифрования выполняются побитно, и блочные алгоритмы, которые выполняют операции шифрования над группами битов [3].

Обычно в серверах БД встроена реализация нескольких наиболее распространенных и надежных симметричных алгоритмов, как блочных, так и поточных: DES, Triple_DES, Triple_DES_3KEY, DESX, RC2, RC4, RC4_128, AES с ключами длиной 128 (Rijndael), 192 и 256 бит.

Недостатком этой системы является сложность передачи ключа. То есть, если пользователи географически далеки друг от друга, появляется необходимость найти надежный способ передачи для обмена секретными ключами.

В системах с открытым ключом для шифрования и расшифрования используются различные ключи. Ключ шифрования является открытым, а ключ расшифрования хранится в секрете. При этом открытый ключ шифрования составлен так, что он не позволяет вычислить секретный ключ шифрования. Математическая взаимосвязь между закрытым и открытым ключами делает каждую пару ключей уникальными.

При использовании асимметричных криптоалгоритмов возникает проблема распространения множества открытых ключей, которая решается с помощью построения Инфраструктуры Открытых Ключей (Public Key Infrastructure – PKI), на основе базы данных цифровых сертификатов.

Сертификаты – это по существу асимметричные ключи, которые содержат дополнительные метаданные. Эти метаданные включают в себя такую информацию, как время окончания и центр сертификации, выдавший данный сертификат. В случае если необходимо удостовериться в том, что отправитель или получатель данных является тем за кого себя выдает, сертификаты помогают решить эту проблему. Центры сертификации создают сертификат со своей подписью, который отправляется тому пользователю, который его заказал. Когда он будет использовать этот сертификат для отправки данных, получатель сможет проверить его в центре сертификации и удостовериться в подлинности отправителя. Отличие сертификатов от ключей состоит в задании промежутка времени, в течение которых они действуют и уникальных метаданных, указывающих на владельца сертификата. Существуют самозаверительные сертификаты. Например, в своих последних версиях MS SQL Server автоматически создает самозаверительный сертификат при своем первом запуске. Этот сертификат используется для шифрования подключения при выполнении аутентификации MS SQL Server.

Рассмотрим реализацию шифрования в MS SQL Server. В Microsoft SQL Server реализовано прозрачное шифрование баз данных (Transparent Data Encryption). Прозрачное шифрование кодирует базы данных целиком. Когда страница данных записывается из оперативной памяти на диск, она шифруется. Когда страница загружается обратно в оперативную память, она расшифровывается. Таким образом, база данных на диске оказывается полностью зашифрованной, а в оперативной памяти – нет. Основным преимущест-

вом TDE является то, что шифрование и дешифрование выполняются абсолютно прозрачно для приложений. Использовать преимущества шифрования может любое приложение, использующее для хранения своих данных Microsoft SQL Server. При этом модификации или доработки приложения не потребуется.

В Microsoft SQL Server функции шифрования были улучшены и расширены. Для увеличения надежности криптозащиты и уменьшения нагрузки на систему применяется специальная иерархия ключей.

1. Каждой базы данных шифруется при помощи специального ключа – Database Encryption Key.

2. Database Encryption Key шифруется сертификатом, который создан в базе данных Master.

3. Сертификат базы данных Master шифруется ее главным ключом.

4. Главный ключ БД Master шифруется главным ключом службы Service Master Key.

5. Главный ключ службы SMK шифруется службой защиты данных операционной системы.

Также в Microsoft SQL Server имеется шифрование соединения между сервером и клиентом. В ранних версиях для передачи конфиденциальных данных использовался протокол SSL, то теперь пакеты «оборачиваются» в его логическое продолжение – протокол TLS. SQL Server всегда шифрует сетевые пакеты, связанные со входом в систему. Если сертификат не был предоставлен на сервере при запуске, SQL Server создает самозаверяющий сертификат, который используется для расшифровки пакетов входа. Сервер создает собственный сертификат, который принимается клиентом, но шифруется лишь информация о соединении.

Чтобы шифровать всю информацию по каналу «клиент-сервер-клиент», необходимо выдать серверу корневой (доверенный) сертификат, импортировать его на клиентские станции и настроить схему взаимодействия криптоалгоритмов. Одной из наиболее результативной схем будет шифрование трафика симметричным методом, в то время, как ключи защищаются открытыми сертификатами.

Рассмотренные встроенные криптографические средства взаимно дополняют друг друга и являются неотъемлемой частью комплексной защиты баз данных, без которых невозможно организовать надежную защиту данных.

Список литературы

[1]. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2012. - 592 с.

[2] *http*://infocom.uz [Электронный ресурс] URL: http://infocom.uz/2005/08/22/kriptograficheskaya-zaschita-bazyi-dannyih/ (дата обращения 27.09.2019)

[3]. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. - М.: 2015. - 480с.

Рунов Илья Евгеньевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: ierunov@yandex.ru

Е.С. Еськов

ПРИМЕНЕНИЕ РЕВЕРС – ИНЖИНИРИНГА ДЛЯ РЕШЕНИЯ ЗАДАЧ ИБ

Обратная разработка (обратное проектирование, обратный инжиниринг, реверс-инжиниринг; англ. reverse engineering) — исследование некоторого готового устройства или программы, а также документации на него с целью понять принцип его работы; например, чтобы обнаружить недокументированные возможности (в том числе программные закладки), сделать изменение или воспроизвести устройство, программу или иной объект с аналогичными функциями, но без прямого копирования.[1]

Для решения задач информационной безопасности реверс-инжиниринг применяется при анализе вредоносных программ, выявлении и ликвидации уязвимостей, определение недекларированных возможностей («программных закладок») и т.д.

Существует базовый алгоритм исследования программы, который показан на примере решения задачи ниже. В зависимости от сложности программы он может изменяться.

В данной статье рассмотрим пример исследования приложения взятого с сайта www.crackmes.one. На этом сайте пользователи выкладывают свои программы, которые являются «загадками», в некоторых необходимо добыть флаг[1], в других исследовать алгоритм для получения «ключей» (с целью написания keygen) и т.д. Существуют различные уровни сложности:

— Легкий;
— Простой;
— Средний;
— Трудный.

Была выбрана программа автора с ником «evilprogrammer». В информации к этой программе дано, что она была написана на языке C/C++ для Windows.

Слова автора : « This is a very easy flag, i made with love for you, there are two ways to resolve it. I hope you will have fun.»[2]

Процесс исследования программы

Первый шаг: запуск программы, на рис. 1 приведен результат выполнения. Результатом выполнения является строка, которая выведена экран «try harder». Эта строка является отправной точкой в дизассемблировании программы.

Для анализа воспользуемся IDA Pro Disassembler. IDA Pro Disassembler (англ. Interactive DisAssembler) — интерактивный дизассемблер, который широко используется для реверс-инжиниринга. Он отличается исключительной гибкостью, наличием встроенного командного языка, поддерживает множество форматов исполняемых файлов для большого числа процессоров и операционных систем.[3]

[1] Флаг – некоторая символьная комбинация, которую выявить при анализе.

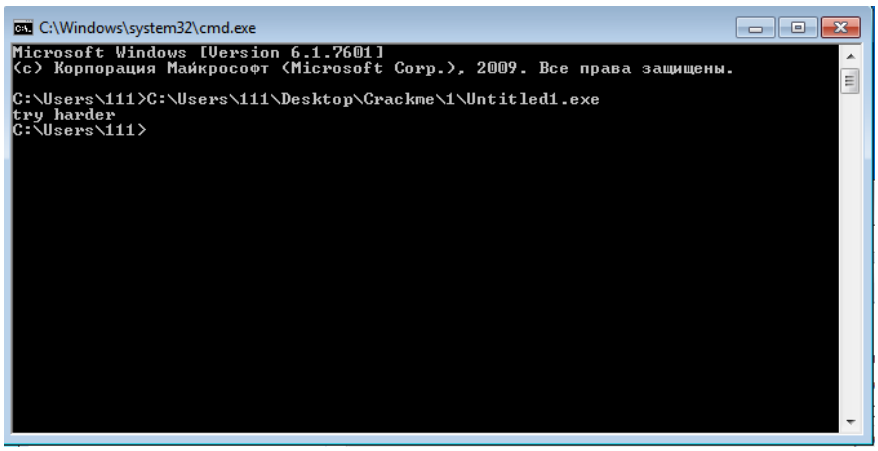


Рис. 1. Результат выполнения программы

Второй шаг: поиск строки. Для того чтобы упростить поиск функции, которая осуществляется вывод строки «try harder» , найдем расположение самой строки (рис. 2).

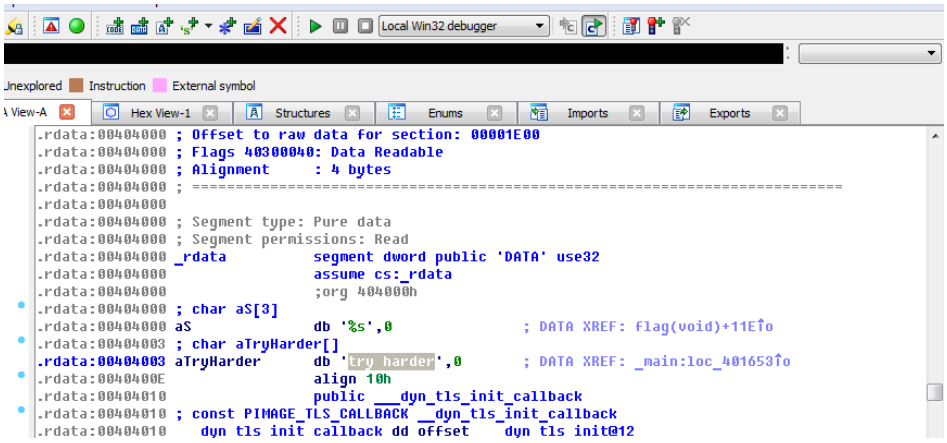


Рис. 2. Поиск строки

На рис. 2 справа от искомой строки находится адрес функции, где она была использована; ссылка является интерактивной, что позволяет перейти к данной функции (рис. 3).

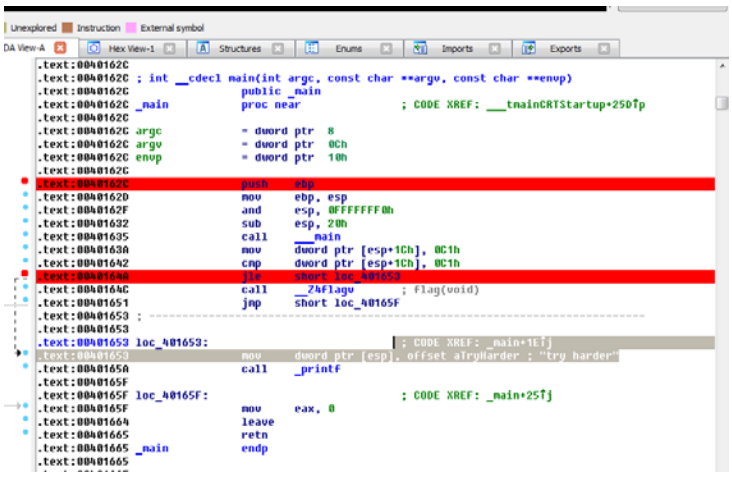


Рис. 3. Функция вывода

Третий шаг: анализ функции. На рис. 3 видно, что в зависимости от выполнения условного перехода, который находится по адресу 0x0040164A, будет выполнена команда с адреса 0x00401653 (вывод «try harder») или вызвана функция _Z4flagv (0x0040164C).

Четвёртый шаг: выполнение функции _Z4flagv. Для исполнения данной функции необходимо отредактировать PE файл с помощью WinHex. WinHex – это универсальный HEX-редактор, который предназначается для работы с операционной системой Windows [3]. Потребуется отредактировать второй операнд команды cmp, виртуальный адрес которой 0x00401642. Нужно сделать так, чтобы первый операнд, значение которого равно 0xC1, был больше второго, следовательно, заменим значение второго операнда на 0x1 (рис. 4).

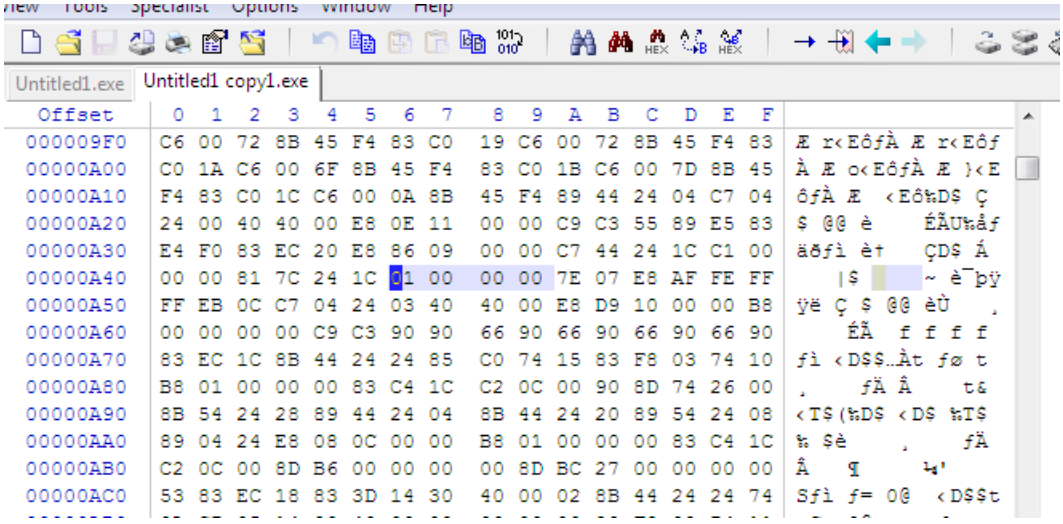


Рис. 4. Редактирование файла

Пятый шаг: проверка результата. Запустив программу мы видим искомый флаг рис. 5.

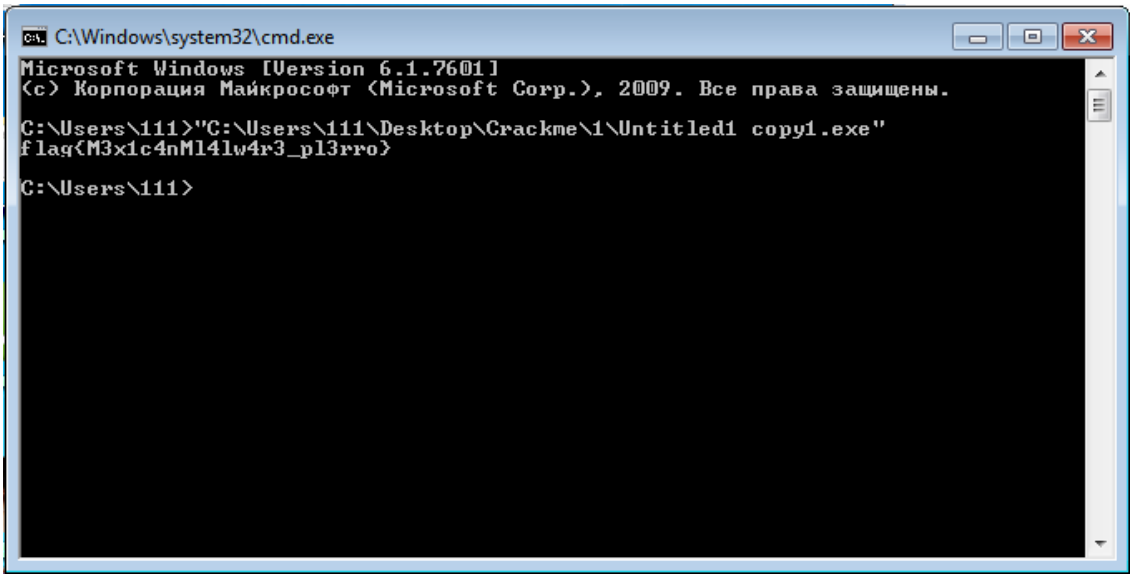


Рис. 5. Результат выполнения редактирование

Существует также альтернативный способ решения задачи, на третьем шаге перейти по интерактивной ссылке на адрес функции _Z4flagv 0x0040164C (рис. 6).

Если обратить внимание на функцию выделения памяти (malloc), то можно догадаться по коду ниже, что флаг задается пользователем поэлементно. Значения, которые помещаются в память по указателю (который хранится в eax), являются «кусочками» флага, а именно символы в ACSII кодировке.

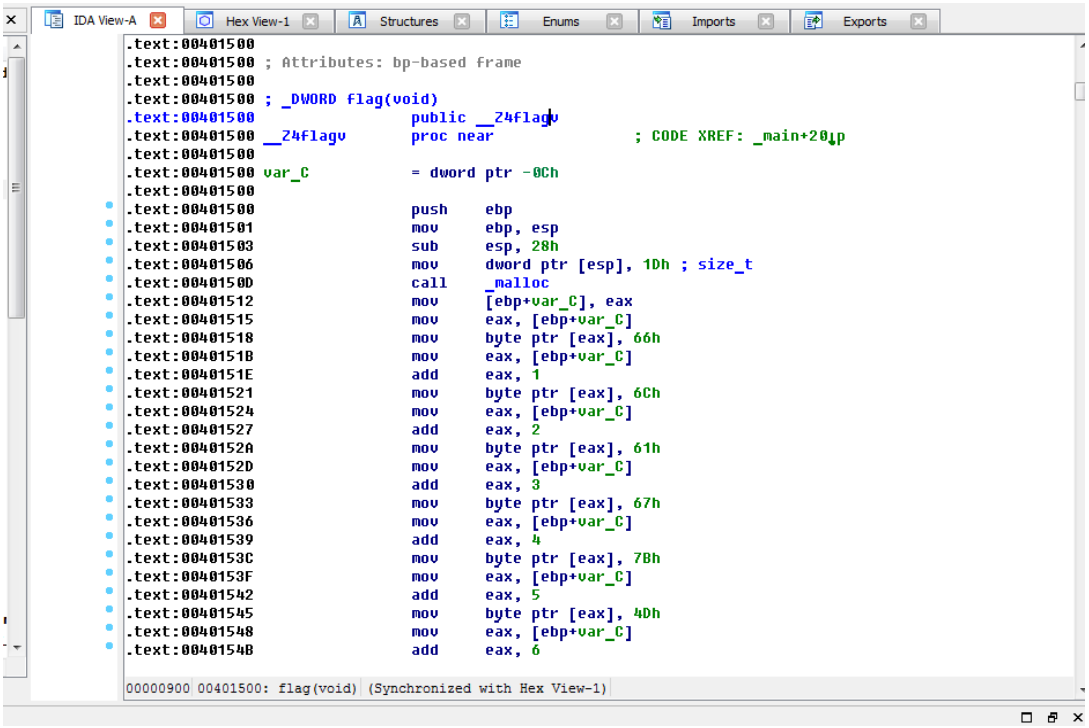


Рис. 6. Формирование флага

Таким образом, было получено представление о том, как работает программа. Данный пример иллюстрирует, как реверс-инжиниринг может применяться в решение задач информационной безопасности, а именно выявление недекларированных возможностей. Основное его назначение это узнать основные принципы функционирования ПО. Например, вместо безобидной программы может исследоваться вредоносное ПО, которое может скрывать свой вредоносный функционал под безобидным и нужным. С помощью анализа можно узнать его алгоритм функционирования, ликвидировать последствия заражения, создать иммунизаторы[2] и сигнатуры для антивирусных баз.

Список литературы

[1]. *Обратная* разработка [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/Обратная_разработка (дата обращения 22.10.2019)

[2] Иммунизаторы - это программы записывающие в другие программы коды, сообщающие о заражении. Они обычно записывают эти коды в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение.

[2] *Crackmes* [Электронный ресурс] URL: https://www.crackmes.one/crackme/5d63011533c5d46f00e2c305 (дата обращения 22.10.2019)

[3] *Майкл Сикорски, Эндрю Хониг.* Вскрытие покажет! Практический анализ вредоносного ПО. – 2018.– С.768.

Еськов Егор Сергеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: egor.esckov@yandex.ru

С.Г. Шитов

ПРОТОКОЛ ГЛОБАЛЬНОЙ МАРШРУТИЗАЦИИ BGP И ЕГО УЯЗВИМОСТИ

Общие сведения о протоколе BGP

Для понимания основных принципов маршрутизации в сети Интернет и осознания производимых в работе действий необходимо провести объяснение базовых понятий. Обмен маршрутами по протоколу BGP предполагает существование логических объединений устройств в автономные системы (AS).

Автономная система (AS) — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом. [1]

На рис. 1 представлены 5 автономных систем с номерами: 10, 200, 3400, 12, 809.

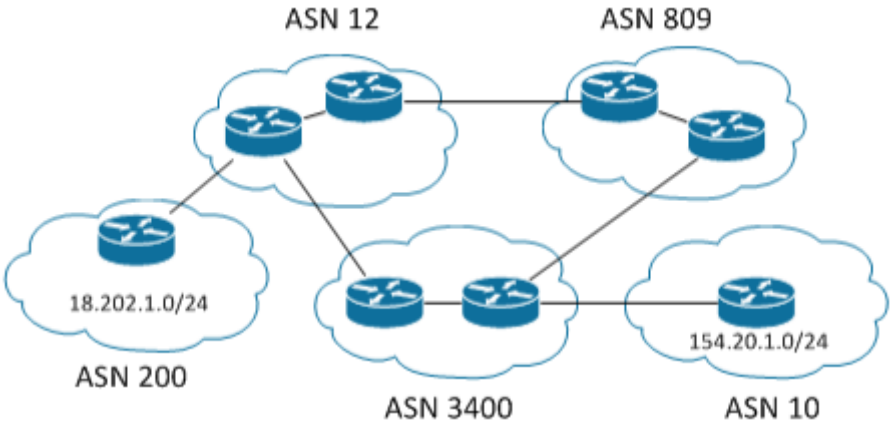


Рис. 1. Пример автономной системы

Все эти автономные системы – публичные. Номера AS выделяются Internet Assigned Numbers Authority, которая также выделяет IP-адреса, региональным интернет-регистраторам блоками. Локальные RIR затем присваивают организации номер AS из блока, полученного от IANA. Организации, желающие получить ASN, должны пройти процесс регистрации в своем локальном RIR и получить одобрение. Текущий список присвоенных ASN можно увидеть на веб-сайте IANA, более подробную информацию о владельце автономной системы можно запросить у RIR, выдавшего этот ASN.

