МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ИНЖЕНЕРНЫЕ КАДРЫ – БУДУЩЕЕ ИННОВАЦИОННОЙ ЭКОНОМИКИ РОССИИ

Материалы VI Всероссийской
студенческой конференции

Йошкар-Ола, 10-13 ноября 2020 г.

Часть 4

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ОСНОВА СТРАТЕГИЧЕСКОГО ПРОРЫВА В СОВРЕМЕННОЙ ПРОМЫШЛЕННОСТИ

Йошкар-Ола
2020

УДК 378:62
ББК 74.48:30
И 62

И 62 **Инженерные кадры – будущее инновационной экономики России:** материалы VI Всероссийской студенческой конференции (Йошкар-Ола, 10-13 ноября 2020 г.): в 8 ч. *Часть 4: Информационные технологии – основа стратегического прорыва в современной промышленности.* – Йошкар-Ола: Поволжский государственный технологический университет, 2020. – 217 с.

ISBN 978-5-8158-2217-7
ISBN 978-5-8158-2221-4 (Ч. 4)

В рамках Всероссийской студенческой конференции представлены результаты научно-исследовательских работ студентов, магистрантов, аспирантов в области информационных технологий, компьютерных сетей, искусственного интеллекта, информационной безопасности, робототехники с перспективой их практического использования.

УДК 378:62
ББК 74.48:30

ISBN 978-5-8158-2221-4 (Ч. 4)
ISBN 978-5-8158-2217-7

ПРЕДИСЛОВИЕ

Современные методы и подходы в области информационных технологий на основе широкого использования последних достижений науки и техники предъявляют сегодня новые требования к уровню подготовки инженерных кадров. Будущие специалисты-профессионалы должны быстро воспринимать передовые знания и воплощать их в практической деятельности. Помогает выработать необходимые навыки сочетание учебно-образовательной и научно-исследовательской деятельности.

В настоящем издании представлены материалы секции «Информационные технологии – основа стратегического прорыва в современной промышленности» Всероссийской студенческой конференции «Инженерные кадры – будущее инновационной экономики России», которая проходила в рамках одноименного форума 10-13 ноября 2020 года в Поволжском государственном технологическом университете.

Все студенты, магистранты, аспиранты ПГТУ и других вузов из различных регионов РФ своим участием в данной конференции внесли большой вклад в свое будущее и в будущее инженерных кадров Российской Федерации.

Тематика секции связана с применением информационных технологий в современном производстве. Материалы конференции отражают результаты молодежных исследований в актуальных областях:

- информационные технологии;
- компьютерные технологии;
- информационная безопасность;
- искусственный интеллект;
- робототехника.

Статьи, предложенные для публикации, рассмотрены программным комитетом конференции. Лучшие из них включены в настоящий сборник. По результатам представленных сообщений многие из авторов отмечены дипломами соответствующей степени.

Оргкомитет и редакционная коллегия сборника выражают искреннюю благодарность участникам конференции, их руководителям и консультантам за высокий уровень докладов. Будем рады видеть Вас в следующем году с новыми актуальными и интересными исследованиями.

УДК 322

Абрамов Данил Юрьевич
направление Информационная Безопасность (специалитет), гр. БИ-51

Научный руководитель
Пекунов Андрей Ананьевич,
доцент кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологически университет», г. Йошкар-Ола

СОВРЕМЕННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данный момент одним из самых высоко конкурентных является финансовый сектор, главными учреждениями которого выступают банки. Их основными задачами оказываются: снижение операционных издержек, поддержание лояльности существующих и привлечение новых клиентов, поэтому на первое место встают такие информационные технологии, которые позволяют максимально снизить затраты на обслуживание клиентов. В связи с этим популярность набирают виртуальные банки, которые имеют значительные отличия от традиционных сетей банковских отделений.

Виртуальный банк — это финансовая организация, которая занимается проведением разнообразных банковских процессов дистанционно через Интернет. Такие банки предлагают абсолютно реальные банковские продукты и услуги на гораздо более выгодных условиях, чем конкуренты. Использование такого вида банков значительно сохраняет время, более того, клиенты имеют возможность оплачивать счета в любое время суток, а также появляется удобство вести контроль над всеми видами денежных операций по банковским картам. Основной выгодой виртуального банка является низкая стоимость финансовых транзакций. Поэтому даже те клиенты, кто оперирует небольшими денежными суммами, приносят прибыль организации. Главная особенность - взаимодействие с банком полностью строится на дистанционной основе, используются разнообразные многоканальные системы предоставления услуг.

Первым в истории виртуальных банков появился банк SecurityFirstNetworkBank в Америке в 1995 г. Сейчас во всем мире существует около шести тысячи сайтов, предоставляющие услуги виртуальных банков. В России посамыми известными виртуальными банками являются «Тинькофф кредитные системы» и «Рокетбанк». «Тинькофф банк» стал первым банком, который отказался от

отделений, чем заслужил большую популярность среди российских банков.

Но, как и любой другой информационной структуре, виртуальные банки обладают одним важным недостатком - возможность незаконного доступа к информации. Именно поэтому, помимо выполнения своей непосредственной деятельности, важной задачей виртуальных банков является обеспечение защиты информации. Основными организационными и техническими мерами становятся: защита данных от незаконного доступа, блокировки, копирования, распространения и модифицирования. Конфиденциальность данных — это положение, предоставленное данными и определяющее требуемую степень их защиты. К таким видам доверительных данных можно отнести личные данные пользователей, имена, пароли, информацию о кредитных картах, всевозможная внутренняя документация, протоколы, бухгалтерские материалы. Конфиденциальная информация должна быть известна исключительно авторизированным лицам, прошедшим проверку [1].

Информационные системы виртуальных банков состоят из рабочих мест операторов, оснащенные оборудованием, интегрирующим цифровые показания и звуковые сигналы (например, голоса), а также они имеют надежную защиту благодаря устройствам, которые регистрируют, запоминают голоса и контролируют доступ к системе.

Чтобы управлять своим счетом, клиенты используют мобильные устройства (ноутбук, планшет, смартфон), которые имеют подключение к Интернету. При этом любая информация, которая была передана клиентом в банк будет шифроваться при помощи специального безопасного SecureSocketsLayer (SSL) -соединения.

Помимо типовых процедур оформления документов, банк предоставляет клиентам всю необходимую информацию о порядках работы с данным видом банков. В эти порядки входит предоставление возможности самостоятельного выбора систем безопасности для защиты всех электронных счетов клиентов от незаконного взлома. Аутентификация и идентификация — это основа систем защиты информации. Использование карт с переменным одноразовым или многоразовым паролем является одним из методов аутентификации (запрос пароля будет происходить при каждом включении в систему)[2].

У множества виртуальных банков имеется стандартное звено, которое характерно для любого банка: DigitalLightProcessing (DLP) - система - антивирусная система доступа пользователей к базам данных, осуществляющая контроль пользователей, которым доступны

различные подключения. Кроме того, есть составляющее звено, определенное спецификацией работы банка. Такжеиспользуютсятакиепродукты, как McAfee, Juniper, Balabit, Good for Enterprise, HP Arcsite, Imperva ит. д.

Для контроля доступа к базам данных банки используют программно-аппаратный комплекс ImpervaDatabaseSecurity, который позволяет в клиентских системах таких, как CRM, выявлять странное поведение пользователей, проводить контроль обращений администраторов и обычных пользователей напрямую в базе данных, обеспечивает комплексную прозрачность использования данных, прав доступа и уязвимостей.

Следующее решение в осуществлении информационной безопасности - MDM (MobileDeviceManagement) - BYOD (BringYourOwnDevice), которое предусматривает контроль над мобильными пользователями.

BYOD — это подход к организации рабочего места сотрудника, при котором он применяет свое личное устройство для доступа к информационным ресурсам компании. BYOD-технологии позволяют не только категорировать работников фирмы и простых гостей на этапе аутентификации, но и вводить более сложную иерархию политик доступа к корпоративным ресурсам с учетом типа устройства, с которого пользователь входит в сеть, откуда именно человек заходит в сеть и что делает в сети.

MDM - необходимое решение для сотрудников банка для того, чтобы быть мобильными и эффективными вне офиса, иметь возможность использовать электронную почту. Данное решение состоит из двух частей: контрольного центра и клиентского программного обеспечения, которое включает средство шифрования для обеспечения конфиденциальности рабочих данных, и позволяет держать всю рабочую почту на устройстве в «боксе», находящемся под защитой. В «бокс» помещаются:

электронный почтовый ящик, календарные даты и события. Передача почты с сервера банка на основной модуль выполняется по защищенному узлу.

Если мобильное устройство сотрудника было утеряно или украдено, администратор ИБ благодаря MDM сможет быстро среагировать. «Бокс» с файлами будет уничтожен, либо устройство будет заблокировано, а информация удалена. Подобные действия реализуются специальными командами, отправленными на устройство через консоль.

Более того, доступ к «боксу» ограничен паролями разной степени сложности.

MDM-системы могут иметь встроенные антивирусные программы, а также могут быть частью мульти платформы системы информационной безопасности. Одними из лучших программных продуктов для MDM являются: GoodforEnterprise, McAfee, SAP, MobileIron[3].

В процессе построения защиты возникают сложности со своевременной обработкой информации. С нарастанием ее объема, администраторам информационной безопасности все сложнее анализировать возникающие угрозы и предотвращать их. Напомощьприходятсистемыкатегории SecurityInformationandEventManagement. Основными назначениями SIEM-систем выступают: консолидация и хранения журналов событий из различных источников, соотношение и обработка событий по правилам, автоматическое уведомление и предоставление средств для исследования происшествий[4].

С каждым днем развитие информационных технологий стремительно растет, а в организациях происходят кардинальные перемены в системах безопасности, вследствие чего компании-разработчики предлагают новые совершенные решения по защите информационных ресурсов. Но вместе с улучшающими преобразованиями появляются и новые угрозы, а риски в будущем остаются неопределенными, поэтому требования по созданию совершенно новых моделей программных средств будут повышаться, и проблема обеспечения сохранности конфиденциальной информации всегда будет актуальна.

Список литературы:

1. Banki.ru – финансовый журнал
2. https://www.banki.ru/wikibank/internet-bank/
3. Тинькофф Банк
4. https://www.tinkoff.ru/
5. LMsoft - Интеграция IT- систем
6. http://lmsoft.ru/products/produkty-mdm/
7. ITGlobal- компания, поставщик услуг
8. https://itglobal.com/ru-ru/company/glossary/security-information-and-event-management-siem/

УДК 322

Аипов Радик Гаязович
направление Информационная Безопасность (магистратура), гр. ИБм-21

Научный руководитель
Пекунов Андрей Ананьевич
доцент кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологически университет», г. Йошкар-Ола

СОЗДАНИЕ ШИФРОВАННОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ МЕЖДУ ПОДВЕДОМСТВЕННЫМИ ОРГАНИЗАЦИЯМИ

Актуальность работы: В связи с информатизацией всех значимых объектов организации, а также согласно требованиям Российского законодательства и нормативных документов ФСТЭК встала необходимость обеспечить безопасность получения, хранения и обработки персональных данных сотрудников организации возникла необходимость в сертифицированном решении для построения защищенного канала передачи данных и повышения надежности к различного рода кибератакам.