Типы BGP соседств:

–Внутренний BGP (Internal BGP, iBGP) — BGP работающий внутри автономной системы. iBGP-соседи не обязательно должны быть непосредственно соединены. То есть между соседями должна существовать логическая связь, но не обязательно физическая;

–Внешний BGP (External BGP, eBGP) — BGP работающий между автономными системами. По умолчанию, eBGP-соседи должны быть непосредственно соединены, иметь прямое физическое подключение.

Если iBGP-маршрутизаторы работают в нетранзитной AS, то соединение между ними должно быть full mesh(каждый с каждым). Это следствие принципов работы протокола — если маршрутизатор, находящийся на границе AS, получил обновление, то он передает его всем соседям; соседи, которые находятся внутри автономной системы, больше это обновление не распространяют, так как считают, что все соседи внутри AS уже его получили.

На рис. 2 представлены графически типы BGP соседств.

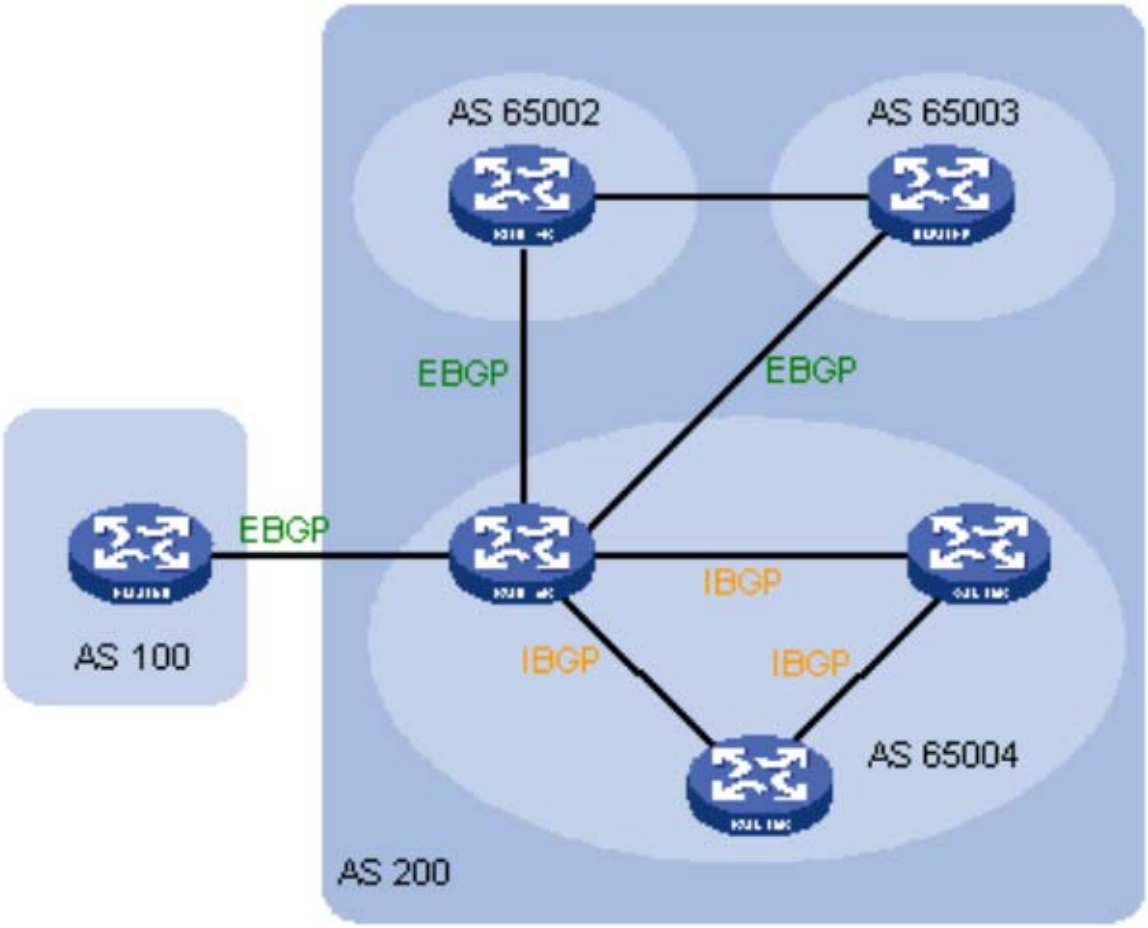


Рис. 2. Типы BGP соседств

Уязвимости протокола BGP

Недостатки работы протокола показывают уязвимости BGP и соответственно обязывают приступить к их исправлению. Так как протокол BGP работает по протоколу TCP на 173 порту и устанавливает внешние маршруты, а также прослушивает 179 порт, то соответственно BGP уязвим для атак на TCP. Также протокол имеет относительно низкое время сходимости. Протокол BGP еще можно назвать дистанционно-векторным протоколом, так как между маршрутизаторами передается не информация о состоянии линков, а сами маршруты.

Опасности данного протокола, которые обоснованы двумя ведущими уязвимостями:

1. BGP не содержит внутреннего механизма обеспечения крепкой обороны единства и актуальности данных, а еще аутентификации партнеров для извещений, передаваемых меж узлами BGP.

2. Отсутствует устройство обеспечения достоверности атрибутов пути, анонсируемых AS (autonomous system).

Так как протокол BGP используется для объединения сетей и обменом информацией между ними, то были рассмотрены типы сообщений BGP и уязвимости, связанные с ними.

У BGP имеются 4 типа сообщений:

–OPEN

–KEEPALIVE

–NOTIFICATION

–UPDATE

Внешние атакующие имеют все шансы применить неверные сообщения OPEN, KEEPALIVE, NOTIFICATION или же UPDATE для нарушения соединений среди партнеров BGP. Они имеют все шансы применить сообщения UPDATE для нарушения маршрутизации без разрыва соединений среди партнеров. Внешняя атака может не соблюсти ассоциации меж партнерами методом вставки неверных пакетов TCP, которые не соблюдают обработку соединений TCP. В целом способности внешних атакующих по использованию неверных извещений BGP и TCP ограничены (но не предотвращаются полностью), из-за обработки порядковых номеров TCP.

Партнеры BGP имеют все шансы сами разорвать соединения между собой в любой момент, применяя для сообщения NOTIFICATION. Внедрение извещений OPEN, KEEPALIVE или же UPDATE не провоцирует вспомогательного риска. Впрочем, партнеры BGP имеют все шансы не соблюсти картину маршрутизации (что вполне реально), применяя сообщения UPDATE, имеющие неверную информацию о маршрутах. В частности, неверные атрибуты ATOMIC_AGGREGATE, NEXT_HOP и AS_PATH, а также неточный смысл NLRI в сообщениях UPDATE могут дать все шансы не соблюсти маршрутизацию. Внедрение не мешает данному типу атак со стороны узлов BGP.[2]

Маршрутизация между автономными системами на основе протокола BGP также является одним из наиболее уязвимых элементов Интернета. Это объясняется, во-первых, тяжелыми последствиями неверной работы BGP-маршрутизаторов провайдеров, когда маршруты во многих частях Интернета вдруг исчезают или оказываются ложными для значительной части пользователей. Во-вторых, причина повышенной уязвимости протокола BGP по сравнению с внутренними протоколами маршрутизации OSPF или IS-IS является то, что «собеседники» BGP-маршрутизатора находятся за пределами административной ответственности его организации и поэтому возможностей для проверки достоверности маршрутных объявлений BGP намного меньше, чем в случае внутренних протоколов, когда администратор всегда может проверить конфигурацию любого маршрутизатора и понять причины некорректного или подозрительного поведения.[3]

О значительной части крупных инцидентов, произошедших в Интернете по "вине" протокола BGP, трудно сказать, так как неизвестно произошел ли этот инцидент из-за ошибки конфигурирования маршрутизатора персоналом провайдера или же эта была спланированная и осуществленная атака.

Описывая уязвимости BGP - маршрутизации появляется новое действующее лицо провайдер-злоумышленник (malicious ISP), который вольно или невольно создает проблемы для остальных провайдеров.

Возьмем, например, первый и широко-известный инцидент с BGP - маршрутизацией, который очень ярко выявил уязвимости BGP, которые затем много раз проявляли себя в аналогичных ситуациях. Такой инцидент произошел 25 апреля 1997 года. В этом случае многие провайдеры обнаружили, что в их маршрутизациях исчезли маршруты, списывающие путь к сетям Интернет. Оказалось, что виновником данного инцидента был единственный маршрутизатор одного клиента провайдера AS7007, который после реконфигурирования начал генерировать некорректные объявления не о своих сетях, причем с более специфическим адресом, чем адреса этих сетей в маршрутизаторах своего провайдера и большинства других провайдеров интернета, в результате чего их записи были вытеснены из таблиц маршрутизации этой более специфической описью.

Инцидент с AS7007 был первой масштабной демонстрацией уязвимости маршрутизации на основе протокола BGP, который был разработан, как и другие протоколы стека TCP/IP, в расчете на доброю волю всех пользователей Интернета и не имел никакой защиты от ошибок или недоброго умысла.

В дальнейшем подобные случаи повторялись достаточно регулярно, например, еще один инцидент с известным видеохостинговым сайтом «Youtube», который случился в 2008 году. В этом случае «Pakistan Telecom» пытался заблокировать доступ к «Youtube» для пользователей Пакистана, но вместо этого допустил утечку специфических маршрутов к «Youtube» в Интернет. Подобные инциденты являются следствием того, что маршрутное объявление BGP формируется шаг за шагом многими провайдерами, при этом достоверность информации каждого шага проверить невозможно, так как у провайдера имеется полная свобода действий при обработки маршрутного объявления и передаче его соединением провайдерам.

В данной статье были рассмотрены общие сведения о протоколе BGP и некоторые уязвимости, то есть слабые места работы протокола динамической маршрутизации BGP, которые помогли провайдерам усовершенствовать протокол для дальнейшей работы в сети Интернет. Выявлено, что основные уязвимости находятся в сообщениях при передаче информации между соседями, а также в маршрутизации между AS. На основе двух рассмотренных инцидентов, связанных с протоколом динамической маршрутизации BGP можно сделать вывод о несовершенстве его работы. На примере BGP-маршрутизации можно увидеть насколько незащищенным может быть протокол, при постороннем вмешательстве в его работу.

Список литературы

[1]. *Автономная* система (Интернет)// Wikipedia – свободная энциклопедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BD%D0%BE%D0%BC%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%28%D0%98%D0%BD %82%29 (дата обращения: 27.10.2019).

[2]. *BGP* или «протокол на трёх салфетках». [Электронный ресурс]. URL: http://blog.tran.su (дата обращения: 27.10.2019).

[3]. *RFC* 4272 — Анализ уязвимостей протокола BGP. [Электронный ресурс]. URL: http://muff.kiev.ua (дата обращения: 27.10.2019).

Шитов Сергей Геннадьевич – студент, ЗАО НПФ «Сигма». E-mail: barselona123@gmail.com

А.А. Чураков, А.В. Козина

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ МИНИМИЗАЦИИ ЛОГИЧЕСКИХ ВЫРАЖЕНИЙ МЕТОДОМ КВАЙНА-МАК-КЛАСКИ

Почти все булевы функции выражаются неоднозначно через исходные функции, исходя из этого, одной из задач при проектировании устройств на базе логических элементов является нахождение такой формы ее представления, которая позволяет построить электрическую схему так, чтобы использовать минимальное количество элементов. При решении данной задачи заданную булева функцию сначала удобнее представить в некоторой исходной канонической форме, называющуюся нормальной, а только затем преобразовать ее. Каноническими формами представления булевой функций являются совершенная дизъюнктивная нормальная форма (СДНФ) и совершенная конъюнктивная нормальная форма (СКНФ).

Способы минимизации

Существует несколько вариантов упрощения логических выражений:

–Равносильные преобразования (эквивалентные преобразования)

–Метод карт Карно (куб Карно, диаграмма Карно)

–Метод Квайна-Мак-Класки [1]

Для упрощения выражений в разрабатываемой программе был выбран метод Квайна-Мак-Класки из-за его возможности компьютеризации, и не большего усложнения с ростом количества переменных исходного выражения и усложнения самих выражений.

Этот метод заключается в следующем:

1. Термы, на которых определена заданная функция записываются в виде их двоичных эквивалентов;

2. Эти термы разбиваются на группы, в каждую группу входят термы с равным количеством единиц или нулей;

3. Производится попарное сравнение термов в соседних группах, с целью формирования термов более низких рангов;

4. Составляется таблица, строки в которой являются исходные термы, а столбцы — термы низких рангов;

5. Расставляются метки, отражающие поглощение термов высших рангов (исходных термов).

6. Термы, не подлежащие исключению, образуют ядро. Для каждого из них имеется хотя бы один столбец, перекрываемый только этой термой.

7. Для получения минимальной формы достаточно выбрать из терм, не входящих в ядро, такое минимальное их число с минимальным количеством букв в каждом из этих терм, которое обеспечит перекрытие всех столбцов, не перекрытых членами ядра [2].

Реализация системы

Разработанное приложение обеспечивает построение таблицы истинности по введённому логическому выражению, состоящему из элементарных логических операций: дизъюнкция, конъюнкция, отрицание, и предоставляет на основании данного выражения упрощенное логическое выражение методом Квайна-Мак-Класки.

Приложение создано с использование языка C++, обладающего высокой производительностью [3] и фреймворка Qt, обеспечивающего кроссплатформенность разработанного приложения [4].

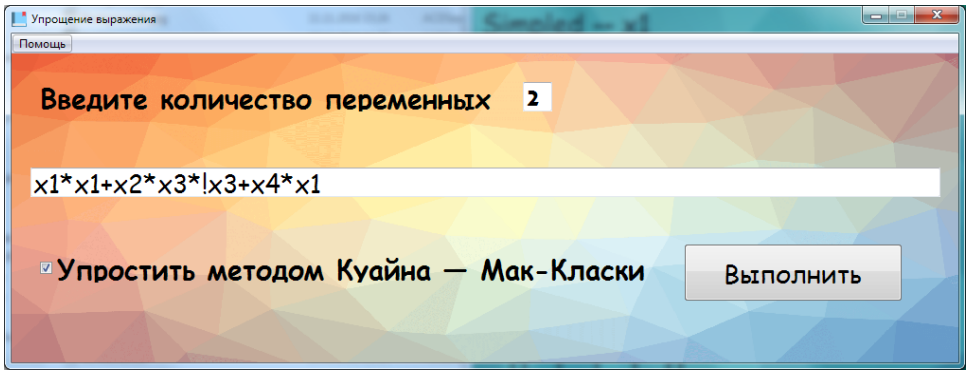


Рис. 1. Главное окно приложения

Графический интерфейс состоит из трех окон: главного окна, окна справки и окна результатов. В главном окне вводится логическое выражение и устанавливается флаг, отвечающий за то, будет ли выражение упрощено или только построена таблица истинности (рис. 1).

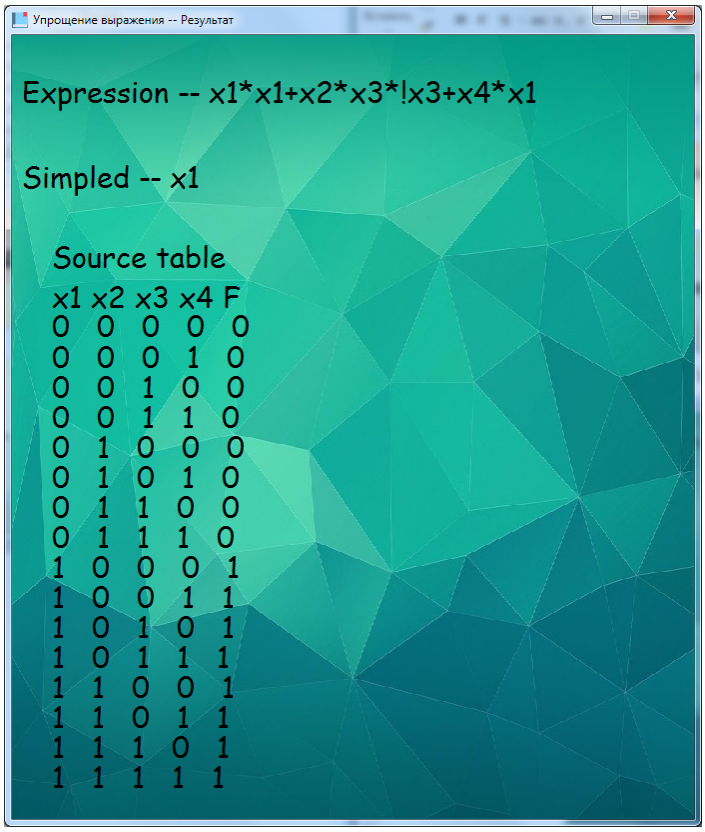


Рис. 2. Окно результата

В окне результата можно увидеть введенное исходное выражение, таблицу истинности для него и, если был установлен флаг упрощения выражения, упрощенное логическое выражение (рис. 2).

Заключение

В рамках данной работы было разработано кроссплатформенное приложение, которое минимизирует введенные пользователем логические выражения методом Куайна – Мак-Класки и строит его таблицу истинности.

Список литературы

[1] *Глухов М.М.* Математическая логика. Дискретные функции. Теория алгоритмов [Электронный ресурс] : учебное пособие / М.М. Глухов, А.Б. Шишков. — Электрон. дан. — Санкт-Петербург : Лань, 2012. — 416 с. — Режим доступа: https://e.lanbook.com/book/4041. — Загл. с экрана.

[2] *Ерусалимский Я.М.* Дискретная математика. Теория и практикум: учебник / Я.М. Ерусалимский. Санкт-Петербург: Лань, 2018. — 476 с. URL: https://e.lanbook.com/book/106869.

[3] *Рихтер Д.* Windows via C/C++. Программирование на языке Visual C++, СПб: Питер, 2016, с. 876.

[4] *Qt* 5.10. Профессиональное программирование на C++. - СПб.: БХВ-Петербург, 2018. - 1072 с.

Чураков Александр Александрович - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: jumandj@yandex.ru

Козина Анастасия Валерьевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasiya-kozin@list.ru

Е.М. Бандурина, А.В. Ткаченко, Ю.С. Белов

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ ИНФОРМАЦИИ

Введение. Антивирусные приложения, по сути, поставляются с каталогом уже проверенных вирусов и сопоставляют коды и шаблоны в файлах и веб-страницах с уникальными битами и шаблонами, которые составляют код вируса. Если они совпадают, файл помещается на карантин, что означает, что он перемещается в новое и безопасное место, чтобы в последствие не заразил никакие другие файлы в системе. Антивирусные программы также проверяет наличие любого вредоносного поведения в системе, например, подозрительные записи реестра или автозагрузка неизвестной программы при запуске системы, таким образом защищая наш компьютер от зашифрованных вирусов или вирусов, которые до сих пор не были идентифицированы или обнаружены[1]. Ниже будет произведен анализ работы различных методов обнаружения вирусов, которые антивирус может использовать для защиты компьютера.

Обнаружение сигнатур. Принцип сигнатур заключается в следующем – антивирусная лаборатория выявляет новый вирус с последующим анализированием, выявляя сигнатуру – особый цифровой признак вредителя (вроде отпечатка пальца). Сигнатуры вносят в базу, которую скачивает пользователь при последующем обновлении.

Для обеспечения успешного результата при использовании данного метода необходимо постоянно, желательно в онлайн режиме, пополнять базу обнаруженных антивирусных ПО новыми определениями. Сигнатуры загружаются в базу посредством анализа всех обнаруженных копий, принадлежащего одному вирусу. Сигнатуры должны содержать только уникальные части из файлов, довольно характерные и идентифицируемые, чтобы предотвращать даже минимальную возможность ошибочного срабатывания. Разработка сигнатур – ручной процесс, затруднительно поддающийся автоматизации. Несмотря на массу проведенных исследований посвящённых автоматической генерации сигнатур, нарастающий полиморфизм и «метаморфизм» вирусов и атак делают синтаксические сигнатуры бессмысленными. Антивирусные компании вынуждены выпускать большое количество сигнатур для всех вариантов одного и того же вируса, и если бы не закон Мура[3], ни один современный компьютер уже не смог бы закончить сканирование большого числа файлов с такой массой сигнатур в разумное время.

Перейдя непосредственно к анализу работоспособности, начнем с положительных черт метода сигнатур. Сигнатуры позволяют определить вирусную атаку с высокой точностью и малой долей ложных вызовов, метод является достаточно надежным, а также проверенным временем, ведь используется достаточно долго.

К недостаткам относится обязанность постоянного обновления сигнатур, так как большинство антивирусов не умеют обнаруживать новые вирусы самостоятельно. Также отрицательным является и тот факт, что доставка новых сигнатур до пользователей не всегда своевременная. Современные вирусы распространяются гораздо быстрее обнаружения, добавления и выпуска сигнатуры, не говоря уже о загрузки её в базу компьютера. Также стоит отметить огромное количество подобных троянов, которые имеют схожие сигнатуры. Из-за этого приходится разрабатывать шаблон, который вносится с базу, а затем на его основе разыскивается нежелательное ПО. При этом иногда могут возникать ложные срабатывания антивирусов.

Эвристическое сканирование. Еще одной наиболее распространённой формой обнаружения, которая использует алгоритм для сравнения сигнатур известных вирусов с потенциальной угрозой является эвристическое обнаружение. Большинство современные антивирусных приложений использует технология эвристического сканирования. Оно также часто применяется в совокупности с методом обнаружения сигнатур для поиска полиморфных вирусов. Антивирус, выпущенный с этой формой сканирования, также может обнаружить вирусы, которые еще не были идентифицированы и выпущены в качестве нового вируса, однако помимо этого он может генерировать ложноположительные совпадения, что означает, что антивирусный сканер имеет возможность сообщать о неинфицированном файле как о зараженном.

Несмотря на то, что эвристический анализ позволяет обнаруживать новые вирусы и уже существующие варианты вирусов, эффективность действительно низка с точки зрения количества ложных срабатываний . Это связано с тем, что компьютерные вирусы, как и биологические вирусы, постоянно меняются и развиваются. Поскольку эвристический анализ основан на сравнении подозрительного файла с другими уже известными вирусами, он часто пропускает некоторые вирусы, которые содержат новые коды или методы работы[2].

Обнаружение на основе поведения. Если вирус проходит вышеуказанные методы обнаружения, антивирус наблюдает за поведением программ, запущенных на компьютере. Он запускает предупреждение, если программа начинает выполнять странные действия, такие как изменение настроек других программ или удаленное подключение к компьютеру. Обнаружение на основе поведения- это полезный метод для поиска вирусов или любых других типов вредоносных программ, которые пытаются украсть или войти информацию.

Чтобы выявить, насколько описанные выше методы являются оптимальными для защиты информации, проанализируем запросы из интернета, где упоминается о том, что анализируемый экземпляр вирусного ПО совсем недавно начал свое распространение. Чаще всего это либо первая треть, либо середина активной фазы обработки его различными антивирусными компаниями. На основе информации, взятой в интернете, составим гистограмму,

где значения по вертикали—количество вирусных экземпляров, значения по горизонтали—количество сработавшего антивирусного обеспечения.

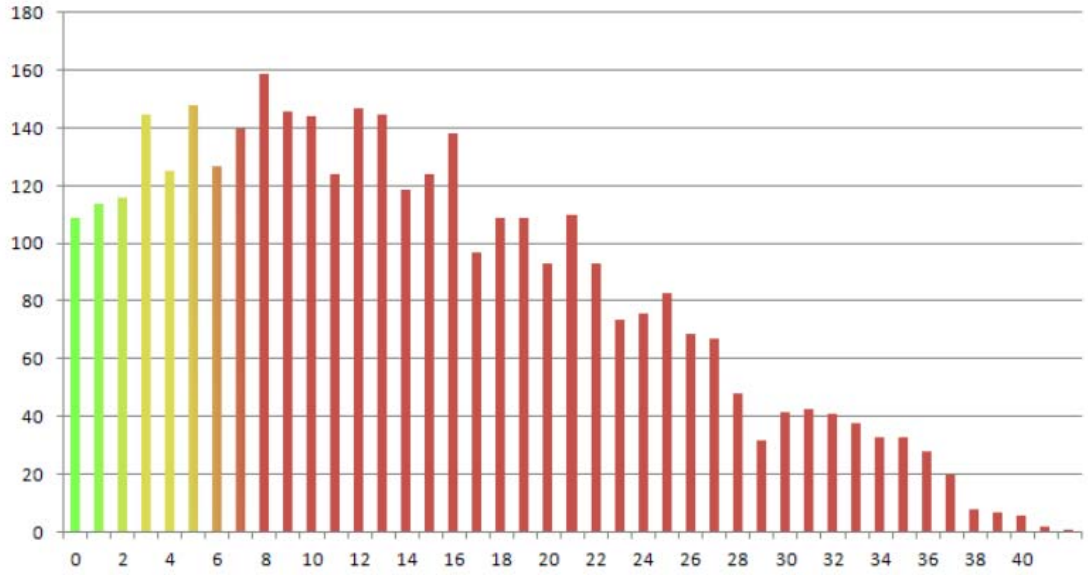


Рис. 1. Анализ обнаружение вирусного ПО приложениями от количества различных вирусных копий

Глядя на этот график, приходим к выводу, что в области, расположенной около 0 значения, а также с малоизвестным вирусным кодом находится очень много ложных срабатываний. Это означает, что эвристическое сканирование работает не особо успешно, слишком сильно злоупотребляя своей работой в обнаружение нового вида вирусных экземпляров. По сути, мы обнаружили одну из главных проблем поиска вирусов — ложные срабатывания. Далее посмотри, насколько хорошо с ней справляются современные антивирусные продукты. В данный момент, наибольший процент обнаружения вирусов(80%) за немецкой компанией GData. Тогда, изучив методы, которые они использует и сопоставив с изложенными выше, не беря в расчет технологию «двойного сканирования» придем к выводу что они всё же используют эвристику в большей степени, с поправкой на добавление новых возможностей и решений.

Список литературы

[1]. *Гульев И.А.* Создаем вирус и антивирус : учебное пособие / И.А. Гульев. — 2-е изд. — М: ДМК Пресс, 2006. — 304 с.

[2]. *Климентьев К.Е.* Компьютерные вирусы и антивирусы: взгляд программиста / К.Е. Климентьев. — М: ДМК Пресс, 2013. — 656 с.

[3] *Мейер Б.* Инструменты, алгоритмы и структуры данных : учебное пособие / Б. Мейер. — 2-е изд. — М: ИНТУИТ, 2016. — 542 с.

Бандурина Екатерина Михайловна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: bandurinakatya7@yandex.ru

Ткаченко Анастасия Владимировна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasiyatkach96@gmail.com

Белов Юрий Сергеевич - доцент, канд. физ.-мат. наук КФ МГТУ им. Н.Э. Баумана. E-mail: iu4-kf@mail.ru

И.Д. Феоктистов

СТРУКТУРА И ПРИНЦИП РАБОТЫ СИСТЕМ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современное веб-приложение состоит из большого количества систем и средств, которые отправляют различные события информационной безопасности (ИБ). Вне зависимости от количества уже внедренных средств защиты информации (СЗИ), если своевременно не реагировать на возникающие угрозы ИБ, то их эффективность стремится к нулю. Для решение данной проблемы необходимо внедрять систему мониторинга событий информационной безопасности [1].

Системы мониторинга событий ИБ – это системы, которые позволяют осуществлять [2]:

– Сбор, хранение, анализ событий ИБ;

– Корреляцию собранных событий и обнаружение инцидентов ИБ;

– Расследование и анализ инцидентов ИБ.

Задачи.

Системы мониторинга событий решает следующие задачи:

- Оперативное обнаружение, реагирование и контроль обработки инцидентов ИБ;
- Обнаружение новых типов инцидентов, которые не детектируются другими средствами ИБ;
- Контроль состояния ИБ для руководства организации;
- Создание единого центра мониторинга ИБ в организации;
- Автоматизации процесса обнаружение инцидентов ИБ;
- Снижения потерь в результате реализации рисков ИБ.

Структура.

Системы мониторинга событий ИБ в общем состоят из следующих модулей:

– агенты – это программы, расширения или плагины, которые входят в состав системы мониторинга событий ИБ, который выполняет функции переноса и преобразования записей системного журнала от целевой системы в коллектор системы мониторинга событий ИБ. Существуют безагентные системы мониторинга событий ИБ [3]. Такие системы самостоятельно передают записи системного журнала коллектору, что снижает нужду в установке агента;

– сервер-коллектор – это сервер, который собирает и структурируют события от множества источников;

– сервер-коррелятор – это сервер, который собирает и обрабатывает информацию от коллекторов и агентов. После получения и категорирования событий, применяются конкретные политики.

Существует два типа политик:

•генеральная серверная политика, которая применяется к каждому входящему событию;

•специальные политики для определенных событий, они используются для фильтрации событий и упрощения работы.

Корреляция применяется для снижения числа ложных срабатываний системы и изменения приоритета и вероятности события, после чего происходит оценка рисков. Оценка рисков строится на трех факторах: приоритет, вероятность, ценность системы;

– сервер баз данных – это сервер, который хранит журналы событий.

Принцип работы (рис 1.)**.**

Системы мониторинга событий ИБ - это платформа, которая позволяет собирать события от различных ИТ- и ИБ-устройств, которые уже развернуты в сети вашей организации [4], такие как:

– Серверы приложений;
– Базы данных;
– Межсетевые экраны и IPS;
– Различные активные сетевые устройства;
– Средства антивирусной защиты;
– Системы обнаружения и предотвращения утечек информации;
– Любое другое устройство, расположенное в сети вашей организации.

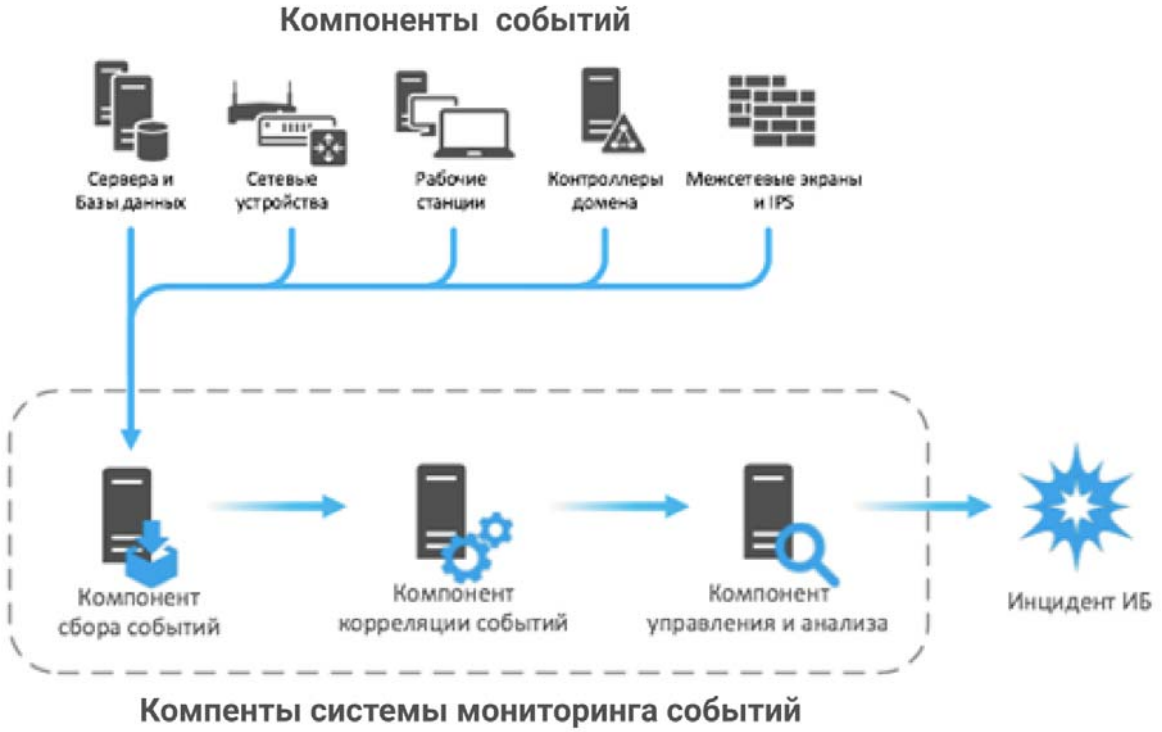


Рис. 1. Принцип работы системы мониторинга событий ИБ

Система мониторинга событий ИБ собирает информацию из различных источников с помощью агентов и серверов-коллекторов в централизованное хранилище данных, что позволяет впоследствии анализировать события в

целом. После сбора информации системы мониторинга событий ИБ начинает анализ этих событий, требующийся для обнаружения инцидента. Для этого применяются два основных метода корреляции:

– Сигнатурный – метод, основанный на правилах;

– Бессигнатурный – метод, основанный на поиске аномального поведения информационной системы.

По результатам анализа данная система показывает выявленные инциденты ИБ. Для того чтобы система мониторинга событий ИБ эффективно выполняла свои задачи в конкретной организации, требуется правильная конфигурация корреляционных механизмов и постоянная их модификация. Такие системы начинают окупать себя значительно позже ее внедрения, особенно при применении бессигнатурных методов корреляции, которые требуют накопления статистических данных.

Список литературы

[1] *Шелестова О.* Что такое SIEM? URL: http://blog.ptsecurity.ru/2012/10/siem.html. (дата обращения 30.10.2019)

[2] *Мониторинг* событий ИБ, StyleTelecom. URL: http://styletele.com/Solutions/informatsionnaya-bezopasnost/monitoring-sobytiy-ib-siem (дата обращения 30.10.2019)

[3] *Золутихин А.В, Тимохович А.С.* Прицип работы и типовая структура средств управления событиями безопасности инфомации. URL: https://cyberleninka.ru/article/v/printsip-raboty-i-tipovaya-struktura-sredstv-upravleniya-sobytiyami-bezopasnosti-informatsii (дата обращения 30.10.2019)

[4] *Сравнение* SIEM-систем, СёрчИнформ SIEM.URL: https://searchinform.ru/products/siem/sravnenie-siem-sistem/ (дата обращения 30.10.2019)

Феоктистов Илья Дмитриевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: feoktistov.ilya@yandex.ru

А.Е. Юнеева, А.В. Козина, Ю.С. Белов

УЯЗВИМОСТИ В БЕЗОПАСТНОСТИ НЕЙРОННЫХ СЕТЕЙ

Введение. Нейронные сети и глубокое обучение в настоящее время обеспечивают лучшие решения многих проблем в распознавании изображений, распознавании речи и обработке естественного языка. Нейронные сети на данный момент – очень перспективная и распространенная технология, которая, как и другие разработки в области программного обеспечения может поддаваться взлому.

Нейронные сети становятся все более и более повсеместными в современном мире, и они часто внедряются без особого рассмотрения их потенциальных недостатков безопасности. Это привело к появлению новой области кибербезопасности, которая рассматривает уязвимости нейронных сетей и то, как мы можем защитить их от использования хакерами.

Виды атак. В классификации хакерских атак существует два основных типа: атаки белого ящика и атаки черного ящика.

Атака белого ящика происходит, когда кто-то имеет доступ к базовой сети. В этом случае становится известна архитектура сети. Как только станет понятно, как структурирована нейронная сеть, хакеры получат необходимые знания, которые позволят им внедрить неправильные действия, поскольку знание структуры сети может помочь выбрать наиболее опасные атаки, а также выявить слабые места, относящиеся к структуре сети.

Атака черного ящика происходит, когда знаний о базовой сети нет. Архитектуру нейронных сетей можно рассматривать как черный ящик. Даже если атаковать черный ящик трудно, оставить его непроницаемым остается маловероятным. Для атаки необходима нейронная сеть, как определенный механизм, считывающий изображение и выдающий вероятности принадлежности его типам. Таким образом, в данном методе необходимо знать данные о входных изображениях.

Уязвимости нейронных сетей. Нейронные сети являются универсальными аппроксиматорами функций. Это означает, что если данная нейронная сеть имеет достаточно большую емкость (достаточное количество узлов - весов и смещений), то в данной задаче появляется возможность аппроксимировать любую нелинейную функцию, используя нейронную сеть. Однако у вышесказанного существует некая условность - сети могут быть весьма чувствительны к вводимым данным. Поэтому относительно легко обмануть сеть, если вы знаете верные методы. Управляя определенными узлами изображений, появляется возможность активировать нейроны, связанные с некоторыми функциями, которые могут заставить сеть давать ложные результаты. Голосовой помощник – технология, которая работает с помощью нейронной сети, следовательно при правильном подходе к алгоритму взлома, у хакеров появляется возможность получить доступ к вашим личным данным. Отсюда и возникает вопрос об уязвимостях нейронных сетей.

По сути, атаки на нейронные сети включают введение стратегически размещенного шума, предназначенного для обмана сети путем ложного стимулирования потенциалов активации, которые важны для получения определенных результатов. Такой метод называется «состязательная атака». Иными словами, в изображении шума происходит изменений некоторых пикселей, вследствие чего нейронная сеть начинает выдавать некорректный результат (рис.1):

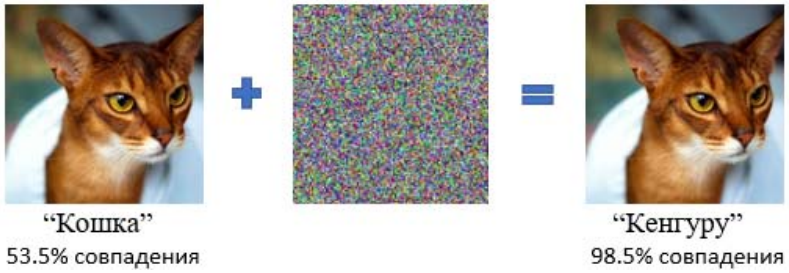


Рис. 1 Применение «состязательной атаки» для изменения результата

Существует много алгоритмов искажения изображения, все они состоят из следующих этапов: получение входного изображения заданной нейронной сети, создание неправильных пикселей, сложение пикселей неправильного изображения со пикселями изображения, заданного первоначально. В математическом представлении переменные x и x' - исходное изображение и изображение искаженное. Тогда уравнение неправильного изображения выглядит следующим образом: $x' = x + \Delta$. Несмотря на то, сколько правильных изображений будет получено на вход, вероятность сломать нейросеть искаженным изображением всегда будет иметь некоторый процент.

Заключение. На данный момент нейронные сети пока что находятся на начальных этапах разработки, и в это время существуют большие риски, связанные с их безопасностью. В теории существуют способы обхода таких взломов, как «состязательная атака» и т.п., при которых возможно было бы обучить нейросеть помнить конкретные модели и смысловые пиксели, благодаря чему вероятность сбить верный ответ стремится к нулю. Однако решение таких проблем находится еще на этапе разработки и, возможно, в дальнейшем найдет свое применение в защите работ нейросетей.

Список литературы

[1] *Нелинейное* программирование [Электронный ресурс]//Интернет-энциклопедия “Википедия”: сайт - Режим доступа: https://en.wikipedia.org/wiki/Nonlinear_programming (Дата обращения 05.11.2019)

[2] *Нейронные* сети и глубокое обучение [Электронный ресурс]// Научное пособие “ Neural Networks and Deep Learning ”: сайт - Режим доступа: http://neuralnetworksanddeeplearning.com/index.html (Дата обращения 03.11.2019)

[3] *Практические* атаки черного ящика против машинного обучения [Электронный ресурс]//Электронный журнал “Cornell university”: сайт - Режим доступа: https://arxiv.org/abs/1602.02697 (Дата обращения 05.11.2019)

Юнеева Анастасия Евгеньевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: skyferryan@gmail.com

Козина Анастасия Валерьевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasiya-kozin@list.ru

Белов Юрий Сергеевич - доцент, канд. физ.-мат. наук КФ МГТУ им. Н.Э. Баумана. E-mail: iu4-kf@mail.ru

СЕКЦИЯ 9.

ДИНАМИКА, ПРОЧНОСТЬ И НАДЕЖНОСТЬ ПОДЪЕМНО-ТРАНСПОРТНЫХ, СТРОИТЕЛЬНЫХ, ДОРОЖНЫХ МАШИН И ОБОРУДОВАНИЯ

Н.Г. Сысенко, А.Г. Черенков, М.А. Карпов, В.А. Ермоленко

ВЗВЕШИВАНИЕ ГРУЗОВ ПРИ ЭКСПЛУАТАЦИИ СТРЕЛОВОГО КРАНА

Краны стрелового и передвижного типа предназначены для выполнения строительно-монтажных операций на малоэтажном строительстве, а также для механизации работ при погрузочно-разгрузочных работах на железнодорожном транспорте.

Кран состоит: из рельсовой тележки 1 (рис. 1); стрелы 2, закреплённой с помощью оттяжки 4; механизма подъёма груза 3; поворотной рамы с противовесом 5. Тележка установлена на четырёх одноребордных колёсах 6 и имеет возможность передвигаться по рельсам.

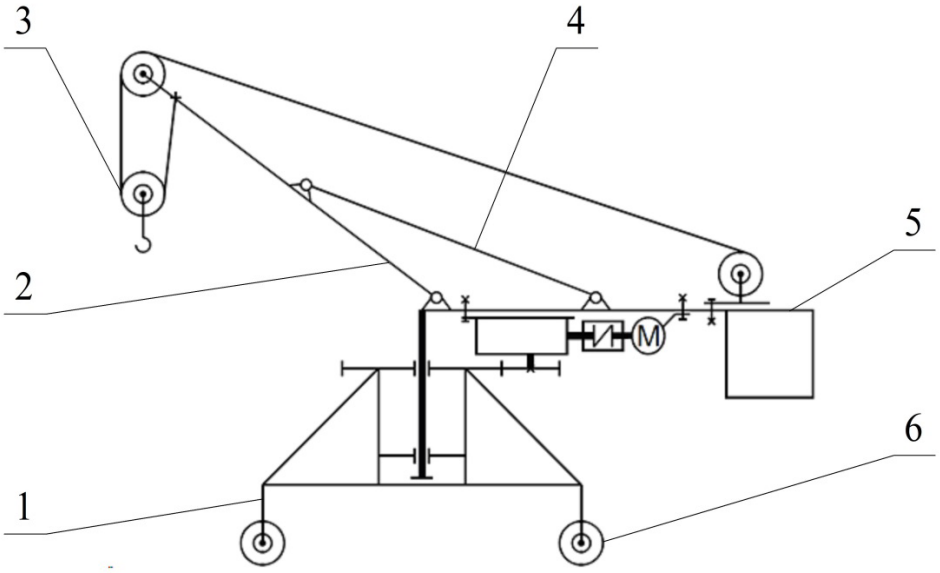


Рис. 1. Кран стреловой передвижной типа «Пионер» [1].

Ограничитель грузоподъёмности или крановые весы на этом кране заводом-изготовителем [1] не предусмотрены.

Целью работы является оснащение кранов разработанными нами приборами-индикаторами массы груза и проверка точности индикатора массы груза. Для установления соответствия показаний индикатора истинному значению массы груза был проведен эксперимент. На стреловой кран «Пионер» (рис. 1), под оттяжку, установили указатель массы груза (рис. 2). Прибор состоит из тензометрической пружины и индикатора часового типа с ценой деления 1 мкм. Затем, поочерёдно, с помощью крана, поднимали грузы разной массы. Результаты заносили в табл. 1.