Исходя из поставленной цели, в работе решаются следующие **задачи**:

1) Испытания выбранного программного продукта на предмет отказоустойчивости;

2) Испытания выбранного программного продукта предмет надежности хранения секретных ключей и системных данных ограниченного доступа;

3) Исследование выбранного программного продукта на предмет совместимости с различным сетевым оборудованием;

4) Испытания выбранного программного продукта на предмет качества шифрования передаваемой информации;

5) интеграция программного продукта с используемыми аппаратными средствами и прикладным программным обеспечением организации.

6) Исследование и составление схемы локальной сети существующей инфраструктуры.

7)Исследование инфраструктуры на предмет возможности реализации защищённого канала связи, возможности эксплуатируемого оборудования и локальной сети.

8) Возможность построения модели защищенного канала связи поверх существующей инфраструктуры, а именно совместимость с различным оборудованием и программными продуктами эксплуатируемыми в организации

9) Выбор готового решения для создания шифрованного канала связи из существующих на рынке РФ с соответствием с действующим законодательством РФ, требованиям ФСТЭК, ФСБ в плане безопасности и защите передаваемой информации, иметь сертификаты на соответствие требованиям безопасности для средств защиты конденфициальной информации, включая персональные данные.

10) Тестирование выбранного программного решения построения шифрованного канала передачи данных;

Объектом исследованияявляются рассматриваемые программные продукты, выбранные для построения шифрованного канала передачи данных.

Предмет исследования составляет процесс создания и испытаний шифрованного канала передачи данных в организации и дальнейший его анализ с целью выявления угроз информационной безопасности.

Методы исследованиястатистические методы, методы прогнозирования и обнаружения угроз, криптографические методы, математический анализ, дискретная математика, теория полей и колец, методы шифрования, статистика.

Новизна исследованиязаключается:

- в предложенном программном решении построения шифрованного канала передачи данных для организации, отличающемся качественным шифрованием от известных способов создания защищенного канала передачи данных.

- в стойкости созданного защищённого канала к криптовзлому, и в скорости обработки информации.

Практическую ценность работы составляет реализация интеграции выбранного программного продукта с существующей инфраструктурой организации, в том числе с программным обеспечением из реестра отечественного ПОв целях исполнения плана по импортозамещению, отличающегося качественным шифрованием от известных способов создания защищенного канала передачи данных.

Выводы: В данной работе произведено исследование инфраструктуры на предмет возможности реализации защищённого канала связи, возможности эксплуатируемого оборудования и локальной сети.

Выбрано готовое решение для создания шифрованного канала связи из существующих на рынке РФ с соответствием с действующим законодательством РФ, требованиям ФСТЭК, ФСБ в плане безопасности и защите передаваемой информации, имеющее сертификаты на соответствие требованиям безопасности для средств защиты конденфициальной информации, включая персональные данные.

Осуществлено исследование выбранного программного продукта на предмет совместимости с различным сетевым оборудованием; испытание выбранного программного продукта на предмет качества шифрования передаваемой информации;

Осуществлены испытания выбранного программного продукта на предмет отказоустойчивости, испытание выбранного программного продукта на предмет отказоустойчивости; испытания выбранного программного продукта предмет надежности хранения секретных ключей и системных данных ограниченного доступа; исследование и составление схемы локальной сети существующей инфраструктуры.

Произведена интеграция программного продукта с используемыми аппаратными средствами и прикладным программным обеспечением организации.

Показана возможность построения модели защищенного канала связи поверх существующей инфраструктуры, а именно совместимость с различным оборудованием и программными продуктами эксплуатируемыми в организации

Реализована возможность построения модели защищенного канала связи поверх существующей инфраструктуры, а именно совместимость с различным оборудованием и программными продуктами эксплуатируемыми в организации

Показана возможностьиспользования рассматриваемого решения для создания шифрованного канала передачи данных на устаревшем оборудовании, на программном обеспечении из реестра отечественного программного обеспечения.

Осуществлён качественный выбор из существующих на сегодняшний момент российских решений по построению шифрованного канала передачи данных между подведомственными организациями.

Список литературы:

1. Пазизин, С.В. Основы защиты информации в компьютерных системах. / С.В. Пазизин – Москва, ТВП, 2003;

2. Грязнов Е.С., Панасенко С.А. Безопасность локальных сетей, Москва,издательство «ПиК», 2006.- 525с.;
3. Мельников В.В. Защита информации в компьютерных системах, Москва,Финансы и статистика, Электронинформ, 1997;
4. Моддовян А.А.., Моддовян Н.А., Советов Б. Я. Криптография, СПб.,издательство «Лань», 2000;
5. Норткатт С. и др. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу, Москва, Издательство «ЛОРИ», 2002;
6. А.Ю. Щеглов. Защита компьютерной сети от несанкционированного доступа, издательство «НиТ», Спб., 2009;
7. Романец, Тимофеев, Шаньги и «Защита информации в компьютерных сетях»;

УДК 004

Андреева Анастасия Ивановна
Направление Информационная безопасность автоматизированных систем (специалитет), гр. БИ-51

Научный руководитель
Александров Александр Петрович
доцент кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ КАНАЛАМ

Цель работы –осуществление мер по предотвращению утечки информации по акустическому каналу с помощью технической защиты.

В любой организации существует информация, утечка которой может нанести большой урон для бизнеса. Создавая систему защиты информации в организациях, необходимо учитывать угрозу утечки по акустическим каналам. Поскольку в акустических каналах утечки средой распространения информации является окружающий нас воздух, к закрытию возможности утечки по таким каналам стоит подойти особо тщательно. Поэтому при построении технической защиты информации на организации **актуально рассмотреть** необходимые меры, направленные на ликвидацию возможности выхода защищаемой информации по акустическим каналам за пределы периметра безопасности.

Акустическая защита – совокупность мер, направленных на исключение возможности утечки конфиденциальной информации за счет акустических полей.

Для обеспечения защиты используют пассивные и активные методы. Пассивные методы включают в себя звукопоглощение и звукоизоляцию. Звукопоглощение обеспечивается применением специальных герметических панелей из стекловаты высокой плотности различной толщины. Звукоизоляция обеспечивается специальными звукоизолирующими покрытиями стен. Звукоизоляцию целесообразно применять только в небольших помещениях, т.к. в больших помещениях звуковая энергия максимально поглощается, не достигнув стен. В тех случаях, когда пассивные меры не обеспечивают необходимого уровня безопасности, применяются активные методы.

К активным средствам относятся генераторы шума – технические средства, вырабатывающие шумоподобные электронные сигналы. Эти сигналя подаются на соответствующие датчики акустического или вибрационного преобразования. Акустические датчики предназначены для создания акустического шума в помещениях или вне их, а вибрационные – для маскирующего шума в ограждающих конструкциях (приклеиваются к ним, создавая в них звуковые колебания). Примером данного генератора является система виброакустического зашумления «Заслон». Система позволяет защитить до 10 условных поверхностей, имеет автоматическое включение вибропреобразователей при появлении

акустического сигнала. Эффективная шумовая полоса частот 100-6000 Гц[1].

Наиболее эффективным средством обнаружения диктофонов и акустических закладок является нелинейный локатор, устанавливаемый на входе в выделенное помещение и работающий в составе системы контроля доступа.

Для обнаружения работающих в режиме записи диктофонов применяются так называемые детекторы диктофонов. Принцип действия приборов основан на обнаружении слабого магнитного поля, создаваемого генератором подмагничивания или работающим двигателем диктофона в режиме записи.Дальность обнаружения диктофонов в неэкранированных корпусах может составлять 1 ... 1,5 м.

Зона подавления диктофонов зависит от мощности излучения, его вида, а также типа используемой антенны. Обычно зона подавления представляет собой сектор с углом от 30о до 80ои радиусом до 1,5 м (для диктофонов в экранированном корпусе)[3].

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно частота излучения около 20 кГц), воздействующие непосредственно на микрофоны диктофонов или акустических закладок, что является их преимуществом. Ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты диктофона или акустической закладки (усилитель начинает работать в нелинейном режиме) и тем самым - к значительным искажениям записываемых (передаваемых) сигналов. Например, комплекс «Завеса» при использовании двух ультразвуковых излучателей способен обеспечить подавление диктофонов и акустических закладок в помещении объемом 27 м3[4].

Также существуют программно-аппаратные комплексы для проверки выполнения нормальной эффективности защиты речевой информации от её утечки по акустическим и виброакустическим каналам. Одним из программно-аппаратныхкомплексов акустических и виброакустических исследований является «Спрут-7».Комплекс предназначен для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам, а также за счет низкочастотных наводок на токопроводящие элементы ограждающих конструкций зданий и сооружений инаводок от технических средств в речевом диапазоне частот, образованныхза счет акустоэлектрических преобразований. Комплекс обеспечивает измерение характеристик акустических сигналов, в том числе октавный,треть октавный анализ и анализ с использованием функции быстрого преобразования Фурье (БПФ), проведение исследований характеристик и проверку эффективности систем акустического и виброакустического зашумления, измерение уровней сигналов акустоэлектрических преобразователейс использованием функции БПФ[5].

В настоящее время на рынке конкурируют более 20 специализированных фирм, занимающихся разработкой, производством и реализацией технических средств защиты информации, которые позволяют эффективно решать задачу защиты информации от акустической речевой разведки. Совершенствование аппаратуры осуществляется в направлениях удешевления, увеличения функциональных возможностей и уменьшения мешающего влияния на объекты защиты [1].

Список литературы:

1. Ярочкин В.И.Информационная безопасность: Учебник для студентов

2. вузов. — М.: Академический Проект; Гаудеамус, 2-е изд.2004. — 544 с.
3. Хлестова Д.Р. Защита информации от утечки поакустическим каналам — Международный научный журнал «Символ науки» №11-3/2016 ISSN 2410-700X_. УДК 004
4. ВоронаВ. А., КостенкоВ. О.Способы и средства защиты информации от утечки по техническим каналам —Comp. nanotechnol,2016, № 3, 208–223с.
5. Хореев А.А. Техническая защита информации. Том 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008.
6. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО«Издательство Машиностроение», 2009 – 508 с.

УДК 004.056(075.8)

Андреев Дмитрий Александрович
направление «Информационная безопасность» (специалитет), гр. БИ-51

Научный руководитель

Нехаев Игорь Николаевич,
кандидат технических наук, доцент
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ В СРЕДЕ UNITY

Информация – один из самых важных частей любого ресурса. Её своевременное получение, эффективное использование, надлежащее хранение и безопасная передача играют определяющую роль в деятельности ресурса, сказываются на его прибыльности и развитии.

Однако есть, конечно, и существенный минус. Информация, хранящаяся в информационных ресурсах, находится под угрозой: её могут уничтожить, украсть, умышленно удалить или исказить. К тому же существует проблема того, что программисты, отлично знающие как правильно писать код, строить архитектуру программы не всегда хорошо понимают, как эту программу защитить.

Моей задачей является разработать систему, с помощью которой даже не знающий способы защиты приложения от различных угроз

безопасности человек, понимающий в программировании мог защитить свой продукт, написанный в среде Unityна языке C#.

Комплексной система называется, так как состоит из нескольких подсистем: подсистема шифрования переменных, подсистема шифрования текстовой информации, подсистема отправки подписанный сообщений на сервер.

Данные подсистемы были выбраны не случайно, проанализировав угрозы я выбрал наиболее востребованные и часто встречающиеся на реальной практике и постарался [1][2] найти наиболее оптимальные способы защиты от них.

Далее по подробнее о каждой.

Рис 1.

Подсистема шифрования переменных

Данная подсистема позволяет не хранить ее значение в чистом виде в памяти операционной системы. При помощи алгоритмов шифрования значение переменной всегда хранится в виде строки в памяти и не

может быть изменено спри помощи вредоносных программ, которые направлены на атаку памяти данного типа.

```
namespace UniCrypt.SafeVariableSpace
{
    public abstract class SafeVariable<T>
    {
        protected ICryptoAlgorithm CryptoAlgorithm;
        protected string EncryptedString;

        public T Value
        {
            get => Decrypt(EncryptedString);
            set
            {
                EncryptedString = Encrypt(value);
            }
        }

        public SafeVariable(ICryptoAlgorithm cryptoAlgorithm)
        {
            CryptoAlgorithm = cryptoAlgorithm;
        }

        public SafeVariable(string algorithmName)
        {
            CryptoAlgorithm = AlgorithmsStorage.Get(algorithmName);
        }

        public abstract T Decrypt(string message);
        public abstract string Encrypt(T value);
    }
}
```

Рис. 2.

Подсистема шифрования текстовой информации

Данная подсистема позволяет шифровать любую текстовую информацию, будь то игровые сохранения или просто информация, которую не рекомендуется показывать пользователям.

```
public class FileSaver<T> where T: class
{
    private string _fileName;
    private string _path = Application.persistentDataPath;
    private string _fullPath;

    public FileSaver(string fileName)
    {
        _fileName = fileName;

        _fullPath = $"{_path}/{_fileName}.txt";
}

    public FileSaver(string fileName, string path)
    {
        _fileName = fileName;
        _path = path;

        _fullPath = $"{_path}/{_fileName}.txt";

    }

    public void Save(T obj)
    {
        string jsonData = JsonUtility.ToJson(obj);

        if (!File.Exists(_path))
        {
            File.Create(_fullPath);
        }

        using (StreamWriter writer = new StreamWriter(_fullPath, false))
        {
            writer.Write(jsonData);
        }
    }
```

Рис. 3.

Подсистема отправки подписанный сообщений на сервер

Данная подсистема позволяет без особого труда отправлять подписанные запросы на сервер, а также проверять подпись на ответах сервера.

[3] Суть данного методы заключается в том, что злоумышленник может подменять запросы на сервер или отправлять ложные самостоятельно. Подписанные же сообщения практически невозможно подменить или изменить, так как сервер будет всегда проверять, подписано оно пользователем или нет.

Дополнительные функции

В качестве дополнительных функций мною были добавлены следующий программные модули:

- Модуль умного таймера – Данный модуль отвечает за то, что бы невозможно было обойти внутри игровой таймер при помощи изменения времени на устройстве. Данный таймер работает по такому принципу: после входа в приложение, при наличии интернет соединения, он отправляет запрос на сервер времени, в случае, когда

интернет соединения нет или сервер не отвечает, таймер сбрасывает время, которые пользователь провел вне игры.

- Криптографический модуль -Данный модуль использует IMEIкод устройства как ключ шифрования, для того что бы не хранить ключ шифрования в явном виде, так же данный модуль добавляет в данный ключ “соль” и различные битовые сдвиги, что бы его было сложнее восстановить.

Заключение

В результате работы, я получил работающую систему защиты, которую уже можно использовать по назначению. В своем новом проекте я обязательно включу ее в работу, что бы найти в ней возможные проблемы, такие как баги, ошибки, так как такие вещи обычно проявляют себя только во время реальной разработки. В планах улучшать данную систему, добавлять новые методы защиты и улучшать уже существующие.

Список литературы:

1. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.
2. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.
3. П. А. Тимошин,Перспективы развития электронной подписи, 2007, 223 с.

УДК 004.056

Апакаеа Яна Андреевна
направление Информационная Безопасность (специалитет), гр. БИ-51

Научный руководитель
Чекулаева Елена Николаевна,
канд. экон. наук, доцент кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологически университет», г. Йошкар-Ола

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ООО «АРБ МЕДИА»

Введение

Информация является одним из важнейших ресурсов любого предприятия.Своевременное получение информации, эффективное

использование, надлежащее хранение и безопасная передача являются ключевыми факторами в деятельности предприятия. Данные факторыотражаются на прибыльности и развитии предприятия или организации.

На сегодняшний день, для работы с информацией используются различные технические устройства. Однако, чаще всего, это – компьютер (или сеть компьютеров), подключенный кИнтернет сети.

Сложно переоценить эффективность ПК и скорость передачи данных через Интернет. Ни одна папка с бумажными документами не способна вместить столько информации и ни один факс не сможет передатьинформацию с такой скоростью. В этом основной плюс современных компьютерных технологий.

Несмотря на это, за этим всем кроетсязначительный минус:информация, хранящаяся в ПК предприятия и передаваемая его сотрудниками через Интернет, находится под угрозой.Информацию могут украсть, исказить,или уничтожить. Выход из строя компьютерной техники может привести к потере информационных данных,поэтому они должны быть соответственным образом защищены. Защита должна проводиться комплексно, защищая от всех возможных рисков.

Комплексная защита информационных ресурсов предприятия представляет собой систему мер по хранению, шифрованию, мониторингу доступа к ресурсам и их обмена. Данная система мер обеспечивает:

- защиту информации от разного рода вирусов и хакерских угроз;
- сохранность данных при физической утрате и поломках носителей информации;
- безопасность доступа к хранимым ресурсам;
- восстановление информационной системы в случае повреждений.

Конфиденциальная информация хранится на специальном секретном и удаленном сервере. Доступ к ней контролируется и определяется только руководством предприятия (ограничивается или разрешается определенным сотрудникам).

Система защиты информации создается из интегрированных моделей и включает в себя:

- терминальный модуль;
- модуль резервного копирования;
- модуль реагирования;
- модуль шифрования.

Терминальный модуль – это централизированная, управляемая IT инфраструктура предприятия с изолированным сервером для хранения

информации. Он обеспечивает сбор данных в безопасном месте (на одном или нескольких секретных серверах) и их защиту от несанкционированного доступа.

Модуль резервного копирования предназначен для создания копий информационных данных на основной и резервный секретный сервер. При возникновении какой-либо внештатной ситуация (отключения или сбоя основного секретного сервера, например), системы модуля переадресовывают информацию на резервный сервер. Вся информация, собранная и хранящаяся данным образом, шифруется модулем шифрования.

Модуль шифрования реализует кодировку буквенных и цифровых данных крипто стойкими алгоритмами. Ключи кодировки и шифровки информации передаются пользователю (руководителю) предприятия и не известны обслуживающему систему защиты персоналу. Заданный модуль обеспечивает защиту архивов, баз данных, приложений и электронной почты. С его помощью можно замаскировать факт наличия какой-либо конфиденциальной информации. Припоявлении какой-либо угрозы информационные данные блокируются модулем реагирования.

Модуль реагирования представляет собой модуль удаленного действия. Он предоставляет возможность при помощи так называемой «тревожной кнопки» включать, выключать и перезагружать секретный сервер. Кнопкой служит радио-брелок или кодовое SMS-сообщение. Отправленный «тревожной кнопкой» сигнал автоматически отключает все системы удаленного сервера. При этом, хранящаяся информация шифруется на жестких дисках. Восстановление информации можно будет произвести только при помощи специального ключа (карта Micro-SD), хранящегося у первого лица предприятия.

В заключении хочется отметить, что современная информационная безопасность компании строится на концепции комплексной защиты информации, предполагающей одновременное использование многих взаимосвязанных программно-аппаратных решений и мер социального характера, поддерживающих и дополняющих друг друга.

Список литературы:

1. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264 с. : ил.

2. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

3. Москвитин, Г.И. Комплексная защита информации в организации / Г.И. Москвитин. - М.: Русайнс, 2017. - 400 с.

УДК 836.2

Ахметзянова Лейсан Рустемовна
направление «Информационная безопасность» (специалитет), гр. БИ 41

Научный руководитель
Сидоркина Ирина Геннадьевна
доктор технических наук, профессор кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АНАЛИЗ СПОСОБОВ КЛАССИФИКАЦИИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ЗАЩИТЕ ИНФОРМАЦИИ

Актуальность использования систем обнаружения вторжений подтверждается растущим интересом крупных и мелких организаций, потому что является ключевым компонентом комплексной системы защиты информации.

Система обнаружения вторжений (СОВ) - это программные системы, предназначенные для выявления и предотвращения неправомерного использования компьютерных сетей и систем. Есть несколько разных способов классификации СОВ. В данной статье сосредоточимся на двух способах: обнаружение неправильного использования и обнаружение аномалий. Подход к обнаружению злоупотреблений исследует сетевую и системную активность на предмет известных злоупотреблений, обычно с помощью некоторой формы алгоритма сопоставления с образцом (рис. 1).

Рис. 1. Обобщенная архитектура системы обнаружения злоупотреблений

А подход к обнаружению аномалий основывает свои решения на профиле нормального поведения сети или системы, часто построенном с использованием статистических методов или методов машинного обучения (рис.2). Любое событие, не соответствующее этому профилю, считается аномальным.

Рис. 2. Обобщенная архитектура системы обнаружения аномалий

Таким образом, каждая из рассматриваемых систем имеет свои сильные и слабые стороны. Системы, основанные на неправильном использовании, обычно имеют очень низкую частоту ложных срабатываний, что указывает на частоту ошибок в случае ошибочно обнаруженных случаев невмешательства. По этой причине этот подход можно увидеть на практике в большинстве коммерческих систем. Однако они не могут идентифицировать новые или скрытые атаки, что приводит к высокому уровню ложноотрицательных результатов, которые представляют собой процент ошибок пропущенных случаев обнаружения. С другой стороны, системы, основанные на аномалиях, способны обнаруживать новые атаки, но в настоящее время производят большое количество ложных срабатываний. Это происходит из-за неспособности современных методов, основанных на аномалиях, адекватно справиться с тем фактом, что в реальном мире нормальное, законное использование компьютерной сети и системы со временем меняется, а это означает, что любой профиль нормального поведения также должен быть динамичным.

Делаем вывод, что рассматриваемые системы являются актуальными в СОВ, поскольку контроль системы не имеет никакого смысла без последующего анализа полученной информации. Поэтому важной характеристикой СОВ является анализ накопления ею данных. Этот анализ и описывается в двух системах: подход к обнаружению злоупотреблений и подход к обнаружению аномалий.