Построены экспериментальная и теоретическая зависимости показаний индикатора от массы груза. Получена зависимость линейного характера:

$$m = k \cdot \delta, \qquad (1)$$

где m – масса груза, кг; k – коэффициент тарировки; δ – показания индикатора, мкм.

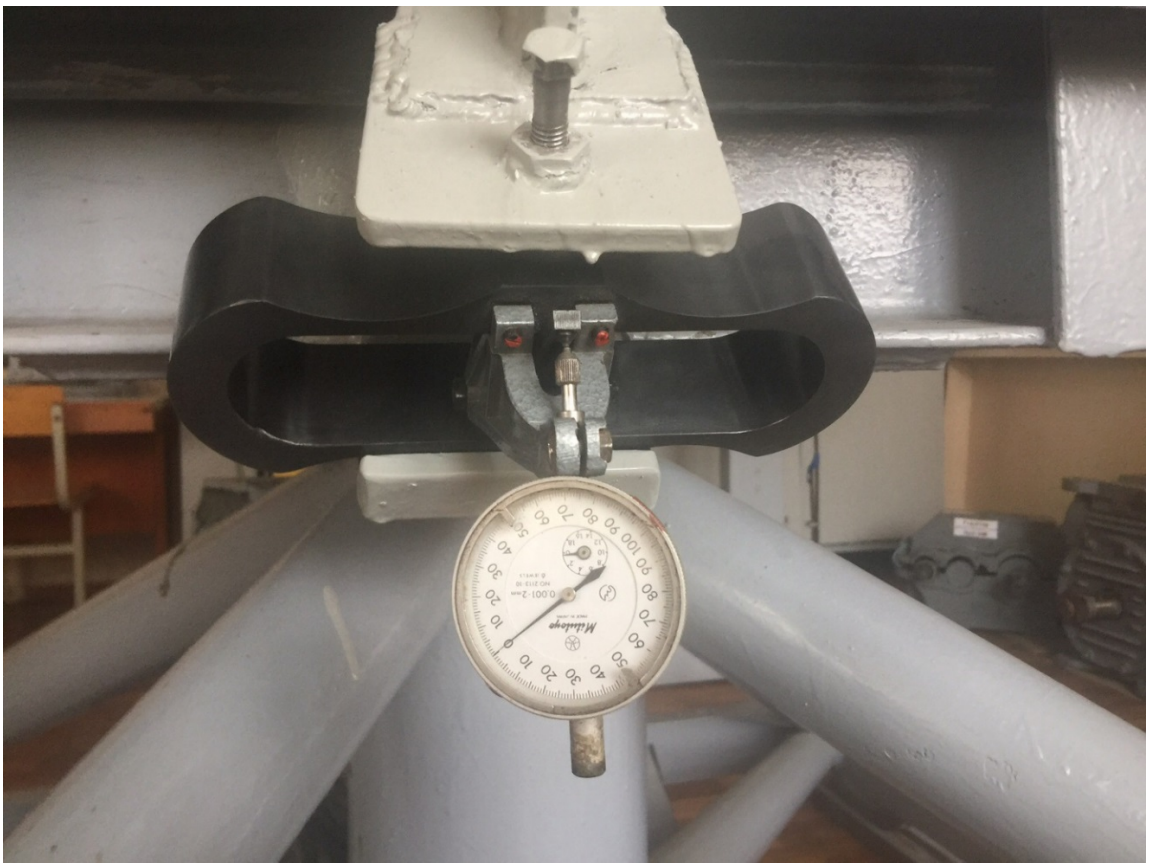


Рис. 2. Тензометрическое кольцо с индикатором

Таблица 1.

Тарировка индикатора

Груз	m, кг	δ, мкм	m_y, кг	ε, %	$\varepsilon_{ср}$, %
Гиря	5	14	4,9	1,8	4
Гиря	10	29	10,2	1,7	
Поддон	12,5	37,5	13,2	5,21	
Гиря	15	43,4	15,2	1,47	
Гиря	20	59	20,7	3,46	
Гиря	25	76	26,7	6,61	
Гиря	30	94	33	9,89	
Поддон и плита	54	162	56,8	5,21	
Поддон и две плиты	94,5	274	96,1	1,68	
Поддон и три плиты	136	375	131,51	3,3	

Полученное уравнение регрессии (2) (рис. 3):

$$m_y = 0{,}351 \cdot \delta; \qquad (2)$$

где m_y – заданная масса груза; δ – показания индикатора. Коэффициент корреляции $R^2 = 0{,}9974$ [2,3]. Среднее значение погрешности 4 %.

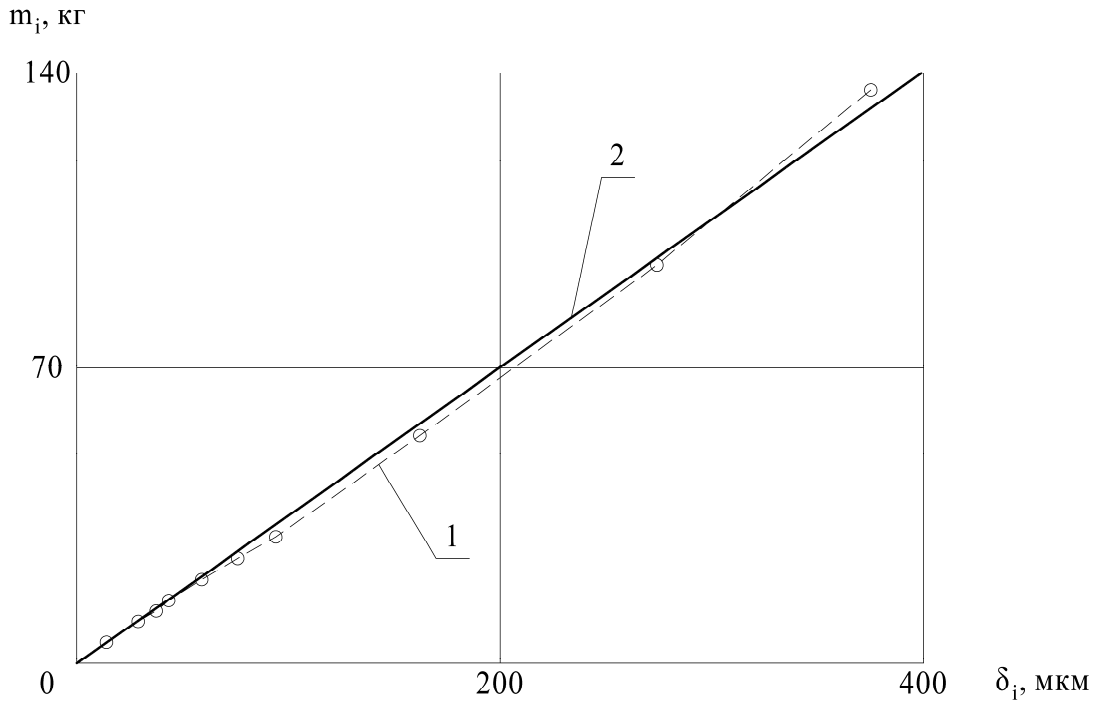


Рис. 3. График экспериментальной (*1*) и теоретической (*2*) зависимостей показаний индикатора от действительного значения массы взвешиваемого груза.

Получены результаты взвешивания различных реальных изделий при помощи данного индикатора:

Таблица 2.

Взвешивание изделий

Изделие	Результат взвешивания, кг	Масса по каталогу, кг
ТКТ – 100	12	Не более 12 [4]
ТКГ – 160	22,5	Не более 25 [5]
ТКГ – 200	27	Не более 30 [5]
Ц2У – 60	88,5	Не более 95 [6]

Вывод: в ходе эксперимента получена зависимость массы взвешиваемых грузов от показаний на индикаторе с погрешностью не более 4%. Это приемлемо при выполнении лабораторных работ. Расхождение результатов взвешивания и масс по каталогу в пределах 1 – 2 кг можно объяснить тем, что лабораторные образцы были взвешены до издания каталогов, т.е. до модернизации изделия.

Список литературы

[1]. *Кран* «Пионер». ООО «ПКЗ» Подольск. [Электронный ресурс]. URL: http://podolsk-kran.ru/katalog/stroitelnye-krany/kran-pioner/ (дата обращения 11.06.19).

[2]. *Адамов А.А.* Теория вероятностей и математическая статистика. Прикладная статистика с использованием MS Excel: учебное пособие. – Пермь; Издательство ПГТУ, 2008. – 174 с.

[3]. *Кобзарь А. И.* Прикладная математическая статистика. Для инженеров и научных работников. – М.: ФИЗМАТЛИТ, 2006. – 816 с.

[4]. *НПО* «ПРОМТЕПЛОСТРОЙ». [Электронный ресурс]. URL: https://www.kontaktor.su/tormoz-kolodochnyj-tkt.html (дата обращения 11.06.19).

[5]. *НПО* «ПРОМТЕПЛОСТРОЙ». [Электронный ресурс]. URL: https://www.kontaktor.su/tormoza--kolodochnye.html(дата обращения 11.06.19).

[6]. *НПО* «ПРОМТЕПЛОСТРОЙ». [Электронный ресурс]. URL: https://www.kontaktor.su/c2u-160.html (дата обращения 11.06.19).

Сысенко Никита Григорьевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: nikita.sisenko@gmail.com

Черенков Александр Григорьевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: al.cherenckov2013@yandex.ru

Карпов Максим Алексеевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: karpovmaksim.ru@mail.ru

Ермоленко Владимир Алексеевич – канд. техн. наук, доцент кафедры «Детали машин и подъемно-транспортное оборудование» КФ МГТУ им. Н.Э. Баумана. E-mail: tvermolenko@yandex.ru.

Д.В. Зайцев

ЗАЩИТА ПОДШИПНИКОВ КАЧЕНИЯ И ЗУБЧАТЫХ КОЛЕС НА ВИБРОПРЕССАХ С ПОВЫШЕННОЙ ЧАСТОТОЙ ВИБРАЦИИ

Вибропресс предназначен для уплотнения бетонной смеси в формах при изготовлении бетонных и железобетонных изделий. Под действием вибрации бетонная смесь приобретает подвижность, обеспечивающее хорошее заполнение формы. Плотность бетонной смеси увеличивается за счет как более компактной укладки частиц заполнителя, так и выделением из смеси пузырьков воздуха. При чрезмерно длительном вибрировании начинается ее расслоение. Поэтому должно быть установлена продолжительность вибрирования. Для достижения лучшего качества уплотнения бетонной смеси часто применяют комбинации различных способов вибрирования. Предполагаем, что увеличение частоты вибрации при формовании блоков и тротуарной плитки из мелкозернистого бетона увеличен до 75…100 Гц способствует повышению их прочности и огнестойкости.

К формуемым бетонным изделиям предъявляются требования среди которых обеспечение достаточной прочности, стойкости к изменению температуры – морозостойкости и теплостойкости. Снижение показателей по указанным критериям приводит к преждевременному разрушению конструкций и к аварийным ситуациям.

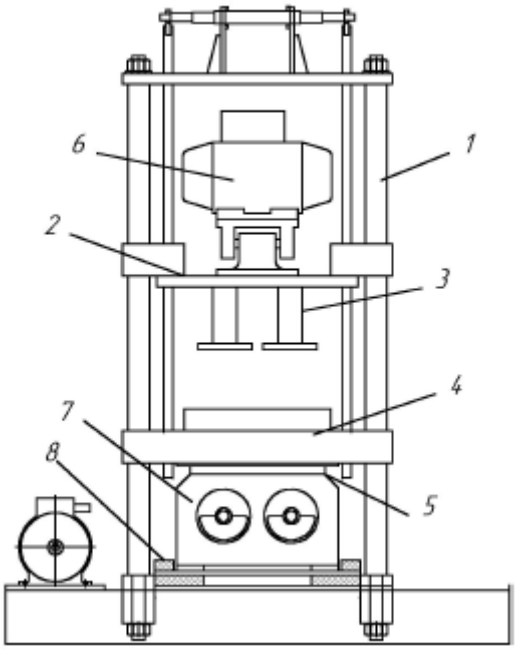


Рис. 1.

Для подтверждения правильности предположения проведен эксперимент на лабораторном вибропрессе (конструкции ХГТУСА) с регулируемым приводом. Вибропресс (рис.1) включает направляющие *1*, траверсу *2* с блоком пуансонов *3*, элементы блока матрицы *4*, *5*, вибропривод пуансонов *6*,

вибропривод блока матрицы *7* и упругие опоры *8*. В эксперименте принята мелкозернистая бетонная смесь жёсткостью порядка 30 с; на постоянных уровнях поддерживались значения: времени процесса формования t = 5 с; статического давления на бетонную смесь p = 0,1МПа; амплитуда колебаний A = 0,8 мм. При фиксированных значениях частот виб-рации были отформованы, выдержаны и подвергнуты разрушению на прессе, в соответствие с требованиями стандартных методик, бетонные изделия. Получены следующие результаты, усреднённые по трём параллельным сериям (табл. 1).

Таблица 1

Частота , Гц	50	55	60	65
Плотность *, кг/м3*	1970	2060	2166	2180
Прочность на сжатие R, МПа	17,7	20,3	25,8	30,7

Получен прирост плотности и прочности на сжатие бетонных образцов при изменении частоты вибрации, что даёт основание ожидать повышения их огнестойкости.

Вместе с тем проблемным остаётся научно обоснованное прогнозирование степени влия-ния регулирования частоты на долговечность и эксплуатационные показатели элементов вибропривода. Оценим это влияние на примере зубчатых конструкций виброприводов пресса, например такого, как на рис. 1.

Исследуем вопросы, связанные с регулированием частоты вращения валов привода вибропресса (например, в диапазоне 50…75 Гц). При этом амплитуда суммарной возмущающей силы вибровозбудителей $F=mr\omega^2$, а также на подшипник $R = 0,25Fk_1k_2$ изменяются пропорционально квадрату отношения сторон $\frac{F_2}{F_1} = \left(\frac{\omega_2}{\omega_1}\right)^2$; $\frac{R_2}{R_1} = \left(\frac{\omega_2}{\omega_1}\right)^2$, где где F - сила вибровозбудителей; ω- угловая скорость; R - радиальная нагрузка.

Мощность на трение в подшипниках вибратора $N=0,5f\omega^3mrd$ изменяется пропорционально кубу отношения частот:

$$\frac{N_2}{N_1} = \left(\frac{\omega_2}{\omega_1}\right)^3$$

Срок службы подшипника при динамической грузоподъёмности C определяется как $L = \left(\frac{C}{R}\right)^m$ и изменяется пропорционально отношению частот в степени 2m:

$$\frac{L_2}{L_1} = \left(\frac{C}{R_2} \cdot \frac{R_1}{C}\right)^m = \left(\frac{R_1}{R_2}\right)^m = \left(\frac{\omega_1}{\omega_2}\right)^{2m}$$

$$L_2 = L_1 \cdot \left(\frac{\omega_1}{\omega_2} \right)^{2m}$$

Так, при m=3 (для шарикового подшипника) имеем:

$$\frac{L_2}{L_1} = \left(\frac{\omega_1}{\omega_2} \right)^6$$

и при m =10/3 (роликовый) получаем:

$$\frac{L_2}{L_1} = \left(\frac{\omega_1}{\omega_2} \right)^{6,67},$$

т.е. происходит резкое снижение ресурса подшипников при увеличении частоты вращения вала.

Для зубчатой передачи вибропривода при изменении частоты вращения изменение допустимых контактных напряжений активных поверхностей зубьев:

$$[\sigma]_H = \frac{\sigma_{H\lim b}}{S_H} \cdot Z_R \cdot K_{HL},$$

где $\sigma_{H\lim b}$ - предел выносливости поверхности зубьев; Z_R - коэффициент шероховатости; S_H - коэффициент запаса; K_{HL} - коэффициент долговечности:

$$K_{HL} = \sqrt[6]{\frac{N_{HO}}{N_{HE}}} \; ; \; N_{HE} = 1800 \cdot i \cdot \omega \cdot \frac{h}{\pi} \; ; \; \frac{[\sigma]_{H_2}}{[\sigma]_{H_1}} = \sqrt[6]{\frac{\omega_1}{\omega_2}}$$

При эксплуатации, обслуживании и ремонте усовершенствованной машины можно прогнозировать изменение энергетических, прочностных и эксплуатационных показателей при увеличении частоты вибрации:

- повышение мощности привода
- уменьшение интервала времени между заменами подшипников (или подбор подшипников большей динамической грузоподъёмности)
- снижение допускаемых напряжений, т.е. необходимость повышения прочности зубчатых колёс и оснастки

Таким образом можно сделать вывод, что для повышения прочности и морозостойкости формуемых на вибропрессах бетонных мелкозернистых изделий увеличивать частоту вибрации до 75…100 Гц. При увеличении частоты вибрации бетонная смесь приобретает подвижность, обеспечивается хорошее заполнение формы, повышается прочность изделия. Получены зависимости, позволяющие учитывать влияние изменений параметров вибрации на долговечность и эксплуатационные показатели элементов привода вибропресса. В тот же момент нужно решить проблемы долговечности работы рабочих элементов электропривода вибропресса.

Результатом данной научно-исследовательской работы будет являться повышение прочности и морозостойкости формуемых на вибропрессах бетонных изделий, базирующийся на увеличении частоты вибрации до

75…100 Гц, а также предусмотрены способы увеличения долговечности подшипников и зубчатых колес.

Список литературы

[1]. *Электромеханические* системы автоматизации стационарных установок / под общ. редакци-ей В.Ф. Борисенко. – Донецк: ДонНТУ, НПФ «МИДИЭЛ», 2005. – с. 208-211.

[2]. *Уткин В.Л.* Новые технологии строительной индустрии. – М.: ЗАО «Русский издательский дом», 2004. – 116 с

[3]. *СП* 24.13330.2011 Свайные фундаменты. Актуализированная редакция СНиП 2.02.03-85 (с Опечаткой, с Изменением N 1) URL: http://docs.cntd.ru/document/1200084538

Зайцев Дмитрий Владимирович - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: zaitsevdima19951@yandex.ru

И.Н. Кириллов, С.Л. Заярный

ИССЛЕДОВАНИЕ КОНТАКТНЫХ ВЗАИМОДЕЙСТВИЙ В БОЛТОВЫХ СОЕДИНЕНИЯХ ПЕРЕМЕННОЙ СТРУКТУРЫ В ХОДЕ АКТИВНОГО ЭКСПЕРИМЕНТА

Фрикционные соединения на высокопрочных болтах следует рассматривать как совокупность элементов, подчиняющихся различным механизмам повреждаемости, но взаимосвязанных условиями функционирования. Определение степени взаимовлияния и взаимозависимости степеней поврежденности элементов такого соединения возможно только на основе проведения экспериментальных исследований. При этом может быть установлена степень поврежденности соединения в целом, как производная величина от степени поврежденности составляющих его элементов. [1]

Воспользуемся методами планирования эксперимента и представим исследуемый объект как «черный ящик», имеющий входы $x_1, x_2 ... x_n$ (управляемые независимые параметры) и выход *y*. Интересующее нас свойство *y* объекта зависят от *n* независимых переменных $(x_1, x_2 ... x_n)$ и мы хотим выяснить характер этой зависимости – $y = f(x_1, x_2 ... x_n)$ о которой имеем лишь общее представление. Величина *y* является откликом, а сама зависимость $y = f(x_1, x_2 ... x_n)$ – функцией отклика. Переменные x, принято называть факторами. Также на объект воздействуют возмущающие факторы, они являются случайными и не поддаются управлению. [3]

При исследовании болтового соединения нам будет необходимо постоянно вносить изменения и коррективы в проходящие во время эксперимента процессы, поэтому будем проводить активный эксперимент.

Согласно вышесказанному, нами было определено 7 факторов, оказывающих влияние на силу трения между контактирующими поверхностями в болтовом соединении.

Введем обозначение наших факторов: x_1 – структура соединения (число соединяющих болтов); x_2 – суммарная сила затяжки болтового соединения; x_3 – качество контактирующих поверхностей (необработанная, обработанная); x_4 – температура, при которой работает болтовое соединение (нормальная, отрицательная); x_5 – наличие или отсутствие смазки в соединении; x_6 – наличие различных поверхностно-активных веществ; x_7 – фактор старения (релаксации).

Все факторы кроме второго являются качественными, факторы x_5, x_6 являются физически несочетаемыми, а факторы x_4, x_7 являются несочетаемыми в располагаемых условиях испытаний. С учетом этих особенностей целесообразно рассмотреть четыре матрицы планирования эксперимента (табл. 1):

2^4 с факторами x_1, $x_2 x_3$, x_6; 2^4 – с факторами x_1, $x_2 x_4$, x_5; 2^4 – с факторами x_1, $x_2 x_5$, x_7; 2^4 – с факторами x_1, $x_2 x_6$, x_7.

Таблица 1.

Матрица планирования ПФЭ 2^4

Номер опыта	x_1	x_2	x_3	x_6	y	Номер опыта	x_1	x_2	x_3	x_6	y
1	–	–	–	–	y_1	9	–	–	–	+	y_9
2	+	–	–	–	y_2	10	+	–	–	+	y_{10}
3	–	+	–	–	y_3	11	–	+	–	+	y_{11}
4	+	+	–	–	y_4	12	+	+	–	+	y_{12}
5	–	–	+	–	y_5	13	–	–	+	+	y_{13}
6	+	–	+	–	y_6	14	+	–	+	+	y_{14}
7	–	+	+	–	y_7	15	–	+	+	+	y_{15}
8	+	+	+	–	y_8	16	+	+	+	+	y_{16}

Испытания планируется проводить на разрывной машине МИ-40КУ (рис. 1.), которая используется совместно с компьютером и обеспечивает построение диаграмм зависимости силы от деформации на дисплее.