Список литературы:

1. Р. А. Голдсби, Т. Дж. Киндт, Б. А. Осборн и В. Х. Фриман. Куби Иммунология. У. Х. Фриман, 5-е издание, 2002 – с.200.
2. О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова «Обнаружение вторжений в компьютерные сети (сетевые аномалии)». Учебное пособие для вузов, 2013 – с. 221.
3. Howell D. Hackers often choose their corporate targets. // Investors Business Daily. — January 30, 2002 – p.207-220.
4. А.У. Актаева, Р. Ниязова, Н. Гагарина «Искусственной интеллектуальной системы для обнаружения вторжений», Текст научной статьи по специальности «Автоматика. Вычислительная техника»,2017 – с.49-50.

УДК 004.056.57:004.725.7

Бородин Андрей Викторович
направление Информационная безопасность (магистратура), гр. ИБм-21

Научный руководитель
Чекулаева Елена Николаевна
канд. экон. наук, доцент кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

О ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ РЕВЕРС-ИНЖИНИРИНГУ В СРЕДЕ ТУМАННЫХ ВЫЧИСЛЕНИЙ

Цель работы – исследование возможности существования скрытых вычислительных процессов в среде туманных вычислений. Показана связь идеи трансформации потока управления программы некоторым процессом, как метода обфускации, с возможностью подобной организации распределенных вычислений в сетях передачи данных, как метода маскировки отдельных процессов.

Актуальность. Степень воздействия информационных технологий на жизнь человека неуклонно возрастает. У этого феномена есть как положительные, так и отрицательные стороны.

Действительно, постоянный рост степени интеграции электронных схем, прогресс в деле микроминиатюризации сенсоров и исполнительных механизмов совместно с ростом энергонасыщенности последних, а также рост энергоемкости портативных источников питания, привели к появлению таких феноменов, как «смартфон», «интернет вещей», «умные дома», «умные улицы», «умные города», «дроны», освоившие не только три пространственных измерения, но и

основные среды присутствия технологий человечества, и т. п. Названные изменения, в целом, привели к удивительному росту качества жизни в мире. С другой стороны, начало XXI века было потрясено рядом скандалов, связанных с тотальной слежкой за деятельностью людей со стороны спецслужб технологически высокоразвитых стран и стран, кардинально ограничивающих права своих граждан.

Даже поверхностное осознание приведенных фактов делает очевидным формирование вывода о новом качестве вызовов, встающих перед человечеством. Одним из таких вызовов является предмет настоящей статьи. Результаты, описываемые здесь, могут быть использованы как во благо Человека, так и против него. В этом смысле актуальность предлагаемого исследования представляется весьма значительной. Речь пойдет о технологиях туманных вычислений и о возможности существования в рамках этих технологий вычислительных процессов, осознание цели, существования которых, доступно лишь их создателям.

Предварительные замечания. Термин «туманные вычисления» был введен в оборот вице-президентом компании CiscoSystems, Inc. Флавио Бономи в 2011 году. Он предложил концепцию туманных вычислений по аналогии с «облачными вычислениями», как расширение «облака» до границ сети. Технологически, концепция туманных вычислений тесно связана с распределёнными (облачными) дата-центрами, в которых серверы дата-центров могут располагаться во многих местоположениях, вплоть до границы сети. Таким образом, отличительная черта туманных вычислений – приближенность к конечным пользователям и поддержка их мобильности. Иначе говоря, среда туманных вычислений – локальные сети домашних хозяйств, предприятий и организаций, а также разного рода mesh-сети. Хостами среды туманных вычислений выступают смарт-сенсоры, контроллеры исполнительных устройств, internet-камеры, разного рода шлюзы и т. п.

Основные результаты. Оказывается, в среде туманных вычислений очень легко организовать скрытые вычислительные процессы. Для этого достаточно, чтобы хосты интернета вещей (IoT) могли функционировать в режиме «запрос-ответ». Заметим, этот режим является вполне естественным для IoT. Формализация соответствующего режима работы приведена в работе [3].

Базовая идея организации скрытых вычислительных процессов взята из статьи [2] и монографии [5]. В этих работах описана технология обфускации, основанная на предварительной деструктуризации

программы (сведении ее к спагетти-коду) с последующей псевдослучайной маркировкой операторов, некоторым их переупорядочиванием, а также с внедрением конструкции выполнения каждого оператора по маркеру. Соответственно псевдослучайный процесс, порождающий последовательность маркеров, обеспечивает эквивалентность потока управления модифицированной программы (без учета выполнения вспомогательных конструкций) и исходной. Такого рода преобразование исходной программы заметно усложняет задачу реверс-инжиниринга кода в ручном режиме. К тому же замена псевдослучайного процесса управления потоком на трудно обратимый процесс в сочетании с ограничением ресурса использования программы делает такуюобфускацию доказательно стойкой, в том числе и для автоматизированных методов реверс-инжиниринга [1]. Дополнительным фактором повышения стойкости к реверс-инжинирингу может стать рандомизация потока управления [4].

Теперь представим, что маркированные операторы спагетти-кода, иначе, элементарные функции скрытого вычислителя (ЭФСВ), распределены по хостам IoT (например, один оператор – одно устройство), а контекст исполнения оператора, его исходные и выходные данные передаются по сети в режиме «запрос-ответ». В таком случае реверс-инжиниринг обфусцированного процесса потребует совместной ревизии программного обеспечения всех хостов. Учитывая потребность в большинстве случаев в физическом доступе к устройствам при подобной ревизии, а также возможность реализации устройств на различных аппаратно-программных платформах, можно говорить о возникновении значительных трудностей в реализации автоматизированного реверс-инжиниринга даже в общем случае. Еще сильнее эта проблема усложняется в случае различий в имущественных правах на отдельные устройства и места их дислокации.

Рассмотрим принципы организации скрытых вычислительных процессов в среде туманных вычислений. Возможны два способа организации скрытых вычислений: синхронный и асинхронный.

При синхронном способе организации вычислений одно из устройств берет на себя функцию координатора. Это устройство собирает таблицу соответствия имеющихся в сети ЭФСВ сетевым адресам устройств и, в дальнейшем, осуществляет последовательное обращение к ЭФСВ с целью организации того или иного скрытого вычислительного процесса. Реверс-инжиниринг программного обеспечения устройства-координатора может вскрыть лишь факт наличия скрытых вычислений, суть вычислений остается недоступной

до тех пор, пока не удастся восстановить семантику всех вызываемых ЭФСВ.

При асинхронном способе организации вычислений каждый узел после выполнения своей ЭФСВ сам выбирает следующее устройство для выполнения следующей ЭФСВ. При этом инициатором скрытого вычисления может стать любой узел и, в то же время, он может не обладать всей полнотой знаний об инициируемом процессе. В этом случае реверс-инжиниринг оказывается еще более трудоемким по отношению к случаю синхронного способа организации вычислений: даже сам факт существования скрытых вычислений становится трудно идентифицируемым.

Выводы. Итак, в среде туманных вычислений могут существовать трудно обнаруживаемые скрытые вычислительные процессы. Еще более трудоемкой задачей может оказаться задача идентификации назначения этих процессов, цели их существования. Таким образом, с одной стороны, мы получаем уникальный механизм реализации скрытых возможностей сетей, например, по выявлению атак на программное обеспечение узлов сети (через реверс-инжиниринг и последующую модификацию кода с целью достижения нарушителем своих целей [3]), а с другой стороны, с использованием описанного подхода среда туманных вычислений может быть использована собственно нарушителем, также для (негласного) достижения своих целей.

Последний факт заставляет задуматься о мерах противодействия возникновению скрытых возможностей сред туманных вычислений. К этим мерам следует отнести: 1) контроль кода хостов на отсутствие недокументированных возможностей; 2) строгая спецификация сообщений внутри среды туманных вычислений; 3) мониторинг среды передачи данных на предмет соответствия сообщений спецификации; 4) ведение списка разрешенных взаимодействий; 5) взаимная идентификация и аутентификация узлов сети в пределах списка разрешенных взаимодействий; 6) иерархическая организация сети; 7) по возможности разрешение взаимодействия между узлами только разных уровней иерархии сети.

Список литературы:

1. Бородин, А. В. Вариант постановки задачи противодействия реверс-инжинирингу кода в рамках императивной парадигмы программирования / А. В. Бородин // Инженерные кадры – будущее инновационной экономики России. – 2019. – № 4. – С. 8-12.

2. Бородин, А. В. Линейные конгруэнтные последовательности максимального периода в задачах обфускации программ / А. В. Бородин //

Кибернетика и программирование. – 2016. – № 6. – С. 1-19. – DOI: 10.7256/2306-4196.2016.6.18499.

3. Бородин, А. В. О задаче контроля целостности программного обеспечения удаленного недоверенного хоста / А. В. Бородин, А. А. Старовойтов // Актуальные направления научных исследований: перспективы развития: материалы III Международной научно–практической конференции (Чебоксары, 8 октября 2017 г.). – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 119-123. – DOI: 10.21661/r-464620.

4. Вахрамеева, Т. Е. Рандомизация потока управления как дополнительный метод обфускации программ / Т. Е. Вахрамеева, А. А. Романова, А. А. Сенькова и др. // Россия в многовекторном мире: национальная безопасность, вызовы и ответы. Двадцатые Вавиловские чтения: материалы международной междисциплинарной научной конференции. – Ч. 2. – Йошкар-Ола: Поволжский государственный технологический университет, 2017. – С. 203-205.

5. Львович, И. Я. Перспективные тренды развития науки: техника и технологии. Том 1 / И. Я. Львович, В. А. Некрасов, А. П. Преображенский и др. – Одесса: КУПРИЕНКО СВ, 2016. – 197 с.

УДК 004.056

Васильева Елена Сергеевна, Сосорева Анна Игоревна
направление Информационная безопасность автоматизированных систем (специалитет), гр. БИ-42

Научный руководитель
Смирнов Владимир Иванович
старший преподаватель кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА ОНТОЛОГИИ ПО ФИЗИЧЕСКИМ ЭФФЕКТАМ В ПРОГРАММЕ PROTEGE[*]

Цель работы – создание онтологии по физическим эффектам (ФЭ) в программе Protege на основе известных баз данных ФЭ.

[*] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта «Развитие теоретических основ для методов утечки и перехвата речевой информации по техническим каналам с использованием физических эффектов» (проект № 24/2020).

В настоящее время эксперты по предметным областям всё чаще применяют онтологии, поскольку они облегчают работу по поиску информации в конкретной области знаний.

Онтология - это формальное описание понятий предметной области и отношений между ними в рассматриваемой предметной области, свойств каждого понятия, описывающих различные атрибуты понятия, а также ограничений, наложенных на слоты (атрибуты класса) [1]. Онтология облегчает создание и поддержку явных моделей предметных областей и позволяет включать эти модели в программный код [2].

Метод обработки информации на основе онтологии позволяет создавать уникальные справочные системы (программное обеспечение), сокращать время на поиск необходимой информации о ФЭ, а также структурировать ФЭ в удобном для пользователя формате [3]. Знания о ФЭ помогают лучше понимать принципы работы технических систем, их фундаментальные физические возможности и ограничения.

Изучение ФЭ возможны только при наличии полной и достоверной информации: начиная с входного воздействия на систему и заканчивая результатом воздействия. Онтология по ФЭ может использоваться широким кругом лиц: от исследователей до специалистов в данной области.

Существует большое количество различных программных средств и библиотек для создания онтологий. Для разработки онтологии по физическим эффектам использовалась программа Protege.

Программа Protege включает редактор онтологий, который позволяет проектировать онтологии, раскрывая иерархическую структуру классов. Данный инструмент поддерживает язык OWL и позволяет генерировать HTML-документы, которые отражают структуру онтологии [4].

В настоящее время необходимость обработки и хранения ФЭ требует структуризации. В частности, необходимы тщательная проработка понятийной структуры предметной области, а также выделение разных уровней абстракции путем введения универсальных онтологических отношений типа "класс-подкласс", "часть-целое" и т.д. Введение таких отношений приводит к унифицированным иерархическим структурам данных.

Первым шагом при создании онтологии является создание классов (рис. 1). При создании классов использовались работы [5] и [6].

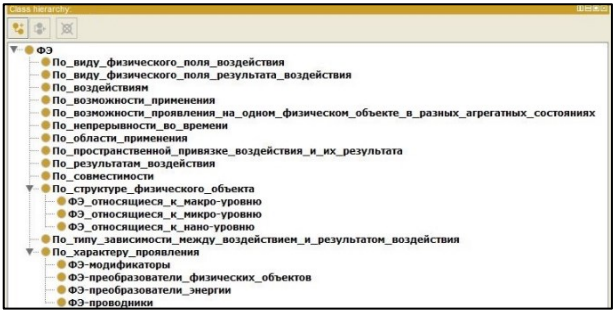


Рис. 1. Создание классов

Далее создаем экземпляры для всех классов (рис. 2).

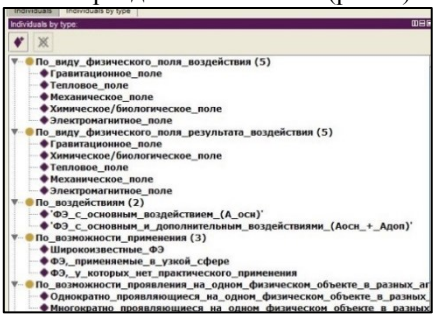


Рис. 2. Создание экземпляров классов

По полученным связям между классами онтологии строим граф. Частичный граф разработанной онтологии представлен на рис. 3.

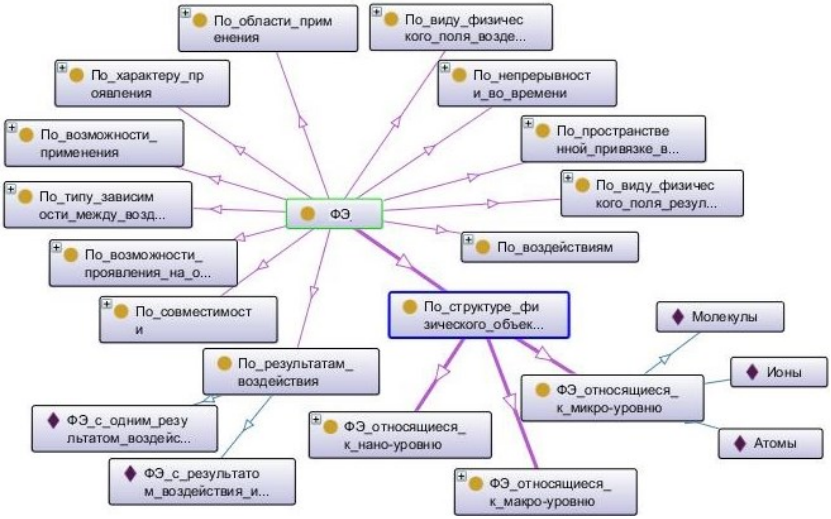


Рис. 3. Частичный граф онтологии

Выводы

Таким образом, разработанная онтология может быть полезна заинтересованным пользователям для информационного поиска проявляющегося эффекта при создании или изучении технической системы (физического объекта). В нее включены: тип взаимодействия, физические поля, их модификации и характеристики, параметры физических объектов, проявляющийся физический эффект, что позволяет детально исследовать закономерности проявления результатов взаимодействия объектов материального мира, осуществляемого посредством физических полей.

Список литературы:

1. Сидоркина И.Г. Системы искусственного интеллекта: учебное пособие / И.Г Сидоркина. – М.: КНОРУС, 2020. – 246 с.

2. Темникова Е.А. Разработка онтологии предметной области на примере учебного центра / Е.А. Темникова // Системный анализ и прикладная информатика. – 2013. – №4 (40). – С. 198-201.

3. Зарипова В.М. Онтологическая база знаний по физико-техническим эффектам для автоматизации технологических процессов. / В.М. Зарипова, И.Ю. Петрова, Ю.А. Лежнина, Е.Н. Фабер // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2015. – №4. – С. 47-56.

4. Белоусова И.Д. Онтологическая модель управления требованиями в процессе профессиональной подготовки ИТ-специалистов / И.Д. Белоусова,

Л.В. Курзаева, Ю.С. Лактионова, А.М. Агдавлетова // Успехи современной науки. – 2016. – Т. 1. – № 3. – С. 98-100.

5. Соболев А.Н. Физические основы перспективной вычислительной техники: учебное пособие / А.Н. Соболев, Б.Ф. Лаврентьев. – Йошкар-Ола: Марийский государственный технический университет, 2007. – 208 с.

6. Сидоркина И.Г. Уточнение классификации технических каналов утечки информации по физической природе носителя с учетом физических эффектов / И.Г. Сидоркина, В.И. Смирнов // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуника-ционные системы. - 2020. - № 1 (45). - С. 37-46.

УДК 001.05

Ватютов Роман Андреевич
направление Радиотехника, гр. РТм-11

Научный руководитель
Егошина Ирина Лазаревна,
доктор технических наук, профессор
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

БОРТОВАЯ РАДИОЛОКАЦИОННАЯ СИСТЕМА ПОСАДКИ ВЕРТОЛЕТА

Одним из самых сложных этапов пилотированию вертолета является посадка на неподготовленную площадку. Эта задача сопровождается повышенным риском аварии и человеческих жертв. Такие тяжелые условия пилотирования существуют в военной авиации, когда необходимо посадить вертолет на неподготовленную или неразведанную площадку, например, высадка, эвакуация, доставка боеприпасов и грузов в боевых условиях. Условия недостаточной видимости являются одной из ключевых проблем при посадке на неподготовленные ПП. Под условиями недостаточной видимости (УНВ) понимается слабая или нулевая оптическая видимость за кабиной обстановки, обусловленная любым из следующих факторов или их сочетанием: слабая освещенность, неблагоприятные метеорологические условия (туман, метель и т. д.), поднимаемый винтом вертолета вихрь твердых частиц. Последний из перечисленных факторов представляет собой особую опасность.

Критическим показателем, снижающим видимость, является то, что воздушная струя от несущего винта поднимает твердую взвесь при

посадке на сухой или заснеженный грунт. Это может привести.к неправильной оценке пилотом положения вертолета относительно земли. Также из-за этого могут остаться незамеченными препятствия в зоне посадки, например, большие камни, статичные и движущиеся объекты. Термин «пыльный вихрь» описывает это явление при посадке или взлете на сухой поверхности. Подобные же условия при посадке или взлете на заснеженной поверхности описываются термином «снежный вихрь».

Согласно данным Управления инспекции по безопасности полетов Федерального агентства воздушного транспорта РФ в период с 2001 по первую половину 2014 гг. события при посадке стали причиной 6 катастроф и 24 аварий гражданскихвертолетов.

Посадка вертолета в УНВ опасна тем, что вынуждает пилота полагаться на собственные ощущения и бортовые навигационные приборы, данных от которых зачастую оказывается недостаточно. Однако, еще проходя обучение, пилоты учатся при посадке полагаться в основном на внешнюю визуальную информацию, самостоятельно просматривая выбранную зону посадки на предмет опасности. При этом наземныеобъектыиспользуютсяимивкачестве ориентиров для управления пространственным положением воздушного судна. Приобретенные навыки становятся особенно важными и необходимыми при посадке или маневрировании вблизи различных препятствий, таких как деревья, линии электропередач, мачты и т. д. Пилоты вынуждены постоянно контролировать пространственное положение вертолета из-за присущей технике неустойчивости. Но при управлении вертолетом в тяжелых метеоусловиях, например, в снегопад или песочную бурю, наземные объекты-ориентиры не позволяют пилотам использовать визуальный способ управления. Из-за отсутствия визуального метода у пилота резко возрастает зависимость от собственных интуитивных ощущений. Однако в необычных гравитационно-инерциальных условиях, как, например, в воздухе, информация, передаваемая вестибулярным аппаратом, может неправильно идентифицироваться мозгом. Это в свою очередь приводит к дополнительным физическим нагрузкам на пилота и может иметь потенциально опасные последствия в таких условиях пилот может испытывать кратковременную пространственную дезориентацию.

Дезориентация может принимать различные фор- мы: пилот не осознает бокового уклона вертолета; у пилота создается ложное ощущение бокового уклона, движения или поворота вертолета, хотя в действительности ВС находится в состоянии висения. Иллюзия

движения может происходить во всех шести степенях свободы движения тела, то есть пилоту может казаться, что вертолет линейно перемещается по декартовым осям *x*, *y*, *z* (иллюзия линейного движения) или поворачивается вокруг любой из трёх взаимно перпендикулярных осей (рыскание, тангаж, крен). Технологические решения проблемы безопасной посадки вертолета на неподготовленную площадку в УНВ находятся на различных этапах готовности. На сегодняшний день в мире активно ведутся разработки по созданию систем посадки вертолета, однако на данный момент не существует готового оборудования для массового производства [4]. Системное решение по обеспечению безопасной посадки должно решать две задачи:

1) обеспечивать ситуационную осведомленность о пространственном положениивертолета;

2) обеспечивать ситуационную осведомленность о состоянии зоны посадки.

Из-за отсутствия аналогов на российском рынке, предлагается использовать радары W-диапазона и лидеры зарубежного производства. Радары W-диапазона – это активная радиолокационная система (РЛС) миллиметрового диапазона с рабочей частотой 77–94 ГГц, которая может осуществлять эффективное сканирование сквозь пыльный вихрь. Лидеры, несмотря на то, что они имеют более высокое затухание в пыльном вихре, дожде и тумане, чем РЛС W-диапазона, при сканировании зоны посадки на наличие препятствий могут обеспечить намного более высокое пространственное разрешение, поэтому целесообразно использовать обе системы как основную и резервную.

Список литературы:

1. Бакулев П.А. Радиолокационные системы. Учебник для вузов. – М.: Радиотехника, 2004, - 320 с.

2. Баскаков А. И. Исследование ослабления радиоволн в гидрометеорах и в пылевом облаке для бортовой радиолокационной системы безопасной посадки вертолета // Радиотехнические тетради. 2011. №44. С. 45-48

3. Основы построения радиолокационных станций радиотехнических войск: учебник / В.Н. Тяпкин, А.Н. Фомин, Е. Н. Гарин [и др.]; под общ.ред. В.Н. Тяпкина. – 2-е изд., перераб. – Красноярск: Сиб. федер.ун -т. – 2016. – 536 с.