Рис.1. Стенд МИ-40КУ с испытываемым образцом

На разрывной машине МИ40КУ установлено специальное программное обеспечение, позволяющее обрабатывать полученные данные и выводить результат в виде диаграммы зависимости усилия от деформации (рис. 2).

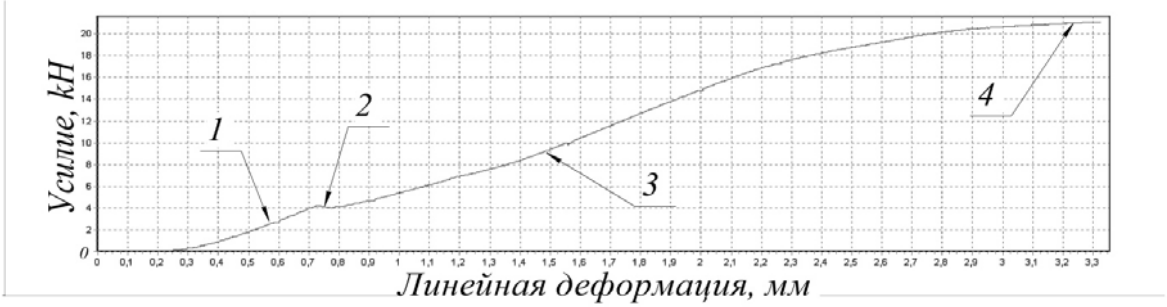


Рис. 2. Диаграмма зависимости усилия от деформации

Проанализировав полученную диаграмму можно выделить четыре характерных участка: участок 1 – линия упругой деформации пластин; участок 2 – момент времени, когда усилие растяжки превысило силу трения между пластинами образца; участок 3 – линия упругой деформации болтов вместе с пластинами; участок 4 – линия пластической деформации пластин образца.

Конструкция образца фрикционного болтового соединения представляет собой стыки двух листов, перекрытых парными накладками с болтами из стали 40Х, представлен на рис.3. При испытаниях образец будет нагружаться контролируемой статической нагрузкой.

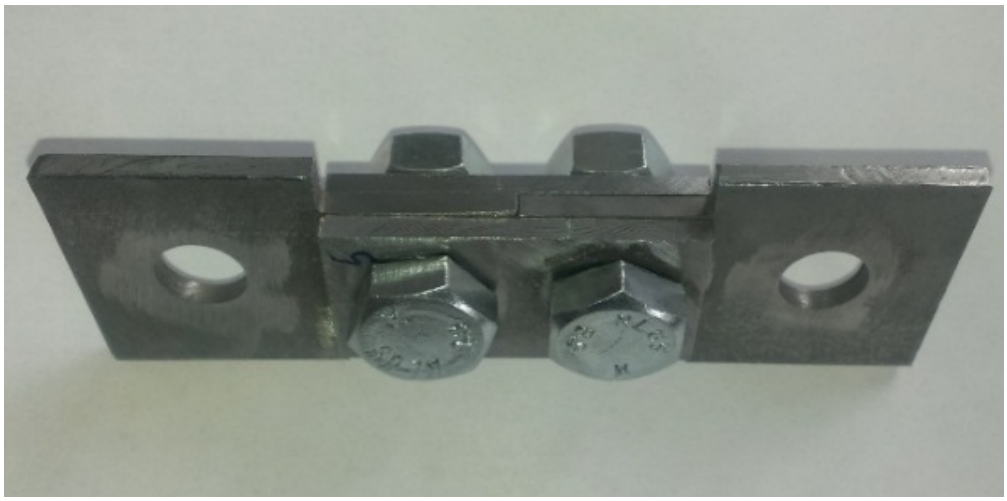


Рис.3. Испытываемый образец

Для получения корректных результатов при сборке образцов должен обеспечиваться максимальный односторонний зазор между элементами соединения в направлении испытательной нагрузки.

Полная деформация, возникающая при испытании, складывается из сопутствующей деформации (включающей в себя деформацию элементов стенда, узлов сопряжения образца и стенда) и собственно деформаций болтового соединения. Величина сопутствующих деформаций учитывается по результатам испытаний тарировочных образцов (рис.4), которые для каждого

из испытуемых болтовых соединений выполнялись из монолитного материала с характерными конструктивными элементами.

Рис.4. Тарировочный образец

Тарировочные и экспериментальные образцы будут подвергаться растяжению на разрывной машине МИ40КУ. При этом затяжка болтов экспериментальных образцов будет во всех случаях одинакова.

Результатом исследования будет являться анализ диаграмм растяжения с различным сочетанием факторов эксперимента. По диаграмме растяжения и по образцам до и после испытания определяется вариант соединения с наиболее лучшими характеристиками.

Список литературы

[1]. *Механика* контактных взаимодействий: учебное пособие / под редакцией И.И. Воровича, В.М. Александрова. – Москва: ФИЗМАТЛИТ, 2003. — 672 с. — ISBN 978-5-9221-0353-9. – Текст: электронный // Электронно-библиотечная система «Лань»: [сайт]. – URL: https://e.lanbook.com/book/59323 (дата обращения: 25.10.2019).

[2]. *Осипов В.О.* Долговечность металлических пролетных строений эксплуатируемых железнодорожных мостов. – М. Танспорт, 1982, 287 с.

[3]. *Сидняев Н.И.* Введение в теорию планирования эксперимента : учебное пособие / Н.И. Сидняев, Н.Т. Вилисова. – Москва : МГТУ им. Баумана, 2011. – 463 с. – ISBN 978-5-7038-3365-0. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/106359 (дата обращения: 25.10.2019).

Кириллов Игорь Николаевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: igor.kirillov40@yandex.ru

Заярный Сергей Леонидович - доцент кафедры «Подъемно-транспортные системы», канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: texnakon@yandex.ru

Д.Д. Козлов, С.Л. Заярный

ИССЛЕДОВАНИЕ КОНТАКТНЫХ ВЗАИМОДЕЙСТВИЙ В СОЕДИНЕНИЯХ ЭЛЕМЕНТОВ ПРИВОДОВ ПТМ И ДМ

Приводы подъемно-транспортных машин состоят из множества различных узлов и деталей, соединенных между собой различными способами. В процессе работы машины происходит изменение характера контактных взаимодействий, вследствие износа сопряжений, что в сочетании с большим количеством деталей приводов значительно влияет на эксплуатационные параметры машин. Следовательно, комплексное определение параметров контактных взаимодействий сопряжений при работе механизмов является важной задачей.

Достоверным методом решения поставленной задачи является экспериментальное определение хаотически изменяющихся силовых воздействий в канате, определяющих процессы износа соединений. вызванных проскальзыванием каната относительно шкива, деформациями в сопряжениях. Установка (рис.1) содержит различные соединения деталей машин, а также канатную систему, выполненную из частей каната и тензометрических устройств [2].

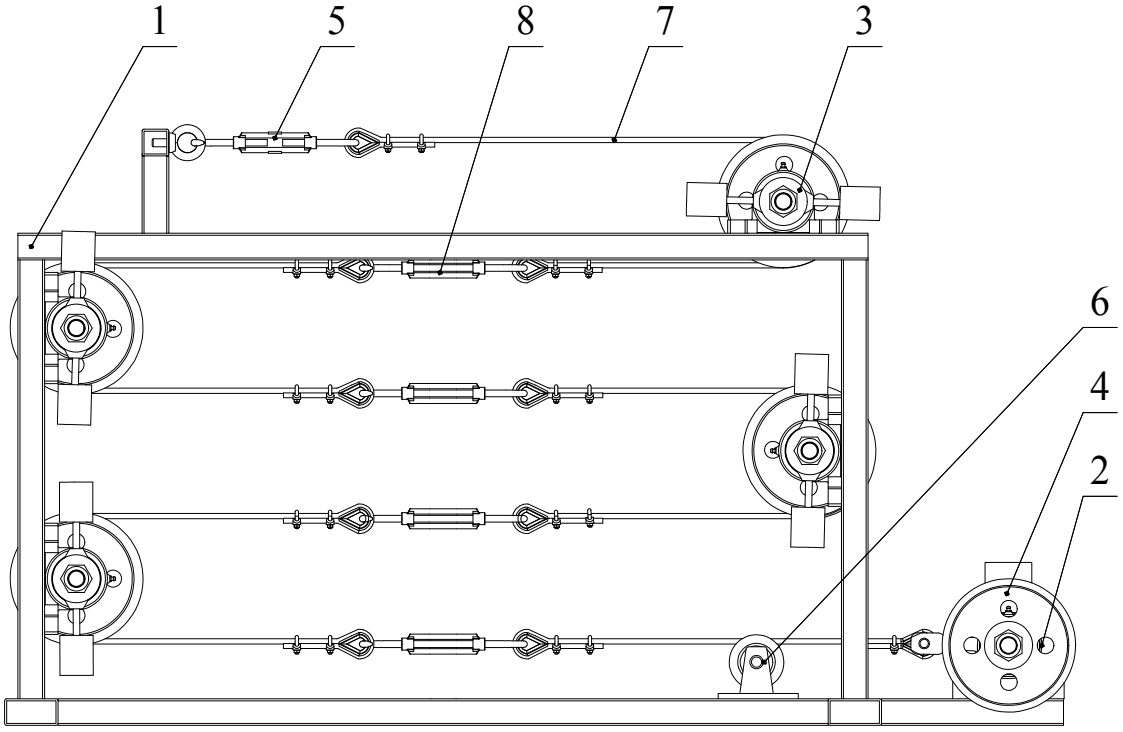


Рис.1. Установка для испытания на изнашивание соединений деталей машин: *1* – рама; *2* – эксцентриковое приводное устройство; *3* – функциональный блок; *4* – тяговый привод; *5* – натяжной узел; *6* - успокоитель; *7* – элемент тягового привода; *8* – тензометрические устройства

Функционально стенд можно представить в виде линеаризованной схемы (рис.2). Канаты заменены гибкими элементами c_{ij}, торсионные валы эле-

ментами c, момент инерции маховиков представлен в виде линейно перемещающейся массы m_j.

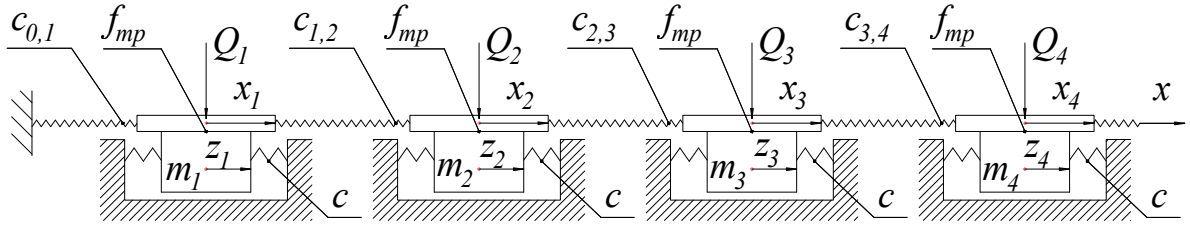


Рис.2. Структурная схема стенда

Силовая цепь стенда представляет собой динамическую систему с кинематическим возбуждением, состоящую из n элементов массой $m_i\left(i \in 1...n\right)$, упругих связей $c_{ij}\left(i, j \in 1...n\right)$ и фрикционных взаимодействий $\tilde{F}_i$ (диссипативным влиянием которых пренебрегаем). В общем случае, математическая модель такой силовой цепи определяется системой уравнений:

$$\begin{aligned}&\left(m_i\ddot{x}_i - 2cz_i\right)\delta\left(\dot{z}_i - \dot{x}_i\right) - c_{i-1,i}\left(x_{i-1} - x_i\right) - c_{i,i+1}\left(x_i - x_{i+1}\right) = \\ &= \tilde{F}_i sign\left(\dot{z}_i - \dot{x}_i\right),\end{aligned} \qquad (1)$$

где $\tilde{F}_i = Q_i f_{imp}$ – сила квазистохастического возбуждения, определяемая случайным характером усилия прижатия каната Q_i и коэффициента трения f_{mp}.

Наличие в уравнении фактора $\tilde{F}_i$ провоцирует квазистохастический характер колебательных процессов в силовой цепи конструкции стенда [2].

Наиболее эффективным режимом испытаний образцов является режимы, при которых функциональные блоки будут находится в состоянии близком к резонансному. Такой режим нагружения является более информативным для анализа контактных взаимодействий сопрягающихся элементов, т.к. увеличивается уровень и скорость проявления дефектов.

Для осуществления заданных режимов испытаний необходимо применение автоматизированных систем научных исследований (АСНИ), одним из основных элементов которой является аналогово-цифровой преобразователь (АЦП). Такая система позволяет осуществить автоматизацию операций регистрации параметров и обработки результатов испытаний.

АЦП преобразует аналоговый сигнал датчиков в код, над котором программное обеспечение выполняет определенные действия. В системах сбора данных общего назначения скорость дискретизации и разрешающая способность обычно имеют средние значения.

Схема системы измерений показана на рис. (рис. 3). ОИ – объект измерения; ДАТ – первичные преобразователи, служащие для преобразования физических элементов в электрический сигнал; КОМ – коммутаторы для последовательного подсоединения датчиков к нормализаторам; НОРМ – нормализаторы предназначены для усиления или ослабления электрического сигнала; АЦП – преобразователь аналоговых сигналов в цифровой код [1].

Использование автоматизированных систем исследований позволяет: оптимально планировать испытания, измерять и регистрировать параметры, обрабатывать информацию в реальном времени; получать результаты для необходимой настройки процесса испытания.

В качестве измерительного устройства используется тензодатчик, относящийся к параметрическому типу, т.е. изменят свои физические свойства (сопротивление) при изменении величины тягового усилия.

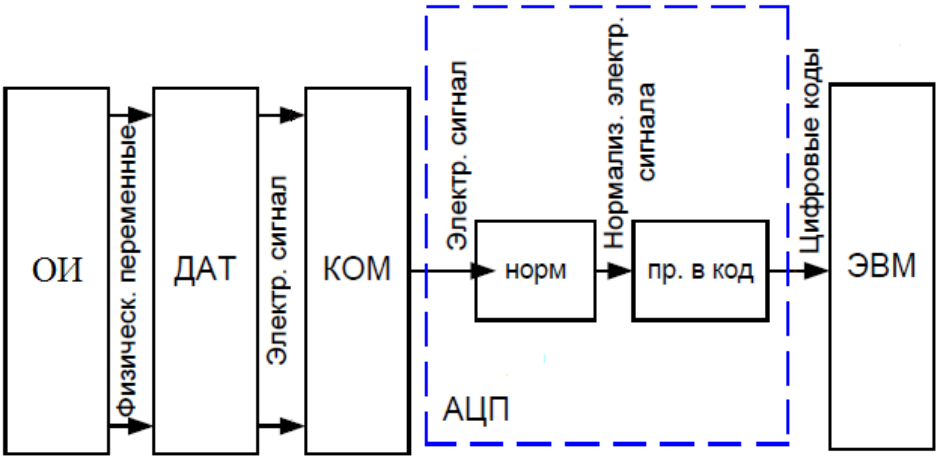


Рис. 3. Структурная схема системы измерений

Данная схема позволяет автоматизировать регистрацию параметров и обработки результатов испытаний.

В результате выполнения эксперимента будет получена зависимость сигнала датчика от периодически меняющейся случайной величины тягового усилия.

$$P = f(X_{изм}), \qquad (2)$$

где P – эквивалентный сигнал на выходе датчика; $X_{изм}$ – значение измеряемой величины.

Характеристики процесса испытаний будут определятся с помощью спектрального анализа над массивом выходных значений АЦП, соответствующих входному сигналу.

При анализе полученных спектров необходимо учитывать, что основной частоте входного сигнала соответствует нулевая гармоника, а остальным частотам – гармонические искажения, тепловой шум и т.д (рис. 4) [3].

Для интерпретации результатов измерений первостепенное значение имеет качество полученной экспериментальной информации. Поэтому необходимо осуществлять контроль измерений с целью выявления грубых ошибок и устранения их влияния. Таким образом будет проводится отбраковка выбросов цифрового кода, вызванных помехами, сбоями аппаратуры.

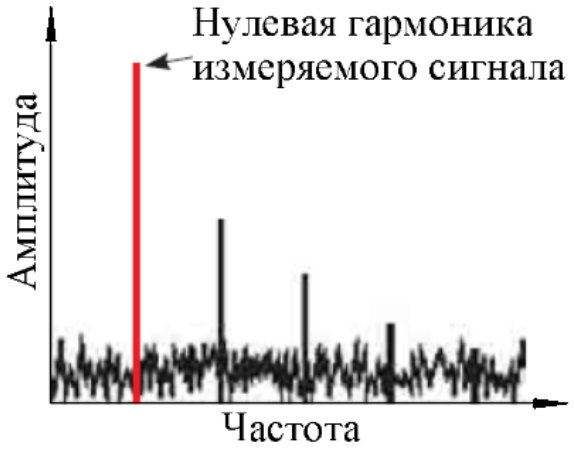


Рис. 4. Пример частотного спектра измеряемого сигнала

В дальнейшем при накоплении статистических данных, сопоставлении расчетных и измеренных результатов испытаний стенда за счет наименее достоверных параметров узлов, будет возможно непрерывно контролировать состояние соединения и прогнозировать их надежность.

Список литературы

[1]. *Фомичев Н.И.* Автоматизированные системы научных исследований. – учеб. пособие – Ярославль.: Яросл. гос. ун-т, 2001. – 112 с.

[2]. *Лесовский И.О., Заярный С.Л.* Моделирование хаотического процесса при стендовых испытаниях элементов привода // Инновационная наука. – 2016 – №6 (2). – с. 106–108.

[3]. *Райс В.* Как работают аналогово-цифровые преобразователи и что можно узнать из спецификации на АЦП? // Компоненты и технологии. – 2005 – №3. – с. 116–121.

Козлов Денис Дмитриевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: bookcasefor@yandex.ru

Заярный Сергей Леонидович - доцент кафедры, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: texnakon@yandex.ru

Д.И. Протасов, Д.Г. Мокин

ИССЛЕДОВАНИЕ ПРИЧИНЫ НЕРАВНОМЕРНОГО ИЗНОСА ЛОПАТОК ДРОБЕМЕТНОГО АППАРАТА

При работе дробеметного аппарата наблюдается интенсивный износ лопаток, который приводит к частой и трудоемкой операции - замене лопаток дробеметного аппарата. Еще более сокращается время между операциями замены лопаток при неравномерном износе лопаток. Износ одной лопатки приводит к замене всех лопаток, независимо от того, износились они или нет, поскольку нарушается балансировка ротора. Кроме того, возникшая неуравновешенность ротора является источником недопустимой вибрации.

Производить балансировку ротора в сборе трудно, и поэтому приходится производить замену всех лопаток независимо от степени их износа. Учитывая, что операция замены лопаток дробеметного аппарата является трудоемкой операцией, занимающей время от одного до четырех человеко-часов, видимо нецелесообразно вторично использовать частично изношенные лопатки. Таким образом, неравномерный износ лопаток в процессе работы приводит к сокращению срока их службы. Время непрерывной работы дробеметного аппарата до замены лопаток принимается за срок службы до первого отказа.

Отказ может наступить по двум причинам:

– в результате потери части массы одной из лопаток $m\varphi$, приводящей к ее поломке;

– по причине возникновения суммарной массы дисбаланса ротора, превышающего критическое значение mдис, приведенных к расстоянию от центра тяжести лопатки до оси вращения.

В результате сокращения времени до первого отказа приходится раньше установленного срока службы останавливать технологический цикл и производить замену всех лопаток ротора. Поскольку, как отмечалось, операция замены является самой частой и дорогостоящей операцией при техническом обслуживании дробеметных аппаратов, важно изучить причины неравномерного износа и найти пути устранения этих причин.

Известно, что износ лопатки пропорционален количеству дроби, прошедшей через нее. Обозначается Δmi - порция дроби, попавшая на i -ую лопатку за один оборот ротора. Если не учитывать диаметр дробинок и радиус захватывающей кромки импеллера, количество дроби, попавшее на лопатку пропорционально радиальной скорости Vi входа дроби в соответствующий i-ый паз импеллера.

$$\Delta m_i = V_i \times \rho \times s \times (2\pi / \omega). \qquad (1)$$

где ω – угловая частота вращения ротора; s – площадь окна импеллера; ρ – плотность потока дроби при прохождении через окно.

Количество дроби mi, прошедшее через паз за п оборотов:

$$m_i = \Delta m_i \times n. \qquad (2)$$

Количество оборотов ротора за время *dt* равно:

$$n = (\omega / 2\pi) dt \,. \qquad (3)$$

Подстановка в (2) и умножение его на коэффициент пропорциональности k позволяет получить износ *i* -ой лопатки за время *dt*:

$$dV_i = (B \times V_i) dt \,. \qquad (4)$$

$$B = k \times \rho \times s$$

Во время вращения ротора паз совершает колебательные движения с частотой вращения ротора в радиальном направлении в случае эксцентриситета А внутреннего отверстия импеллера. Эксцентриситет импеллера может возникнуть во время сборки, так называемый установочный эксцентриситет Ао (статический), а также может возникнуть в результате прецессионного движения оси ротора (динамический эксцентриситет) или динамической амплитуды колебаний ротора Ад. В обоих случаях относительная скорость движения дроби в паз импеллера определяется из выражения:

$$V_i = V_{cp} - A \times \omega \times \cos \alpha_i \,. \qquad (5)$$

где αi – угол между направлением эксцентриситета А и расстоянием OOi (рис. 1).