УДК 004.056

Гаврилов Михаил Владимирович
Направление «Информатика и вычислительная техника» (магистратура),
гр. ИВТМ-01-19

Научный руководитель
Галанина Наталия Андреевна,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения информационных систем
ФГБОУ ВО «Чувашский государственный университет им. И.Н. Ульянова», г. Чебоксары

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЭЛЕКТРОННОГО УЧЕТА УСПЕВАЕМОСТИ СТУДЕНТОВ

Цель работы – проектированиесистемы электронногоучетауспеваемости студентов в балльно-рейтинговом виде.Рассмотрение положительных черт балльно-рейтинговой системы.

Актуальность темы заключается в том, чтовнедрение системы электронного учета успеваемости студентов в образовательный процесс позволяет реализовывать механизмы обеспечения качества и оценки результатов обучения, активизировать учебную работу учащихся, у которых появляются стимулы управления своей успеваемостью.

Ознакомление сбалльно-рейтинговой системой(БРС). Балльно-рейтинговая система[3]- одна из современных технологий, которая используется в менеджменте качества образовательных услуг. Система балльно-рейтинговой оценки знаний является основным инструментом оценки работы студента в процессе учебно-производственной, научной, внеучебной деятельности и определения рейтинга выпускника на выходе. Она позволяет реализовывать механизмы обеспечения качества и оценку результатов обучения, активизировать учебную и внеучебную работу студентов. Достоинства БРС:

- способствует повышению объективности оценки студенческих достижений в учебе. Экзамен перестает быть «последним приговором», потому что он только добавляет баллы к тем, которые набраны за семестр;
- позволяет более точно оценивать качество учебы;
- снимает проблему «сессионного стресса», так как, если по завершении курса студент получает значительную сумму баллов, он может быть освобожден от сдачи экзамена или зачета.

*Выбор средств разработки.*Для разработки системы была выбрана CMSсистема Joomla[1]:это система управления содержимым (CMS), написанная на языках PHP и JavaScript; в качестве хранилища базы данных при разработке использовалась СУБД MySQL[2]. Joomla является свободным программным обеспечением, распространяемым под лицензией GNU GPL.

В первую очередь была спроектирована блок-схема алгоритма работы системы для пользователей,по которой уже разрабатывалась система в зависимости от типа пользователя,который в разработанной системе отличается доступным функционалом.

Для того чтобы интерфейс системы был «дружелюбен» к пользователю, был написан новый собственный шаблон[4] интерфейса, который предоставляет пользователям более удобный ипростойвнешний вид системы.

Каждый студент может зарегистрироваться в системе самостоятельно, но авторизоваться сможет только после того, как будут подтверждены его учетные данные и принадлежность к соответствующей группе.В системе реализованы расписание занятий для каждой группы и электронный журнал по каждому предмету. В этот журнал заносятся данные о посещаемости и активности на парах, а также подсчитывается количество пропущенных занятий и вычисляется предположительная итоговая оценка за семестр. Студенты могут видеть не только свою успеваемость, но и успехи других (рис.).

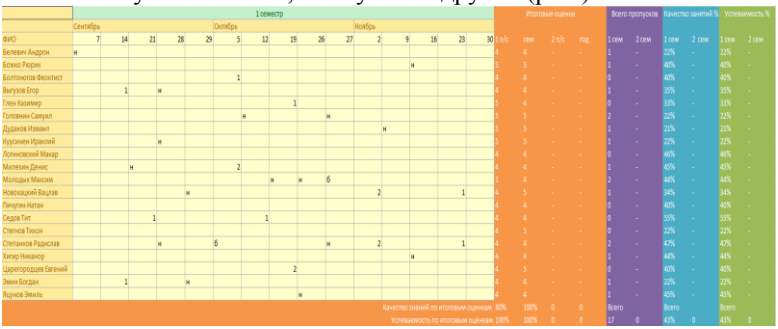


Рис.1. Журнал успеваемости студентов по предмету

В системе по каждому предмету есть возможность просматриватьзадания, которые необходимо выполнить, а также весь необходимый материал для изучения и выполнения лабораторных работ[4]. Подобная реализация очень удобна и упрощает поиск информации.

В своем профиле каждый студент может просмотреть более подробно статистику собственнойуспеваемости и информацию о несданных работах;существует возможность сравнивать текущую успеваемость с другими учебными семестрами.

Заключение. Таким образом, внедрение электронной системы учета успеваемости студентов будет положительно сказываться на успеваемости студентов, позволяя им беспрепятственно «заглядывать» в журнал, оценивать свои успехи, сравнивать их с достижениями других студентов и анализировать свое положение, что существенно повышает мотивацию к учебе.

Список литературы:

1. Joomla[Электронный ресурс] / joomla.org. – URL: http:// joomla.org (дата обращения: 24.10.2020)
2. MySQLReferenceManual[Электронный ресурс] / dev.mysql.com – URL: https:// dev.mysql.com/ (дата обращения: 24.10.2020)
3. Положение о балльно рейтинговой системе [Электронный ресурс] / rea.ru – URL: https://www.rea.ru/ru/org/faculties/turfak/Pages/BRV.aspx/ (дата обращения: 24.10.2020)
4. CSS [Электронный ресурс] / ru.wikipedia.org– URL: https://ru.wikipedia.org/wiki/CSS./ (дата обращения: 24.10.2020)
5. Галанина Н.А. Анализ непозиционных цифровых фильтров по квазипозиционной модели. Вестник Чувашского университета, 2000. - № 3-4.- С. 116-121.

УДК 004.032.26

Ганин Иван Сергеевич
направление Информатика и Вычислительная техника (магистратура), гр. ИВТм-12

Научный руководитель
Малашкевич Василий Борисович,
к.т.н., доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМА РАСПОЗНАВАНИЯ РЕЧЕВЫХ КОМАНД НА ОСНОВЕ НЕЙРОСЕТЕВОЙ МОДЕЛИ АВТОРЕГРЕССИИ

Цель работы –разработка системы распознавания речевых команд на основе нейросетевой модели авторегрессии, в среде разработки Python.

Речь как система, инструментомудовлетворения информационно-коммуникативныхпотребностей человеческого сообщества, остаётся в настоящее время сложной и поддающейся для искусственной реализации компонентой человеко-машинных систем.

В первую очередь это связано с проблемой автоматического распознавания речи, и рамках которой определились три прикладные направления:

- Идентификация голоса;
- Распознавание голосовых команд;
- Распознавание речи – преобразование непрерывных звуковых стимулов (звуков) в грамматически правильный текст.

Наиболее известным подходом к распознаванию речи, хорошо себя и задачах идентификации голоса и голосового управления, является предварительное формирование эталонной базы слов или фраз и последующая, основанная на сравнении с этой базой, идентификация предъявленных звуковых образов. Однакопопытки применениянуказанного подхода для распознавания непрерывной речи оказались неэффективными. Причина этого заключается в несоответствии искусственных процедурраспознаванияслов по априорным распределениям вероятности, появления их вариативных звуковых признаков естественным процессам преобразования звуковых раздражителей в органах чувств человека в элементы языка и, далее, в их графические или семантические эквиваленты.

Выбранная в работенейросетевая концепция моделирования процесса восприятия речи определяет собой способ формирования системы признаков её элементов на основе анализа звуковых раздражителей, которые используются вестественном органе слуха человека. Свойства свидетельствуют об избирательной чувствительности его волосковых леток и спектральным составляющим звукового давления, причем степень возбудимости этих клеток не линейно зависит от давления. Экспериментальное исследование спектрального состава звуков речи для голосового диапазона указывает на достаточность использования для распознавания диапазона частот F=300…2400 Гц, заключающего в себя основную энергию звуковых колебаний. Таким образом, общая последовательность формирования признаков элементов речи, необходима для функционирования нейросети, должна содержать:

- Дискретизацию непрерывного сигнала;
- Разложение сигнала в спектр;
- Выбор необходимого ряда спектральных составляющих. [1]

Исследователи из FAIR и StanfordUniversity опубликовали новую нейросетевую архитектуру для моделирования временных рядов. AR-Net комбинирует в себе преимущества традиционных статистических моделей и нейросетей. Моделирование временных рядов применяется для прогнозирования и распознавания аномалий. Классические модели, как авторегрессия (AR), не способны справиться с большими объемами данных для обучения. В особенности это актуально для данных, которые содержат в себе длительные нелинейные зависимости. Несмотря на это, их преимущество по сравнению с нейросетевыми подходами заключается в интерпретируемости модели и ее легковесности.

Чтобы обойти ограничения по масштабированию статистических моделей, в обработке естественного языка используют sequence-to-sequence модели. В частности методы, которые основаны на RNN. Такие методы позволяют получить более выразительную модель. Несмотря на то, что RNN-методы хорошо масштабируются на большие объемы данных, они могут быть слишком сложными для типичных временных рядов. Это может результировать в невозможность интерпретировать результаты модели. Исследователи фокусируются на необходимости создать масштабируемую и интерпретируемую модель для моделирования временных рядов. AR-Net улучшает классические авторегрессионные модели с помощью дополнительной полносвязной сети. Полносвязная модель не только так же интерпретируема, как и авторегрессия, но и масштабируема и проста в использовании.

Архитектура AR-Net имеет два преимущества перед традиционной статистической моделью:

- AR-Net может улавливать длительные последовательности зависимостей. Это важно для случаев мониторинга высокочастотных данных;
- Модель автоматически выбирает и оценивает важные коэффициенты из авторегрессии

Рассмотрим временной ряд y1 , … , yt, выраженный как процесс в авторегрессионной модели. Чтобы предсказать следующий временной шаг yt, каждая прошлая величина из y умножается на выученный wi вес. Это вес называется коэффициентом авторегрессионной модели.

Если учитывается длительный порядок предшествующих данных, традиционные подходы обучаются медленнее. В AR-Net это обходят с помощью обучения нейросети с стохастическим градиентным спуском.

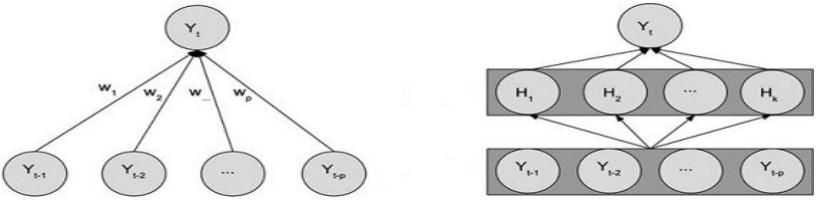


Рис.1.

Слева: самая простая AR-Net без скрытых слоев. Справа: структура стандартной AR-Net

Нейросеть выучивает коэффициенты авторегрессионной модели. AR-Net справляется с предсказанием временных рядов так же хорошо, как и статистическая модель. При этом имеет преимущество при обучении модели на высокочастотных данных.[2]

Список литературы:

1. Система распознавания фонетических образов на основе нейросетевой модели восприятия речи Е.М.Васильвев, В.В. Меренков. [Электронный ресурс] https://cyberleninka.ru/article/n/sistema-raspoznavaniya-foneticheskih-obrazov-na-osnove-neyrosetevoy-modeli-vospriyatiya-rechi/viewer

2. AR-Net: нейросеть для моделирования временных рядов [Электронный ресурс]https://neurohive.io/ru/novosti/ar-net-nejroset-dlya-modelirovaniya-vremennyh-ryadov/

УДК 004.056

Глебова Екатерина Николаевна
Направление Информационная безопасность автоматизированных систем (специалитет), гр. БИ-51

Научный руководитель
Пекунов Андрей Ананьевич
доцент кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СТАТИЧЕСКИЕ МЕТОДЫ АНАЛИЗА КОДА НА ПРЕДМЕТ УЯЗВИМОСТИ

Сейчас очень много говорят о методах статистического анализа кода на уязвимости. Статический анализ кода — это процесс выявления ошибок и недочетов в исходном коде программ.

Главное преимущество статического анализа состоит в возможности существенной снижении стоимости устранения дефектов в программе.

Чем раньше ошибка выявлена, тем меньше стоимость ее исправления.

Инструменты статического анализа позволяют выявить большое количество

ошибок этапа конструирования, что существенно снижает стоимость разработки всего проекта.

Существуют, к примеру, статические анализаторы, работающие в фоновом

режиме сразу после компиляции и, в случае нахождения потенциальной ошибки,

уведомляющие об этом программиста[1]

Задачи статического анализа:

1. Оптимизация программ (вычисление константных выражений, обнаружение мертвого кода, распараллеливание программ)
2. Преобразование программ (перевод на другие платформы, языки и библиотеки)
3. Обфускация/ деобфускация
4. обнаружение ошибок

Для анализа кода приложения на уязвимости обычно используют три подхода, как вместе, так и порознь.

1. Сигнатурный поиск
2. Исследование моделей выполнения кода.
3. Исследование потока вычислений

Рассмотрим каждый подход подробнее

Сигнатурный поиск.

Самый простой метод. Основан на поиске в основном коде вхождений заданной синтаксической модели, которая приводит к возникновению уязвимостей. Очевидно, что из-за этого в качестве основного этот способ не может быть использован – слишком велика вероятность как ложных срабатываний, так и пропущенных угроз. В основном метод используется для выявления подозрительных участков кода, нуждающихся в дополнительном анализе[2].

Исследование моделей выполнения кода

Куда более продвинутый способ. Основан на поиске такой комбинации обрабатываемых приложением данных, которые способны привести к возникновению уязвимости. Метод не учитывает многие факторы кода и зачастую дает ложноположительные результаты. К примеру, такой анализ может обнаружить уязвимость функции к XSS-

инъекции, в то время как на самом деле поток данных успешно фильтруется и осуществление такой атаки невозможно.

Исследование потока вычислений

Основан на использовании символических вычислений – преобразования конкретного кода в его абстрактную интерпретацию, способную эффективно работать не только с четко заданными, но и с неизвестными переменными. В дальнейшем на основе этой методики разрабатывается модель уязвимости к определенному типу атак, записанная символическим языком, что значительно упрощает и уточняет поиск проблемных мест в коде

Виды статического анализа

1. Синтаксический анализ (поиск по шаблону)
2. Анализ потока управления
3. Анализ потока данных (анализ состояний программы)
4. Анализ параллельного выполнения программы

Синтаксический анализ

Рассматривается одна или несколько последовательностей конструкций, без учёта контекста программы.

Поиск в исходном коде конкретных или параметризируемых шаблонов. Параметризируемый шаблон представляет собой конструкции программы и переменные в качестве параметров.

Шаблон представляет собой конструкции программы и переменные в качестве параметров[3].

Анализ потока управления

ControlFlowAnalysis.

Построение графа потока управления или другого представления программы удобного для проведения анализа потока данных (на входе-исходный код, на выходе – модель программы)

Анализ потока данных

Анализируются изменения данных в конструкциях программы

Видыанализапотокаданных: Reaching Definitions, Available Expressions, Constant Propagation, Very Busy Expressions, Анализсостоянийобъектовпрограммы

Классификация:

1. Направление анализа (прямой, обратный)
2. Объединения результатов (may-анализ – полные результаты, must-анализ – точные результаты)[4]

Область статического анализа активно развивается, появляются новые диагностические правила и стандарты, некоторые правила устаревают. Поэтому нет смысла пытаться сравнить анализаторы, на

основании списков обнаруживаемых дефектов. Единственный способ сравнить инструменты, это проверить с их помощью набор проектов и посчитать найденных ими количество настоящих ошибок[5].

Список литературы:

1. ДиодмидисСпинеллис. Анализ программного кода на примере проектов
2. OpenSource/ ДиомидисСпинеллис –М: «Вильямс», 2004. 528 с
3. АветисянА.,БелеванцевА.,Бородин А ., Несов В., Использование статического анализа для поиска уязвимости и критических ошибок в исходном коде программ.//Труды института системного программирования РАН.2011.Т.21.С.23-38.
4. Глухих М.И., Ицыксон В.М. Программная инженерия. Обеспечение качества программных средств методами статического анализа. СПб.: Изд-во Политехн. ун-та, 2011. 150 с.
5. Аветисян А. И. Современные методы статического и динамического анализа программ для решения приоритетных проблем программной инженерии: автореф. дис. … д-ра физ.-мат. наук: 05.13.11/АветисянАрутюнИшханович. – М., 2011. – 36 с.
6. Аветисян А. И., Бородин А. Е. Механизмы расширения системы статического анализа Svace детекторами новых видов уязвимостей и критических ошибок. Труды ИСП РАН том 21, 2011. С. 39-54.

УДК 004.056

Гоголев Игорь Михайлович
направление Информационная Безопасность (магистратура), гр. ИБм-21

Научный руководитель
Михайлов Андрей Владимирович,
доцент, кафедры информационная безопасность
ФГБОУ ВО«Поволжский государственный технологический университет»,г. Йошкар-Ола

SIEM СИСТЕМА ФИНАНСОВОЙ ОРГАНИЗАЦИИ ДЛЯ СБОРА И АВТОМАТИЧЕСКОГО АНАЛИЗА СОБЫТИЙ В КОРПОРАТИВНОЙ СРЕДЕ

Цель работы – Обеспечение качественного выбора из существующих на сегодняшний момент российских SIEM систем для своевременного обнаружение атак и нарушителей в корпоративной среде финансовой организации.

Одной из главных задач для финансовой организации в осуществлении своей деятельности является своевременное проведение платежей и быстрое реагирование на возможные события и угрозы со стороны мошеннических попыток проведения платежей.

За последнее время сильно повысились сложность и координированность атак [1]на информационные системы.Современные киберпреступники при атаках на системы защиты компаний используют все более изощренные методы [2]. Чтобы противодействовать им, службы информационной безопасности вынуждены анализировать и интерпретировать огромное количество событий в день.

Вместе с тем усложняется и применяемый комплекс средств защиты информации— сетевые и хостовые системы обнаружения вторжений, DLP-системы, антивирусные системы и межсетевые экраны, сканеры уязвимостей и прочее. Каждое средство защиты генерирует поток событий с разной детализацией и зачастую увидеть атаку можно только по наложению событий из разных систем [3]. Для оперативного обнаружения и реагирования на возрастающие количеством внешних и внутренних угроз безопасности в информационных системах необходимо иметь инструменты, позволяющие анализировать в реальном времени происходящие события.

Для выхода из создавшейся ситуации финансовым организациям желательно применять в своей деятельности программное обеспечение, которое предоставляет единую архитектуру для интегрирования информации о безопасности и управления событиями (SIEM), определения аномальных ситуаций, анализа инцидентов, реагирования на них, управления настройками и устранения уязвимостей.

Использование системы SIEM в финансовой организации позволит осуществить сбор событий из различных источников и анализ событий,

позволит привести информацию о событиях к единому формату с учетом известных угроз информационной безопасности, так и выявление новых неизвестных угроз.

SIEM система осуществляет сбор логов из различных программных и аппаратных источников и позволяет работать с ними в рамках единого интерфейса, а так же позволяет решать проблемы с оперативным реагированием на события и угрозы проведения мошеннических попыток проведения платежей,

В настоящее время на рынке программных средств SIEM имеются несколько российских разработок.

Исследование компании PositiveTechnologies[4] показало, что трудозатраты наработу с SIEM-системой — больной вопрос

длябольшинства компаний. На рисунке 1 представлены наиболее трудоемкие операции в SIEMсистемах.Больше всего времени отнимают ложные срабатывания (58%) и разбор инцидентов (52%). Приэтом больше четверти респондентов отметили, что у них нет возможности выполнять эти действия: реагировать на инциденты не успевают29%, работать с ложными срабатываниями — 27%.

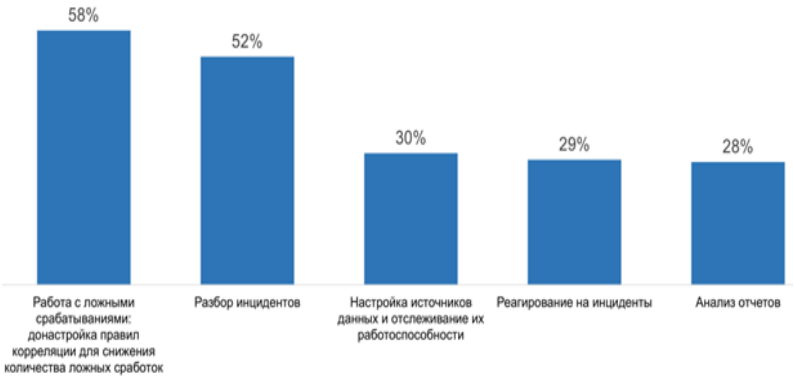


Рис. 1. Самые трудоемкие операции в SIEM
(поданнымкомпании Positive Technologies ptsecurity.com)

Исходя из поставленной цели, в работе решаются следующие **задачи**:

- исследование использования SIEM системы в корпоративной среде финансовой организации;
- тестирование выбранного инструментального средства SIEM;
- определения основных информационных потоков для SIEM систем;
- сбор от существующих в финансовой организации программно-аппаратных источников информации;
- интеграция с SIEM системой собранной информации от используемого программного обеспечения в финансовой организации;
- обработка полученной информации в SIEM системе;
- анализ обработанной информации в SIEM системе;
- формирование отчетной информации по требованиям регулятора в финансовой сфере, на основе полученной и обработанной информации от SIEM системы.

Определенны основные информационные потоки в финансовой организации для использования SIEM системы.

Произведено тестирование нескольких SIEM систем российского производства для сбора и дальнейшего агрегирования разрозненных потоков данных.

Предложен механизм внедрения, использования и интеграции SIEM системы в корпоративной среде финансовой организации.

Проведен анализ в SIEM системе полученной от корпоративных источников информации.

Получена возможность формирование необходимых отчетов на базе SIEM системы для своевременного предоставления регулятору в финансовой области.

Рассмотрена возможность прогнозирования угроз информационной безопасности на основе полученной информации от SIEM системы.

Практическую ценность работы составляет реализация интеграции SIEM системы с существующим программным обеспечением в финансовой организации для мониторинга информационной безопасности, позволяющая реализовать механизм своевременного распознавания угроз информационной безопасности и прогнозирования возможных угроз.

Новизна исследования заключается в предложенном механизме использования SIEM системы в корпоративной среде финансовой организации, отличающемся качественными средствами обнаружения от известных способов обнаружения вредоносных атак.