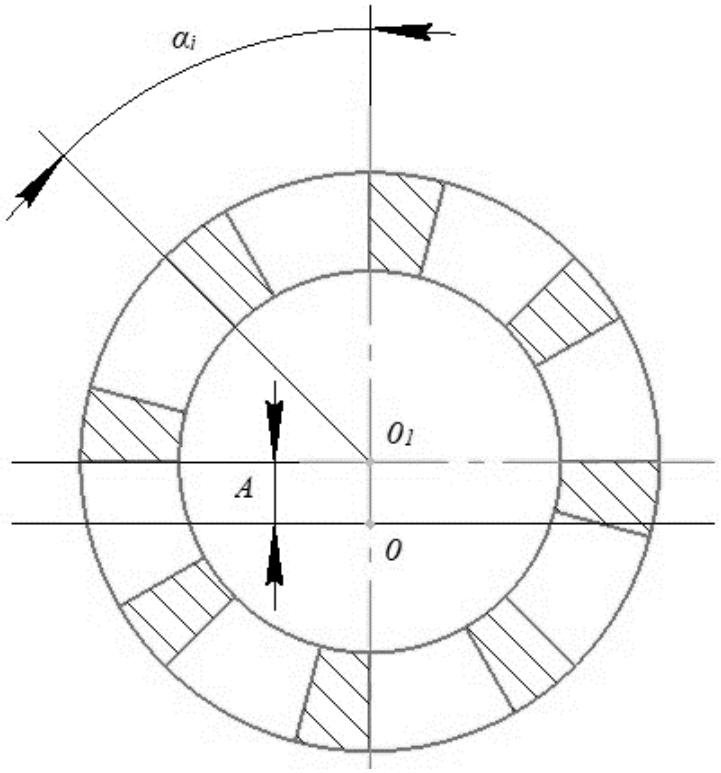


Рис.1 Схема импеллера

Подставляя (5) в выражение (4) и интегрируя обе части можно получить износ U i -ой лопатки (кг) за время t:

$$U_i = B \times t \times (V_{cp} + A \times \omega \times \cos \alpha_i) \,. \qquad (6)$$

Из (6) видно, что быстрее изнашивается лопатка, паз импеллера которой расположен ближе к оси вращения, когда $\alpha = 180°$, в то время износ противо-

положной лопатки, расположенной напротив паза с углом расположения α = 0, является минимальным.

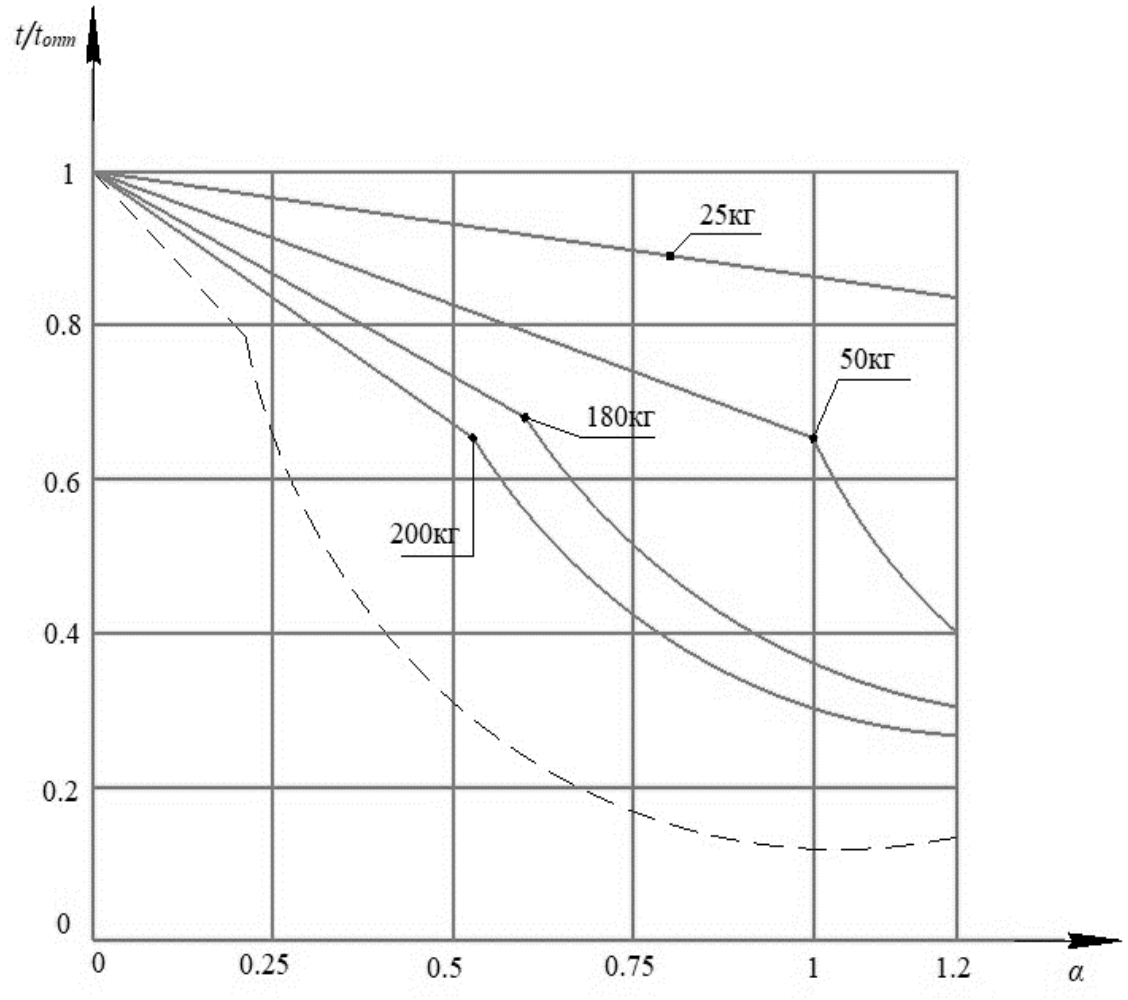


Рис.2

Зависимости относительного срока службы лопаток от значения коэффициента неравномерности износа

На графике (рис. 2) изображены зависимости срока службы до первого отказа от коэффициента неравномерности износа α для ротора с различной массой *m*, для рассмотренного случая установки ротора на упругой опоре, при следующих значениях конструкционных параметров:

t =0,16 м; ω = 250 рад; $Vср$=1, 7 м/с; $Dкр$= 0,6 кг; U = 0,5 кг.

Нижняя пунктирная кривая соответствует установке ротора абсолютно жестко. Верхние кривые последовательно соответствуют массе ротора 200, 180, 50, 25 кг.

Список литературы

[1]. *Кукуй Д.М.* Теория и технология литейного производства. — Минск : Новое знание, 2011. — 406 с.

[2]. *Горохов В.А.* Материалы и их технологии. — Минск : Новое знание, 2014. — 589 с.

Протасов Дмитрий Игоревич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия, volkswagen group rus. E-mail: notniceee95@gmail.com

Мокин Дмитрий Геннадьевич – канд. техн. наук, доцент кафедры «Детали машин и подъемно-транспортное оборудование» КФ МГТУ им. Н.Э. Баумана. E-mail: ded762@bmail.ru.

М.Е. Дьяченко, А.А. Шубин

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОБИЛЬНОГО КОМПЛЕКСА МОДУЛЬНОГО ТИПА ДЛЯ ОЧИСТКИ РЕК И ВОДОЕМОВ

На сегодняшний день наиболее остро стоит проблема загрязнения природной среды, в частности, одного из важнейших природных ресурсов Калужской области - водных объектов.

Мало кто догадывается, что очищая озеро от растительности, водорослей, торфа и сапропеля (сплавины), человек выбрасывает высокоэффективное органо-минеральное удобрение так необходимое сельскому хозяйству.

Исследование данной темы привело к разным технологическим решениям и использованию оборудования для очистки заросших водоемов и природных озер от растительности и торфо-сапропелевых отложений с их подготовкой и переработкой в пастообразные или сыпучие удобрения.

Существует несколько способов по очистке водоемов:

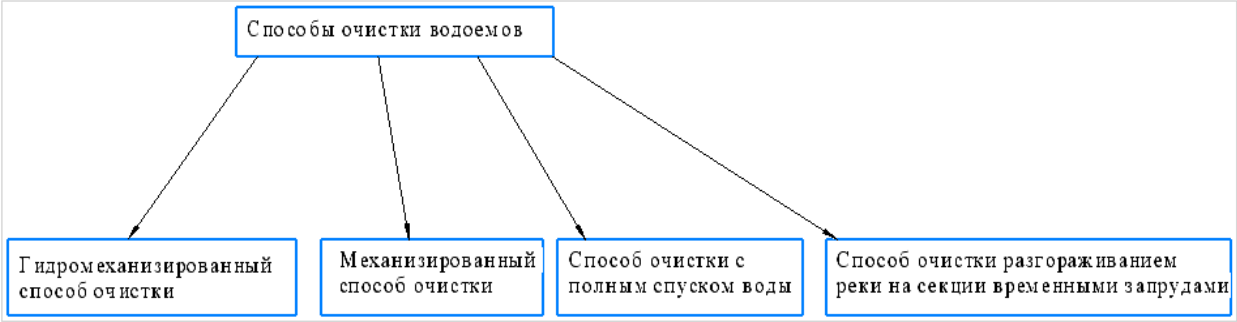


Рис. 1. Структурная схема различных способов по очистки водоемов

Более популярным является гидромеханизированный и механизированный способы очистки водоемов. Одним из изобретений является устройство для очистки водоема и добычи сапропеля содержащее заборный рабочий орган, расположенный в кожухе, со средством перемещения заборного рабочего органа и со средством отвода продукта очистки и привод. [2]

Скопление мусора на дне рек, каналов и вдоль берегов осложняет выполнение дноуглубительных работ. Остатки металла, куски древесины, кирпичи, пластиковые пакеты, покрышки и другой мусор, который находится в воде, забивает входное отверстие и машину приходится периодически останавливать.

Разработка комплекса модульного типа обуславливается необходимостью применения машин по очистки водоемов в различных условиях. Существует несколько аналогов данного комплекса, но из-за отсутствия универсальности, невозможно достичь повышения показателей в данной сфере.

За основу был взят земснаряд Watermaster - многофункциональная машина, являющаяся комбинацией землечерпательной машины с обратным ковшом и землесосом. Для выемки грунта используется прочный гидравлический экскаватор. Основное оснащение для углубления дна способом всасыва-

ния - режущий землесос, самостоятельное движение которого вдоль дна не требует помощи канатов и лебедок. [1]

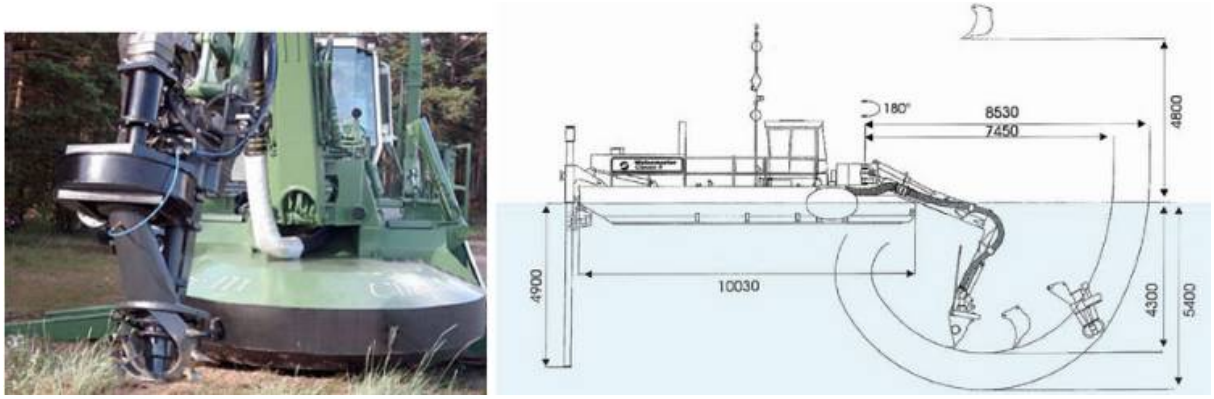


Рис. 2. Земсанряд Watermaster

Также при очистке водоемов от донных отложений, их можно использовать для нужд сельскохозяйственной промышленности. Сапропель в виде сгущенного осадка подается на сепаратор или др. устройство глубокого обезвоживания сапропеля влажностью до 55-75% с последующей грануляцией и сушкой получаемого сырья.

Также внедрение новых технологических процессов по очистке водоемов, с использованием новых устройств позволяет нам разработать мероприятия для выбора установки с целью повышения эффективности и экономичности очистки заиленных прудов.

Исходя из этого мы можем решить задачу по защите водных ресурсов от истощения и загрязнения, и рационального использования сапропеля для нужд народного хозяйства, что является одной из наиболее важных проблем, требующих безотлагательного решения.

Список литературы

[1]. *Комплекс* Watermaster [Электронный ресурс]. – Электрон. дан. – Режим доступа: (https:// watermaster.fi/ concept# superiormobility)

[2]. *Общее* устройство, техническая характеристика комплексов по очистке водоемов [Электронный ресурс]. – Электрон. дан. –Режим доступа: (https://studbooks.net/2462924/ tehnika/naznachenie)

[3]. *Наука* и жизнь [Электронный ресурс]. – Электрон. дан. – Режим доступа: (https://interesnosti.com/14448602427875677 13/ tehnologiya-kruglogodichnoj-dobychi-ozernogo-sapropelya-cherez-skvazhiny/)

Дьяченко Максим Евгеньевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: m.d1ch@yandex.ru

Шубин Александр Анатольевич - доцент кафедры «Подъемно-транспортные системы», канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: shubin55@mail.ru

А.Д. Маханьков, П.В. Витчук

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ УРОВНЯ БЕЗОПАСНОСТИ КОМПОНЕНТОВ И ОРГАНИЗАЦИИ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ЛИФТОВ

Лифт является безальтернативным средством вертикального перемещения людей в зданиях и сооружениях. В этой связи вопросы обеспечения надежности и безопасности эксплуатации лифтов имеют первостепенное значение. Из опыта эксплуатации лифтов известно, на надежность и безопасность их эксплуатации влияют: уровень организации труда и производства; система контроля качества и надежности; качество комплектующих изделий; качество используемого материала; квалификация рабочего персонала; техническое состояние и совершенство используемого оборудования; соблюдение технических требований на изготовление.

Представим процесс технического обслуживания лифтов в виде системы массового обслуживания, которая представляет собой совокупность двух потоков – случайных отказов и случайных ремонтов (рис. 1). Перевод системы слева направо осуществляется интенсивностью отказов λ, а справа налево интенсивностью обслуживания μ.

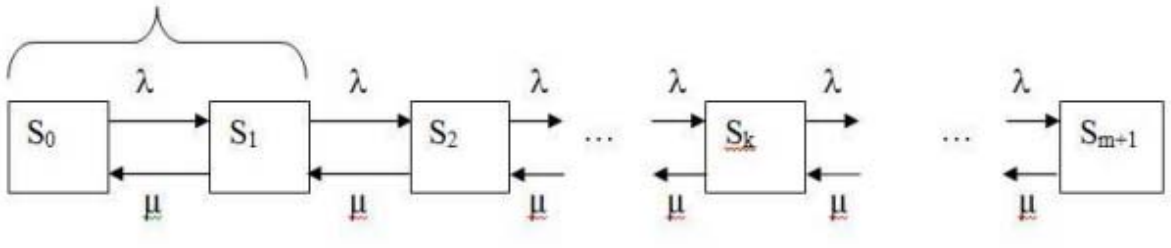


Рис. 1. Граф состояний системы массового обслуживания:
S_0 – канал свободен; S_1 – канал занят, очереди нет; S_2 – канал занят, одна заявка стоит в очереди; S_k – канал занят, *k*-1 заявок в очереди; S_{m+1} – канал занят, *m* заявок стоят в очереди.

Построение и анализ системы (рис. 1) для лифтов позволит определить оптимальное количество лифтов *z*, которые может обслужить один электромеханик. В качестве критерия оптимизации будем использовать значение уровня безопасности лифтов. В соответствии с [1] уровень безопасности для *z* лифтов может быть найден:

$$E_z = \frac{E_\Sigma \cdot K_{\Gamma z}}{K_{\Gamma_\Sigma}} \le \left[E_z \right], \qquad (1)$$

где E_Σ – уровень безопасности для полной совокупности лифтов, обслуживаемых организацией; $K_{\Gamma z}$ – коэффициент готовности для *z* лифтов; K_{Γ_Σ} –

коэффициент готовности для полной совокупности лифтов, обслуживаемых организацией.

Пусть m – количество элементов лифта j от 1…m, а n – количество лифтов i от 1…n. В свою очередь уровень безопасности для полной совокупности лифтов, обслуживаемых организацией:

$$E_{\Sigma} = \prod_{i=1}^{n} \left(1 - R_i\right), \tag{2}$$

где R_i – риск-опасность *i*-го лифта.

Риск-опасность может быть определена:

$$R_n = \prod_{i=1}^{n} R_i = \prod_{i=1}^{n} b_i \cdot r_i, \tag{3}$$

где R_i – риск-опасность *i*-го лифта r_i – ранг ремонтных затрат *i*-го лифта; b_i – вклад *i*-го лифта в риск-опасность.

$$r_i = \prod_{i=1}^{m} r_j, \tag{4}$$

$$R_n = \prod_{j=1}^{m} \overline{R}_j, \tag{5}$$

$$\overline{R}_j = b_j \cdot \overline{r_j}, \tag{6}$$

$$\overline{r_j} = \frac{\sum_{i=1}^{n} r_{ij}}{n}, \tag{7}$$

где r_j – ранг ремонтных затрат *j*-го элемента, $\overline{R}_j$ - средняя риск-опасность *j*-го элемента, $\overline{r_j}$ - средний ранг ремонтных затрат *j*-го элемента.

Исходя из того, что лифт ремонтируется одним электромехаником и стоимость одного часа одинакова при ремонте всех элементов лифта, то ранг ремонтных затрат *j* -го элемента *i*-го лифта можно определить:

$$r_{ij} = \frac{T_{ожij} + T_{p_i j}}{\sum_{ij}^{n} \left(T_{ож} + T_p\right)}, \tag{8}$$

где $T_{ожij}$ – время ожидания исправления неисправности *j* -го элемента *i*-го лифта; $T_{p_{ij}}$ – время ремонта *j* -го элемента *i*-го лифта; $T_{ож}$ – общее время ожидания; T_p – общее время ремонта.

Уравнение наработки на отказ *i*-го лифта имеет вид:

$$T_{o_i} = \frac{N_i \cdot \Delta t}{m_i(\Delta t)}, \tag{9}$$

где $m_i(\Delta t)$ - число отказавших элементов *i*-го лифта в интервале времени от $t - \frac{\Delta t}{2}$ до $t + \frac{\Delta t}{2}$,

N_i - количество элементов *i*-го лифта, вышедших из строя.

Средняя наработка на отказ по всем лифтам:

$$\overline{T}_o = \frac{\sum_{i=1}^{n} T_{o_i}}{n}, \tag{10}$$

Определим коэффициент готовности при обслуживании различного количества лифтов на основе собранных данных об отказах:

$$K_{\Gamma z} = \frac{\overline{T}_o}{\overline{T}_o + T_{ож} + T_p}. \tag{11}$$

Чтобы максимально точно дать информацию о надежности каждого элемента лифта, нами был разработан бланк таблицы данных об отказах, в которой будут записываться собранные данные (рис. 2).

Данные об отказах

Паспорт отказов №_____				№ лифта	Адрес	Год изготовления	Технические характеристики

№ п/п	Дата	Время, ч	Наработка, ч	Содержание отказа	Обстоятельства возникновения отказа	Время восстановления, мин
1	2	3	4	5	6	7
1. 2. 3. …						

_____ (дата) _____ (должность, подпись) _____ (ФИО)

Рис. 2. Бланк таблицы данных об отказах.

В бланке фиксируются подробные сведения об отказах: дата, время, наработка, содержание отказов, обстоятельства возникновения и время восстановления. Эти сведения в последствии определяют:

- Условия эксплуатации изделия;
- Возможные причины возникновения неисправностей;
- Виды неисправностей;
- Условия, при которых возникают неисправности;
- Наработка изделия до появления неисправности;
- Продолжительность поиска и устранения неисправности;
- Типы и количество замененных элементов;
- Трудозатраты, необходимые для устранения неисправности[2].

Таким образом с помощью вышеописанных формул и составленного бланка таблицы данных об отказах, мы сможем в реальных условиях с высокой точностью рассчитать оптимальное количество лифтов на каждого механика для повышения надежности и качества обслуживания, а также дать более точную оценку надежности каждого элемента лифта.

Список литературы

[1]. *Мечиев Аюб Вахаевич*. Разработка путей обеспечения безопасной эксплуатации лифтов: диссертация ... кандидата Технических наук: 05.05.04 / Мечиев Аюб Вахаевич;[Место защиты: ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»], 2018.- 134 с.

[2]. *Ртищев А.Г.* Сбор, обработка и анализ информации о надежности Москва Издательство комитета стандартов, мер и измерительных приборов при совете министров СССР 1970г. 57 с.

Маханьков Артем Дмитриевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: artyommah@yandex.ru

Витчук Павел Владимирович - доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: zzzventor@ya.ru

И.С. Голубев, А.В. Козина, Н.Е. Аверин

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАСЧЕТА ОПТИМАЛЬНЫХ ПАРАМЕТРОВ КАНАТНОГО ДВУХЧЕЛЮСТНОГО ГРЕЙФЕРА

Комплексная механизация и автоматизация погрузочно-разгрузочных, транспортных, складских и других работ является одной из актуальных проблем. Оснащение грузоподъемного оборудования специальными грузозахватными устройствами, а именно грейферными механизмами, способствует решению этой проблемы [1].

Наибольшее распространение получили канатные челюстные грейферы. Такие грейферы применяют для перемещения сыпучих грузов, таких как, уголь, кокс, песок, земля и др., внутри складских помещений, а также для загрузки груза в транспортирующие машины. Грейфер проектируют для конкретного насыпного груза. Поэтому расчет грейфера ведут с учетом характеристик груза: насыпной плотности γ, размера кусков a, податливости груза внедрению челюсти $q0$, коэффициента наполнения и уплотнения kV и группы груза. На основе этих характеристик определяют вместимость грейфера по объему V. При расчете геометрических размеров грейфера используют следующие эмпирические формулы (рис. 1) [2]:

$$\begin{aligned} L&=(2,2...2,6)\sqrt[3]{V_{30}} & l_2&=(0,15...0,25)L \\ \delta&=10...12^{o} & l_3&=(0,55...0,65)L \\ B&=(0,45...0,55)L & e_1&=(0,05...0,06)L \\ l_1&=0,4L & e_2&=(0...0,05)L \end{aligned} \qquad (1)$$

Расчетная масса зачерпываемого груза по ГОСТ составляет:

$$m_{\text{г}} = k_V \cdot \gamma \cdot L \cdot B \cdot h_0 \cdot \left(1-\frac{0,4L}{H_{\text{з}}}\right)\left(0,6+0,8\frac{B}{L}\right)\ln\frac{m_{\text{гр}}}{2 \cdot B \cdot q_0}. \qquad (2)$$

Как видно, значение $m_{\text{г}}$ зависит от эмпирических параметров и статичных параметров грузов, каждый геометрический параметр грейфера может иметь разброс от 20% до 50% в зависимости от выбранных значений коэффициентов. В результате этого габариты грейфера для одного и того же насыпного груза могут отличаться в 2-3 раза.

Для упрощения проектирования канатных грейферов и уменьшения вероятности ошибки при разработке было решено разработать программный продукт, вычисляющий оптимальные параметры канатного двухчелюстного грейфера в зависимости от параметров груза, интерфейс приложения представлен на рис. 2. Основными параметрами, которые требуется минимизиро-

вать при расчётах – это масса самого грейфера и длина тяги, т.к. для более меньшего грейфера требуется меньший кран, на котором он держится, а чем меньше длина тяги, тем он компактнее и меньше троса требуется вытянуть для размыкания челюстей.

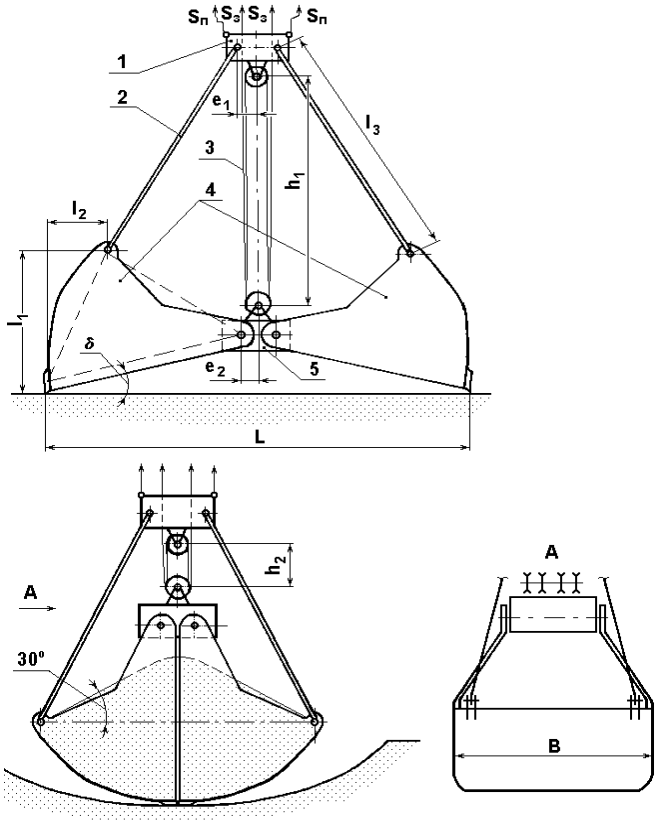


Рис.1. Схема грейфера:
1 – верхняя траверса; *2* – тяга; *3* – замыкающий полиспаст;
4 – челюсти; *5* – нижняя траверса

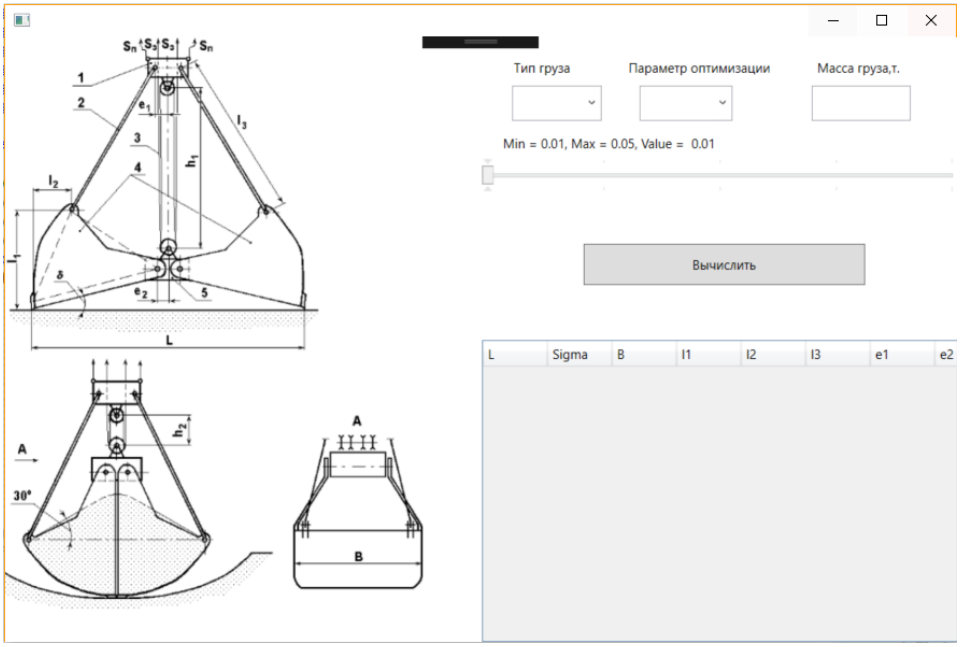


Рис.2. Интерфейс приложения

Приложение разрабатывалось таким образом, чтобы была возможность изменять тип груза, выбирать параметр оптимизации и задавать вес груза, который необходимо поднять рассчитываемым грейфером. Так же можно изменять шаг, с которым будут изменяться использующиеся в точных формулах подбираемые значения.

В приложении используется Excel-файл, в котором содержатся все параметры грузов. Данный формат выбран для того, чтобы инженер, работающий с данным приложением мог изменять параметры грузов, добавлять новые типы и т.д., не обладая знаниями в области программирования.

Для выполнения основной поставленной задачи – расчёта эмпирических формул был разработан основной расчётный алгоритм, заключающийся в последовательной переборке всех возможных значений параметров в точных формулах и дальнейшем расчёте и занесении в таблицу всех возможных результатов, из которых впоследствии, выбираются наиболее оптимальные.

На рис. 3 представлена диаграмма классов разработанного приложения.

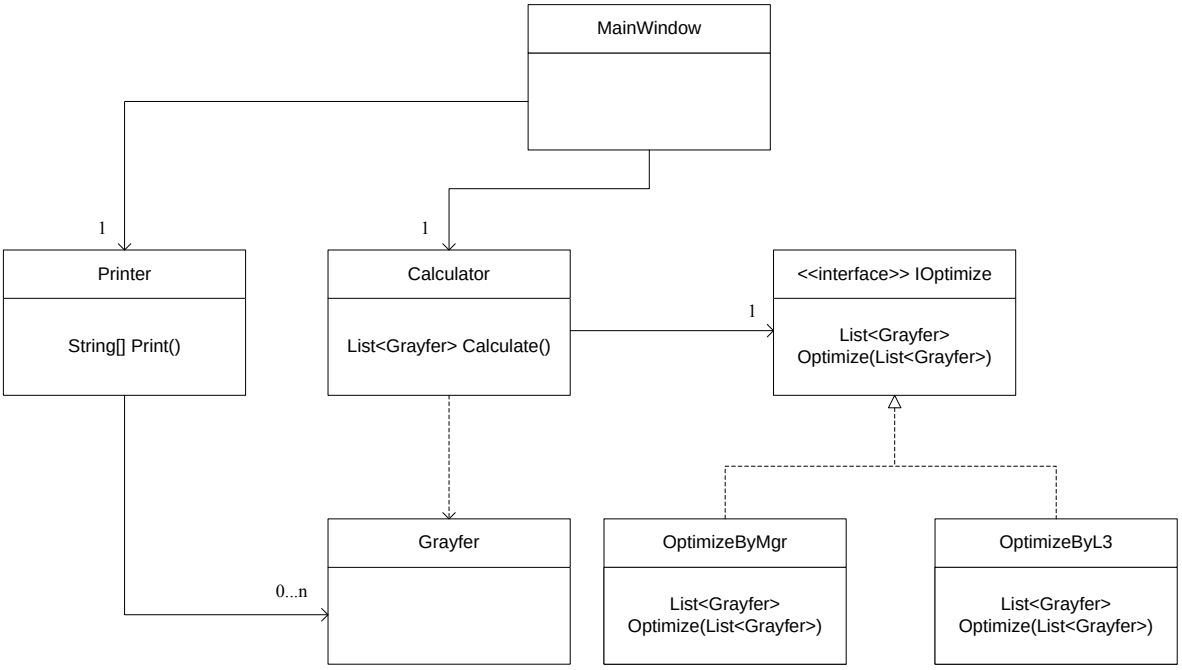


Рис. 3. Диаграмма классов приложения

Для выполнения основной задачи приложения был разработан класс «Calculator», в котором реализован основной расчётный алгоритм. Чтобы была возможна оптимизация по конкретным параметрам были добавлены классы «OptimizerByMgr» и «OptimizerByL3», реализующие интерфейс IOptimizer, имеющий метод Optimize. Данные классы реализуют оптимизацию по таким параметрам как масса самого грейфера и длина тяги соответственно. При такой структуре для добавления нового метода оптимизации достаточно создать новый класс, реализующий интерфейс IOptimize.

Разработанное приложение обладает гибкостью и удобством в эксплуатации. Внедрение данной системы на предприятия позволит увеличить про-

изводительность труда за счет уменьшения времени, затрачиваемого на выполнение расчётов.

Список литературы

[1]. *Вайсон А.А. Андреев А.Ф.* Крановые грузозахватные устройства: Справочник. - М.: Машиностроение, 1982. – 304 с.

[2]. *ГОСТ* 24599-87. Грейферы канатные для навалочных грузов.

[3]. *Панова Т.В., Николаева Н.Д.* Основы алгоритмизации и программирования на языке высокого уровня Си: учебно-практическое пособие. https://e.lanbook.com/book/75168#authors

[4]. *Рихтер Д.* CLR via C#. Программирование на платформе Microsoft.NET Framework 4.5 на языке C#. СПб: Питер, 2017.

Голубев Иван Сергеевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: Ptiz1999@yandex.ru

Козина Анастасия Валерьевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasiya-kozin@list.ru

Аверин Никита Евгеньевич - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: Averin.n.v@yandex.ru

Э.А. Голенкова, П.В. Витчук

РАЗРАБОТКА СТЕНДА ДЛЯ ИССЛЕДОВАНИЯ ТЯГОВОЙ СПОСОБНОСТИ ПРИВОДА ЛЕНТОЧНОГО КОНВЕЙЕРА

Ленточный конвейер – это транспортирующее устройство непрерывного действия, в которых лента является тяговым и грузонесущим органом. Передача тягового усилия и движения ленты осуществляются за счет сил трения от приводных барабанов. Обязательным условием действия этого привода без проскальзывания ленты является создание в ней предварительного натяжения.

Расчет фрикционного привода основан на решении, полученном Эйлером для неупругой гибкой нити. По общей теории фрикционного привода сцепление ленты с поверхностью барабана обеспечивается соотношением между натяжениями ветвей ленты, набегающей на приводной барабан S_2 и сбегающей S_1, определяется зависимостью [1, 2]:

$$S_2 \le S_1 e^{\mu\alpha}, \qquad (1)$$

где α – угол обхвата; μ – коэффициент трения ленты о барабан; e – основание натурального логарифма.

Из формулы (1) очевидно следуют способы увеличения тяговой способности привода конвейера: увеличение угла обхвата на основе применения отклоняющего ролика или многобарабанного привода; увеличение силы прижатия ленты к барабану на основе применения прижимного ролика или прижимной ленты увеличение коэффициента трения ленты о барабан на основе футеровки рабочей поверхности барабана фрикционными материалами.

В первом случае формула (1) примет вид:

$$S_2 \le S_1 e^{\mu\sum_{i=1}^{n}\alpha_i}, \qquad (2)$$

где α_i – угол обхвата, создаваемый i-м устройством; n – число устройств.

Во втором случае формула (1) примет вид:

$$S_2 \le \left(S_1 + N\mu\right)e^{\mu\alpha}, \qquad (3)$$

где N – усилие прижатия прижимного ролика или ленты.

Стоит отметить, что значения натяжений ветвей ленты в реальных конструкциях ленточных ковейеров несколько отличаются от расчетных в силу ряда причин. Поэтому для получения объективных данных предлагается разработать и изготовить лабораторную установку для исследования фрикционного привода ленточного конвейера (рис 1).

Лабораторная установка (рис. 1) для исследования параметров фрикционного привода состоит из сварной рамы, на которой установлен барабан. Концы ленты, огибающей барабана, через динамометры соединены с винтовыми натяжками. На оси барабана шарнирно закреплен рычаг, который закреплен на валу барабана без возможности проворачиваться. На нагружающем рычаге подвешивают грузы. У нижней ветви на подъемниках установ-

лен отклоняющий ролик. Прижимной ролик через динамометр с помощью винта может прижимать ленту к барабану.

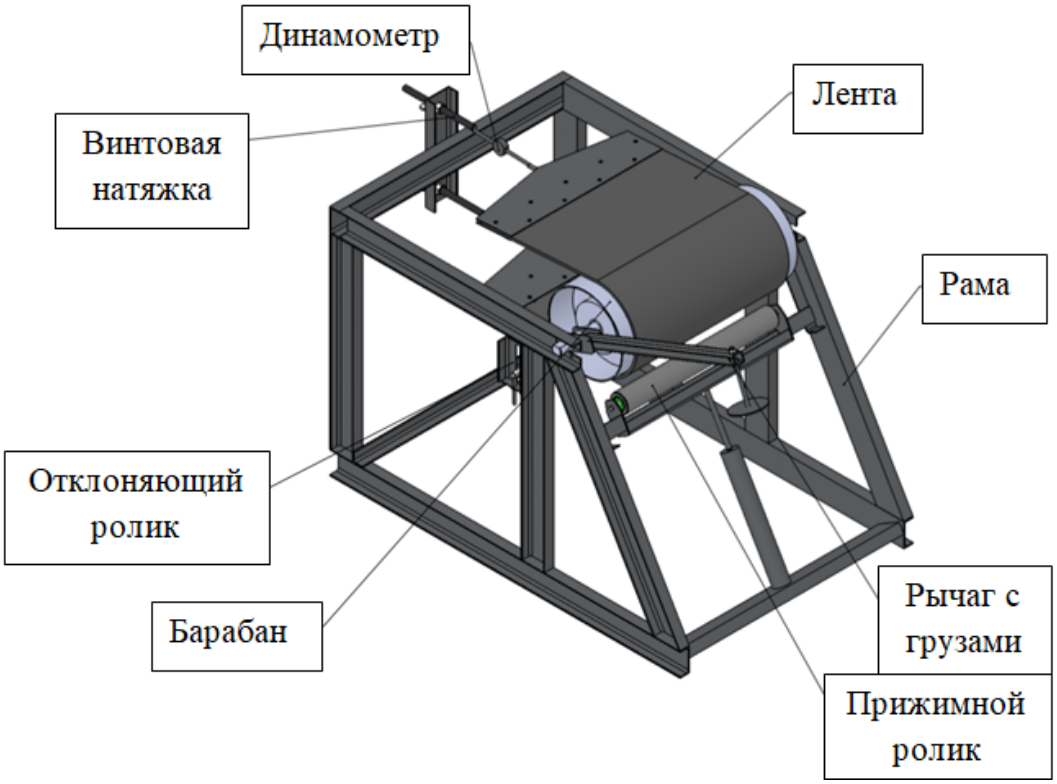


Рис. 1. Стенд для определения тяговой способности привода

Лабораторная установка работает следующим образом. Винтовые стяжки создают предварительное натяжение в сбегающей и набегающей ветвях ленты, значение которого контролируется динамометрами. На рычаг навешивают грузы. тяжкой нижней ветви ослабляют ее натяжение до момента страгивания барабана, после чего снимают показания динамометров. Эти показания будут равны фактическим значениям натяжений в сбегающей и набегающей ветвях ленты в соответствии с формулой (1).

Отклоняющий ролик позволяет прижимать ленту к тыльной поверхности барабана, увеличивая тем самым угол обхвата лентой барабана. Процесс измерения аналогичен предыдущему случаю, расчет соответствует формуле (2).

Прижимной ролик вводится в контакт с барабаном посредством винтовой пары, усилие прижатия контролируется динамометром. Процесс измерения аналогичен предыдущим случаям, расчет по формуле (3).

Список литературы

[1]. *Зенков Р.Л., Ивашков И.И., Колобов Л.Н.* Машины непрерывного транспорта. — М.: Машиностроение, 1987. — 432 с.

[2]. *Дьячков В.К.* Машины непрерывного транспорта — МАШГИЗ 1961г. — 352стр.

Голенкова Эльмира Арастуновна - студентка КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: egolienkova@mail.ru

Витчук Павел Владимирович - доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: zzzventor@ya.ru

Д.В. Трошкина, В.А. Ермоленко

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА РАЗГРУЗКИ ОТВАЛЬНОГО КОНВЕЙЕРА

Большая часть сети железных дорог России находится в зоне умеренного и холодного климата с выпадением осадков в виде снега, поэтому своевременная очистка путей от него имеет большое значение для нормального функционирования транспорта в холодное время года. Для уборки железнодорожных путей используется снегоуборочные поезда, в состав которых входит комплекс непрерывного действия для очистки от снежных заносов, транспортирования и выгрузке снега. В состав комплекса (рис. 1) входят головная машина *1*, промежуточный полувагон *2*, концевой полувагон с системой разгрузки *3*.

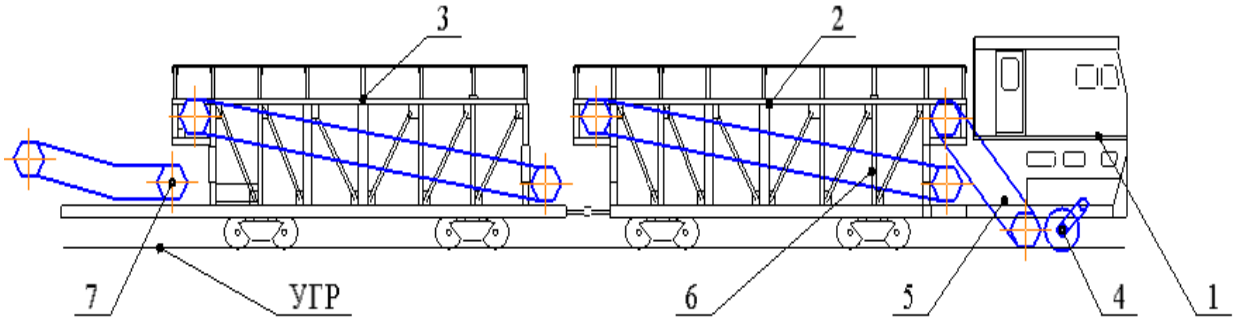


Рис. 1 Схема комплекса для уборки снега с железнодорожного пути:
1- головная машина, *2*- промежуточный полувагон, *3*-концевой вагон,
4- щеточный барабан-питатель, *5*- конвейер-питатель,
6-конвейер накопитель, *7*-отвальный конвейер.

Забор снега осуществляется щеточным барабаном питателем *4*, который подает снег на систему конвейеров, состоящих из конвейера-питателя *5*, конвейера-накопителя *6* и отвального конвейера *7*. С конвейера-питателя снег попадает в промежуточный вагон, предназначенный для накопления и хранения снега. В этом вагоне установлен конвейер-накопитель, скорость которого в разы меньше скорости конвейера-питателя. В конце вагона находится рыхлитель для измельчения крупных кусков наваленного снега. Разрыхленный снег попадает на отвальный конвейер (рис. 2, *а*), состоящий из горизонтальной *1* и наклонной *2* рам и механизма поворота *3*. Горизонтальная рама конвейера служит основанием, которым он крепится к ходовой раме машины *4*, и шарниром поворота. Механизм поворота обеспечивает разгрузку снега по обе стороны от оси пути.

Недостатком такой конструкции является фиксированная траектория движения убранного снега. При неоднократном прохождении поезда в отвалах будут образовываться большие наслоения снега, которые в дальнейшем могут оказывать осложнения на работу подвижных составов.

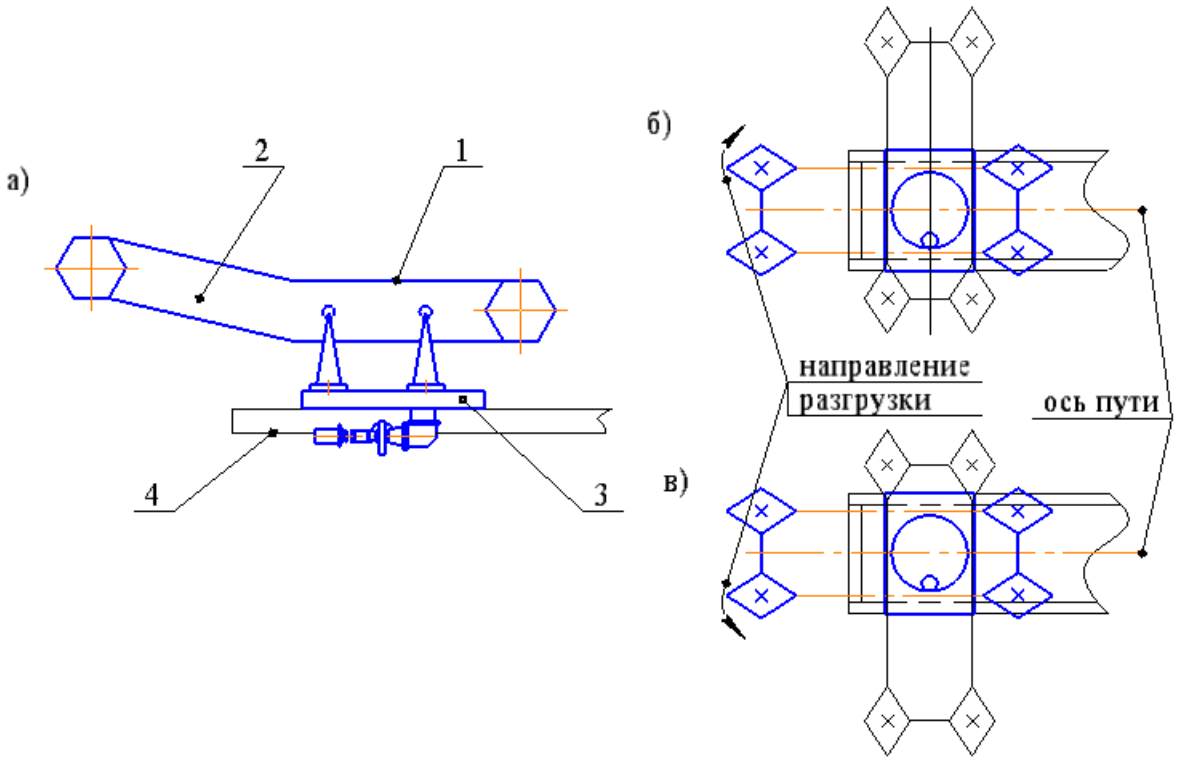


Рис. 2 Схема отвального конвейера:
а- схематичное изображение конвейера; *б*, *в* – способы разгрузки

Предлагаем установить в конце отвального конвейера щиток *2* (рис. 3) с возможностью изменения угла поворота разгрузочного листа относительно горизонта. Регулирование угла поворота будет обеспечиваться при помощи гидроцилиндра *1* и шарнирного крепления щитка *3*. Щиток будет иметь ограниченный диапазон угла поворота. Это условие является необходимым для того чтобы избежать заштыбовки груза на щитке. Внедрение в конструкцию отвального конвейера поворотного щитка позволит регулировать дальность полета струи снега, тем самым образуя несколько гребней неубранного снега.

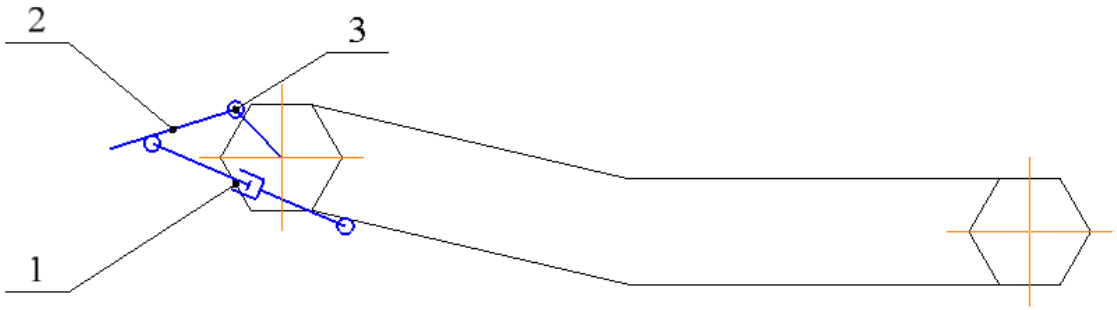


Рис. 3 Схема установки разгрузочного щитка на отвальном конвейере:
1 - гидроцилиндр, *2* - поворотный щиток, *3* - шарнирное крепление

При первом проходе щиток находится в транспортирующем положении, и разгрузка снега происходит под действием силы тяжести и центробежной силы (рис. 4). В данном случае частицы снега отрываясь от поверхности кон-

вейера движутся по параболе, очертания которой можно писать уравнениями координат:

$$x = \upsilon_i t$$
$$y = \frac{gt^2}{2} = \frac{gx^2}{2\upsilon_i^2} \qquad (1)$$

где υ - скорость движения частиц снега, м/с; $g = 9.81\ м/с^2$ - ускорение свободного падения; t - время движения частиц снега, с.

Для внутреннего очертания слоя снега на конвейере:

$$\upsilon_i = \upsilon . \qquad (2)$$

Для наружного очертания:

$$\upsilon_i = \frac{\upsilon\left(r + h_{гр}\right)}{r} , \qquad (3)$$

где r -радиус звездочки, м; $h_{гр}$ - толщина слоя снега на конвейере, м.

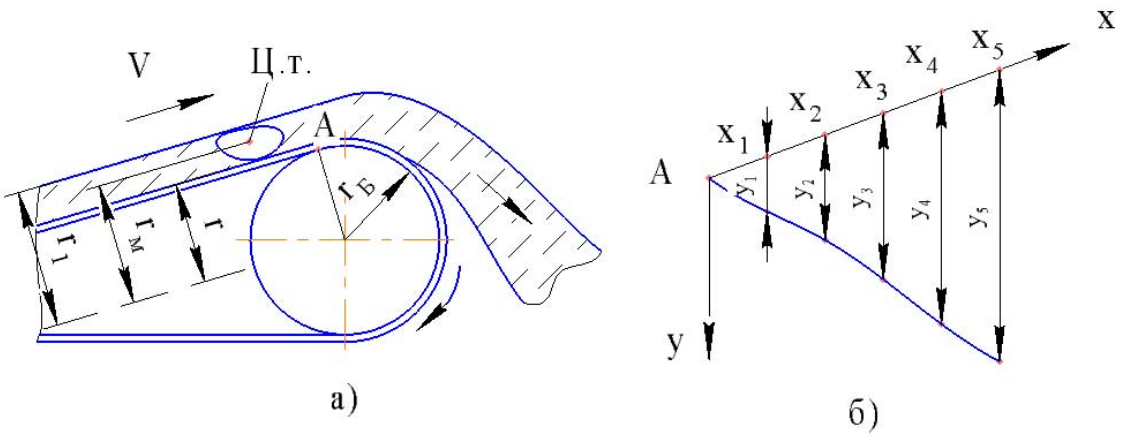


Рис.4 Схема для определения траектории полета частиц снега:
а - траектория полета, *б* - построение траектории полета

При последующих проходах снегоуборочной машины разгрузку производят при помощи поворотного щитка. В этом случае меняется траектория полета частиц. При расчете необходимо учитывать угол поворота щитка относительно горизонта. Значения координат примут вид:

$$x = \upsilon t \cos\theta$$
$$y = \upsilon t \sin\theta - \frac{gt^2}{2} \qquad (4)$$

θ - угол наклона щитка к горизонту, рад.

Дальность полета частицы - это значение координаты х в конце полета

$$L = \frac{\upsilon^2 \cdot \sin 2\theta}{g} + Htg\theta \qquad (5)$$

H - начальная высота выхода снега, м

Список литературы

[1]. *Теклин В.Г.* Путевые струги, снегоочистители, уборочные машины, М.: изд-во Транспорт, 1986г.

[2]. *Коротков В.Н., Завьялов А.А., Новиков Е.К.* Путевые машины и механизмы, Отраслевой каталог. Часть I. М. , 1982, 87 с.

[3]. *Попович М.В.* Путевые машины. Полный курс [Электронный ресурс] : учебник / М.В. Попович, В.М. Бугаенко. — Электрон. дан. — М.: УМЦ ЖДТ, 2009. — 820 с. — Режим доступа: https://e.lanbook.com/book/4185. — Загл. с экрана.

[4]. *Соломонов С.А.* Путевые машины: учебное пособие / С.А. Соломонов, М.В. Попович, В.М. Бугаенко ; под ред. Соломонова С.А.. — Электрон. дан. — М.: УМЦ ЖДТ, 2000. — 756 с.

[5]. *Спиваковский А.О., Дьячков В.К.* Транспортирующие машины, М.: изд-во Машиностроение, 1983г.

Трошкина Дарья Валерьевна - студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: dasha.troshkinaa@yandex.ru

Ермоленко Владимир Алексеевич - доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: tvermolenko@rambler.ru

СОДЕРЖАНИЕ

СЕКЦИЯ 6.
ЭКОЛОГИЯ И БЕЗОПАСНОСТЬ.....3

1. *В.С. Карасев, М.С. Дятлова, Ю.М. Жукова*

   АНТРОПОГЕННОЕ ВОЗДЕЙСТВИЕ ПОЛИГОНОВ ЗАХОРОНЕНИЯ ТВЕРДЫХ КОММУНАЛЬНЫХ ОТХОДОВ НА ОКРУЖАЮЩУЮ СРЕДУ 4

2. *С.А. Зубова, О.А. Прокофьева, М.И. Морозенко*

   ИННОВАЦИОННЫЕ РЕШЕНИЯ ОЧИСТКИ АТМОСФЕРНОГО ВОЗДУХА ОТ ВЫБРОСОВ *ЗАГРЯЗНЯЮЩИХ* ВЕЩЕСТВ..... 7

3. *Я.М. Литвинова, В.В. Коренец, С.Н. Никулина*

   ОСНОВНЫЕ ИСТОЧНИКИ ЗАГРЯЗНЕНИЯ ПОВЕРХНОСТНЫХ ВОД 12

4. *Т.С. Моторова, Е.Э. Комарова, О.В. Яковлева*

   ВОЗМОЖНОСТИ РАЦИОНАЛЬНОГО ВОДОПОЛЬЗОВАНИЯ В РАЙОНАХ С НЕДОСТАТОЧНЫМ ВОДООБЕСПЕЧЕНИЕМ 15

5. *К.В. Бочарова, М.Е. Сафронова, С.А. Кусачева*

   МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ ВОЗМОЖНОСТИ МИКРОБИОЛОГИЧЕСКОЙ УТИЛИЗАЦИИ БИОПОЛИМЕРОВ И НЕФТЕПРОДУКТОВ 19

СЕКЦИЯ 7.
СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАЗЕМНЫХ ТРАНСПОРТНО – ТЕХНОЛОГИЧЕСКИХ СИСТЕМАХ И КОМПЛЕКСАХ. ПРИКЛАДНЫЕ ПРОБЛЕМЫ МЕХАНИКИ 22

1. *Зар Ни Лин, К.В. Чижевский, В.Н. Сидоров, В.М. Алакин*

   АНАЛИЗ МЕЖДУНАРОДНЫХ ЕЗДОВЫХ ЦИКЛОВ АВТОМОБИЛЯ 23

2. *М.А. Карпов, Н.Г. Сысенко, А.Г. Черенков, С.А. Голубина*

   АНАЛИЗ СОВРЕМЕННЫХ ПОДВЕСОК АВТОМОБИЛЕЙ 29

3. *И.А. Зенкина, Д.А. Мамышев*

   ВЫЧИСЛЕНИЕ УРАВНЕНИЯ ТРАЕКТОРИИ ДВИЖЕНИЯ ЗЕМЛИ..... 33

4. *В.Н. Винокуров*

   КРАЕВАЯ ЗАДАЧА ДЛЯ ПОДПЯТНИКА С ГАЗОВОЙ СМАЗКОЙ 35

5. *Тинт Наинг Вин, В.М. Алакин*

   ОБОСНОВАНИЕ ЧАСТНОЙ МЕТОДИКИ ОПРЕДЕЛЕНИЯ ЦЕНТРА ТЯЖЕСТИ АВТОМОБИЛЯ 37

6. *С.С.Остроумов*

   СОВЕРШЕНСТВОВАНИЕ КАРТОФЕЛЕУБОРОЧНЫХ МАШИН В НАПРАВЛЕНИИ СНИЖЕНИЯ ПОВРЕЖДАЕМОСТИ КЛУБНЕЙ КАРТОФЕЛЯ 40

7. М.А. Карпов, В.Н. Сидоров

СПОСОБЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПРИ ТОРМОЖЕНИИ АВТОМОБИЛЯ 44

СЕКЦИЯ 8.
ЗАЩИТА ИНФОРМАЦИИ 48

1 .А.И. Самохина

АНАЛИЗ ВИДОВ *ЭЛЕКТРОННОЙ* ПОДПИСИ ДОКУМЕНТОВ 49

2. А.Г. Гуденко

АНАЛИЗ МЕТОДОВ ЗАПУТЫВАНИЯ КОДОВ 53

3. А.Н. Огарева, А.Б. Лачихина

АНАЛИЗ СРЕДСТВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕЧАТИ БАНКОВСКИХ ДОКУМЕНТОВ 56

4. П.А. Селиванов, Ю.С. Белов

ВВЕДЕНИЕ В ПРОМЕЖУТОЧНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ОРИЕНТИРОВАННОЕ НА СООБЩЕНИЯ (MOM) 60

5. Е.Ю. Шестопалов, А.В. Бурмистров, А.Б. Лачихина

ВИДЫ АТАК НА НЕЙРОННЫЕ СЕТИ 64

6. С.В. Степаненко

ВИДЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ 67

7. К.Н. Солдатов

ДИАГНОСТИКА ФУНКЦИОНИРОВАНИЯ ПРЕДПРИЯТИЯ ПО ОТКЛОНЕНИЯМ В ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ 70

8. П.Ю. Малахов

ЗАРУБЕЖНЫЙ ОПЫТ ФОРМИРОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 73

9. С.С. Щеголихин

ИССЛЕДОВАНИЕ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА 76

10. А.А. Шабанов

К ВОПРОСУ РАЗРАБОТКИ КРИТЕРИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ ПРИНИМАЕМЫХ В ФИЛИАЛАХ КРУПНЫХ КОМПАНИЙ НА ПРИМЕРЕ ПРЕДПРИЯТИЙ АВТОМОБИЛЕСТРОИТЕЛЬНОГО КЛАСТЕРА КАЛУЖСКОЙ ОБЛАСТИ 79

11. А.А. Чураков Е.А. Черепков

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ГРАЖДАН 83

12. С.Е. Липатова, Е.А. Черепков, Ю.С. Белов

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ДАННЫХ НА ОСНОВЕ ТЕХНОЛОГИИ BLOCKCHAIN 86

13. С.А. Медведева, П.В. Фролов, Мазин А.В., Е.В. Вершинин

ОБЗОР ИССЛЕДОВАНИЙ ПО АНАЛИЗУ СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ МЕТОДОВ 91

14. М.Д. Гущина

ОБЗОР МЕТОДОВ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА 95

15. Н.А. Зоринов

ОБЗОР МЕТОДОВ СНИФФИНГА СЕТЕВОГО ТРАФИКА..... 98

16. Я.И. Румякин

ОБЗОР ПОДХОДОВ И ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ РАСПРЕДЕЛЕННОГО УПРАВЛЕНИЯ ДОСТУПОМ МЕЖДУ ПРИЛОЖЕНИЯМИ..... 103

17. В.А. Бессонов

ОБЗОР СИСТЕМЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ ИЗМЕРЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОЙ НАСТРОЙКИ И ВМЕШАТЕЛЬСТВА 107

18. Ю.С. Носова

ОБЗОР УЯЗВИМОСТЕЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ..... 111

19. А.Р. Филатов, М.К. Савкин

ОБЩИЙ ПОДХОД К ТЕСТИРОВАНИЮ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕРВЕРНЫХ ПРИЛОЖЕНИЯХ 114

20. А.Б. Лачихина, А.А. Серегин

ОРГАНИЗАЦИЯ И ПОДХОДЫ МОНИТОРИНГА ФИЗИЧЕСКОГО ПОДКЛЮЧЕНИЯ СЕТИ 118

21. Р.В. Габдуллин, Е.А. Черепков, Ю.С. Белов

ОЦЕНКА ЭФФЕКТИВНОСТИ МНОГОМЕРНОГО ЛИНЕЙНОГО КРИПТОАНАЛИЗА 121

22. А.А. Гапутина

ПЕРЕХОД К СИСТЕМАМ БЕЗОПАСНОГО ОБМЕНА ФАЙЛАМИ НА ОСНОВЕ ТЕХНОЛОГИИ MFT 127

23. И.С. Скубаева

ПОДХОДЫ К МОНИТОРИНГУ ЗАПУЩЕННЫХ ПРОЦЕССОВ В ОС LINUX 130

24. И.Е. Рунов

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ЗАЩИТЫ БАЗ ДАННЫХ 133

25. Е.С. Еськов

ПРИМЕНЕНИЕ РЕВЕРС – ИНЖИНИРИНГА ДЛЯ РЕШЕНИЯ ЗАДАЧ ИБ 137

26. С.Г. Шитов

ПРОТОКОЛ ГЛОБАЛЬНОЙ МАРШРУТИЗАЦИИ BGP
И ЕГО УЯЗВИМОСТИ 142

27. А.А. Чураков, А.В. Козина

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ МИНИМИЗАЦИИ ЛОГИЧЕСКИХ
ВЫРАЖЕНИЙ МЕТОДОМ КВАЙНА-МАК-КЛАСКИ 147

28. Е.М. Бандурина, А.В. Ткаченко, Ю.С. Белов

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ
ВРЕДОНОСНОЙ ИНФОРМАЦИИ 150

29. И.Д. Феоктистов

СТРУКТУРА И ПРИНЦИП РАБОТЫ СИСТЕМ УПРАВЛЕНИЯ СОБЫТИЯМИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 154

30. А.Е. Юнеева, А.В. Козина, Ю.С. Белов

УЯЗВИМОСТИ В БЕЗОПАСТНОСТИ НЕЙРОННЫХ СЕТЕЙ 157

СЕКЦИЯ 9.
ДИНАМИКА, ПРОЧНОСТЬ И НАДЕЖНОСТЬ
ПОДЪЕМНО-ТРАНСПОРТНЫХ, СТРОИТЕЛЬНЫХ,
ДОРОЖНЫХ МАШИН И ОБОРУДОВАНИЯ 160

1. Н.Г. Сысенко, А.Г. Черенков, М.А. Карпов, В.А. Ермоленко

ВЗВЕШИВАНИЕ ГРУЗОВ ПРИ ЭКСПЛУАТАЦИИ СТРЕЛОВОГО КРАНА 161

2. Д.В. Зайцев

ЗАЩИТА ПОДШИПНИКОВ КАЧЕНИЯ И ЗУБЧАТЫХ КОЛЕС
НА ВИБРОПРЕССАХ С ПОВЫШЕННОЙ ЧАСТОТОЙ ВИБРАЦИИ 165

3. И.Н. Кириллов, С.Л. Заярный

ИССЛЕДОВАНИЕ КОНТАКТНЫХ ВЗАИМОДЕЙСТВИЙ В БОЛТОВЫХ
СОЕДИНЕНИЯХ ПЕРЕМЕННОЙ СТРУКТУРЫ
В ХОДЕ АКТИВНОГО ЭКСПЕРИМЕНТА 169

4. Д.Д. Козлов, С.Л. Заярный

ИССЛЕДОВАНИЕ КОНТАКТНЫХ ВЗАИМОДЕЙСТВИЙ
В СОЕДИНЕНИЯХ ЭЛЕМЕНТОВ ПРИВОДОВ ПТМ И ДМ 173

5. Д.И. Протасов, Д.Г. Мокин

ИССЛЕДОВАНИЕ ПРИЧИНЫ НЕРАВНОМЕРНОГО ИЗНОСА ЛОПАТОК
ДРОБЕМЕТНОГО АППАРАТА 177

6. М.Е. Дьяченко, А.А. Шубин

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОБИЛЬНОГО КОМПЛЕКСА
МОДУЛЬНОГО ТИПА ДЛЯ ОЧИСТКИ РЕК И ВОДОЕМОВ 181

7. А.Д. Маханьков, П.В. Витчук

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ УРОВНЯ БЕЗОПАСНОСТИ КОМПОНЕНТОВ И ОРГАНИЗАЦИИ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ЛИФТОВ 183

8. И.С. Голубев, А.В. Козина, Н.Е. Аверин

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАСЧЕТА ОПТИМАЛЬНЫХ ПАРАМЕТРОВ КАНАТНОГО ДВУХЧЕЛЮСТНОГО ГРЕЙФЕРА 187

9. Э.А. Голенкова, П.В. Витчук

РАЗРАБОТКА СТЕНДА ДЛЯ ИССЛЕДОВАНИЯ ТЯГОВОЙ СПОСОБНОСТИ ПРИВОДА ЛЕНТОЧНОГО КОНВЕЙЕРА 191

10. Д.В. Трошкина, В.А. Ермоленко

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА РАЗГРУЗКИ ОТВАЛЬНОГО КОНВЕЙЕРА 194

НАУКОЕМКИЕ ТЕХНОЛОГИИ
В ПРИБОРО- И МАШИНОСТРОЕНИИ
И РАЗВИТИЕ ИННОВАЦИОННОЙ
ДЕЯТЕЛЬНОСТИ В ВУЗЕ

Материалы
Всероссийской научно-технической конференции

Том 2

Научное издание

Все работы публикуются в авторской редакции. Авторы несут ответственность за подбор и точность приведенных фактов, цитат, статистических данных и прочих сведений

Подписано в печать 17.11.2019
Формат 60x90/16. Печать офсетная. Бумага офсетная. Гарнитура «Таймс»
Печ. л. 12,69. Усл. п. л. 11,8

Издательство МГТУ им. Н.Э. Баумана
107005, Москва, 2-я Бауманская, 5

Оригинал-макет подготовлен в Редакционно-издательской группе
отдела научной инновационной деятельности
КФ МГТУ им. Н.Э. Баумана
248000, г. Калуга, ул. Баженова, 2, тел. 57-31-87