Предложен метод прогнозировании в выбранной для использования SIEM системы возможных угроз информационной безопасности на основе тщательного анализа и корреляции информации из различных источников полученной информации, позволяющий обеспечить сокращения времени своевременного обнаружения атак в корпоративной среде финансовой организации.

Выводы

Использование выбранной из предложенных SIEM системы позволит своевременно выявлять злонамеренную активность, попытки взлома инфраструктуры, присутствие злоумышленника, эффективно реагировать и принимать оперативные меры и по нейтрализации угроз, а так же выполнять требования регуляторов в финансовой сфере в области обеспечения защиты информации.SIEM-решения позволят привести информацию о событиях к единому формату с учетом известных угроз информационной безопасности, а так же выявлению новых неизвестных угрози прогнозировать будущие события на основе исторических данных.

Список литературы:

1. Актуальныекиберугрозы IV квартал 2019 года, 2019 – 34с.
2. Кибербезопасность 2019-2020: тенденции и прогнозы, 2019 – 23с.
3. Тестирование на проникновение в организациях финансово-кредитного сектора 2020 (исследование компании PositiveTechnologies), 2020 – 9с.
4. Трудозатраты специалистов по ИБ на работу с SIEM-системами (отчет компании PositiveTechnologies), 2020 – 14с.

УДК 004.056

Грачев Делявер Владимирович, Грачева Кристина Валерьевна
направление Информатика и вычислительная техника (магистратура),
гр.ИВТм-22

Научный руководитель
Мясников Владимир Иванович
д-р техн. наук., доцент кафедры информатики и вычислительной техники
ФГБОУ ВО «Поволжский государственный технологический университет», г.Йошкар-Ола

АНАЛИЗ СПОСОБОВ ОБНАРУЖЕНИЯ ДРОНОВПРИ ИХ ВТОРЖЕНИИ

Цель работы- нахождение наиболее эффективной системы обнаружения дронов, которая должна отличаться высоким коэффициентом распознаваемости объектов и быть работоспособной при любых погодных условиях.

В последнее время наблюдается увеличение количества используемых беспилотных летательных аппаратов (БПЛА).

Актуальность исследования и разработки систем обнаружения дронов в воздушном пространстве охраняемых объектов, создание программного модуля и алгоритмов его функционирования, обусловлена расширением сферы применения подобных устройств. Вместе с их ростом растут и риски, связанные с несанкционированной съемкой объектов частной собственности и контрабандой.

На сегодняшний день существует огромное количество комплексов обнаружения и нейтрализации БПЛА, функционирующих как на одном алгоритме обнаружения, так и сочетающих несколько методов. Одной из подобных систем обнаружения является разработанный комплекс детекции и идентификации БПЛА, эффективность работы которого объясняется применением комплекса различных датчиков.

Элемент комплекса - радиочастотная дрон-детекция не способна обеспечить хорошую эффективность, поскольку оснащена соответствующимидатчиками, сканирующими и анализирующими радиоканалы в диапазоне 2,4 и 5,8 ГГц, которые используются для управления дроном. В настоящий момент, современные модели дронов могут управляться не только по радио частотам, а таже существует возможность выстраивать маршрут полета дрона через GPS или другие навигационные системы.

Еще одним устройством обнаружения дронов могут стать акустические сенсоры, благодаря которым существует возможность отследить БПЛА по звуку их поршневых двигателей и шума пропеллеров. Основными источниками шума БПЛА являются поршневый двигатель ироторы, что обусловлено процессами горения, выпуска отработанных газов и механического перемещения деталей. Более низкие шумовые характеристики имеют электрические двигатели, но их использование в конструкции дронов способствует ограничению дальности полета. Данную информацию можно учитывать при обнаружении данного вида дрона, он будет информировать в каком примерном радиусе располагается нарушитель, управляющий дроном.

Актуальным является способом определения вида дрона по шуму, поскольку каждый дрон обладает уникальным шумовым параметром.[1] Таким образом, можно составить библиотеку, состоящую из звуков различных БПЛА и пропускать поступающий звук, записывающийся посредством чувствительных микрофонов, в режиме реального времени через интеллектуальную систему анализа, которая будет идентифицировать улавливаемые шумы с моделью дрона.

Акустические сенсоры позволяют наземным средствам поиска осуществить отслеживание дронов в пассивном режиме, снижая таким образом вероятность передачи данных противнику о своем месторасположении. Оценив преимущество таких систем отслеживания, следует периодически осуществлять модификацию акустическим систем поиска дронов по мере появления на рынке новых моделей БПЛА, по причине того, что новинки данной техники оснащены системой подавления шума по средствам добавления дополнительных винтов на корпусе БПЛА.Данная технология представляет собой установку микрофонов у основных винтов. Система шумоподавления обрабатывает данные с микрофонов и активирует вторичные винты, основываясь на уровне шума дрона. Вторичные винты вращаются таким образом, чтобы создавать «антишум».

Для более тщательного анализа акустических сигналов в комплексе обнаружения дронов эффективней использовать решетки микрофонов, поскольку использование отдельного микрофона лишит получения качественной оценки акустического сигнала. Ознакомившись с многочисленными статьями можно заметить, что антенные решетки эффективно справляются с обнаружением низко летающих БПЛА на тактических расстояниях.

После цифровой обработки, звуковые сигнатуры БПЛА передаются насервер, где осуществляется идентификация дрона посредством данных из базы всех беспилотников. При опознании объекта как дрона выполняется команда оповещение на мобильное устройство хозяина о несанкционированном проникновении дрона в пределы частной территории.

Существует также система оптического обнаружения, в ней основная видеокамера осуществляет съемку участка воздушного пространства в высоком разрешении. Необходимо учитывать погодные условия и изменения, которые могут произойти, для этого следует использовать камеру уровня защиты IP66 (защита видеокамеры от проникновения пыли и влаги).

В настоящий момент времени наиболее востребованной системой обнаружения БПЛА является система, оснащенная видеокамерами, которые получили усовершенствование как в технологической оснащенности, управляемости системы, так и в алгоритмах распознавания дронов. Данная система наиболее эффективна в сочетании с лидаром (лазерным радаром). [2] Но нужно отметить, что и в таком варианте обнаружения возникают свои сложности: существует огромное количество различных вариаций форм дронов, для точного определения которых необходимо производить множество доработок соответствующих систем. При снабжении системы видео обнаружения стоит учитывать возможность существования неблагоприятных погодных изменений. В данном случае потребуется инфракрасная камера, которая сможет определить размеры и форму дрона в условиях недостаточной видимости.

Еще одним из способов распознавания БПЛА является система на базе радиолокационной системы (РЛС) с технологией MIMO (метод пространственного кодирования сигнала), позволяющий увеличить полосу пропускания канала, в котором передача данных и их прием происходит благодаря системам из нескольких антенн.Существует методиспользования РЛС с многолучевыми приемными антеннами, особенностью которого является потенциальные характеристики при

обнаружении низкоскоростных малогабаритных летающих объектов. Многолучевая РЛС дает возможность обеспечить длительное когерентное накопление отраженного от цели сигнала при кратковременном обзоре широкой контролируемой системой зоны.[3]

Сложность обнаружения дронов радиолокационными системами усложняется тем, что в конструкции дрона небольшое количество металлических частей, многие производители двигателей используют керамику, в том числе оптимизируют формы и ракурсы рассеивания отраженного сигнала, применяя в своих разработках радиопоглощающие материалы.

Весомой причиной сложности распознания дрона является высокая вариативность возможных его форм, этот факт усложняется тем, что дроны могут маскироваться под птиц, самолеты и вертолеты. На первый взгляд, распознавание формы дрона, в отличие от человеческого лица проще, но сложность обусловлена накоплением огромного количества образцов. Для основных предметных областей - распознание лиц, голоса, текста создана огромная база данных, в том числе отработаны алгоритмы, дающие хорошие результаты на этой базе. Относительно дронов, придется соотносить к одному классу образцы самого разного вида, создавать множество классов, поскольку необходимо учесть все возможные формы дронов. Несмотря на то, что проблема решаема, стоит накопить колоссальные библиотеки изображений дронов разных форм с разных ракурсов, и задача усложняется из-за отсутствия качественных алгоритмов распознавания. В добавок изображение дрона, которое поступает в программу для идентификации, может оказаться размытым из-за скорости полета БПЛА.

Выводы

Рассмотрев основные моменты различных способов обнаружения дронов, можно прийти к итогу, что наиболее эффективным решением является комбинирование основных способов обнаружения: использование акустических сенсоров, оборудования радиомониторинга, инфракрасных (ИК) и оптических видеокамер. В том числе, стоит разработать сложный алгоритм для соотнесения дрона к определенному классу, что потребует больших вычислительных возможностей системы. Таким образом, уменьшается количество ошибок определения пролетающего объекта и увеличивается общая эффективность системы.

Список литературы:

1. «Беспилотникив России будут вычислять по звуку» [Электронный ресурс]. Режим доступа: https://www.popmech.ru/weapon/news-634403-bespilotniki-v-rossii-budut-vychislyat-po-zvuku/ (дата обращения 28.10.2020)
2. Фалилеев, В.Ю.,Анализ существующих автоматизированных комплексов защиты от дронов/ В.Ю. Фалилеев. Системный анализ, моделирование боевых действий и систем военного назначения, компьютерные технологии в военном деле. «Воздушно-космические силы.Теория и практика» - 2020. - №14- 131 с. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/analiz-suschestvuyuschih-avtomatizirovannyh-kompleksov-zaschity-ot-dronov (дата обращения: 28.10.2020)
3. Анпилогов В.Р., Шишлов А.В., Эйдус А.Г. Многолучевые антенные системы HTS // Технологии и средства связи. 2013, № 6-2 (99), с. 54 – 67

УДК 633/635

Григорьев Данил Германович
направление Информатика и Вычислительная техника (магистратура), гр. ИВТм-12

Научный руководитель
Малашкевич Василий Борисович,
к.т.н., доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА КОРПОРАТИВНОГО WEB-СЕРВИСА ОБСЛУЖИВАНИЯ СЛУЖЕБНЫХ ЗАПИСОК

Цель работы - разработка корпоративного Web-сайта для обслуживания служебных записок при направлении студентов на мероприятия» в среде разработки «VisualStudioCommunity 2019» с использованием технологии ASP.NET.[1]

В настоящее время трудно вообразить современный мир без информационных технологий, которые могли бы сильно упростить работу в самых разных сферах деятельности. Информационные системы сегодня становятся частью процессов, которые влияют на деятельность предприятий, ускоряют и оптимизируют эти бизнес-процессы.

В настоящий момент повышение степени автоматизации учреждения ведет к повышению стабильности технологического процесса, а также к уменьшению ошибок.[2]

Данная тема обладает актуальностью, которая обусловлена тем, что разработанный автоматизированный модуль согласования служебных

записок при направлении студентов на мероприятия, который будет находиться в корпоративном портале, позволит сократить время согласования СЗ, снизит риск ошибок при создании и уменьшит риск потери документов, т.к. данные хранятся в электронном виде и можно в любой момент сгенерировать документ.

Основной целью проектируемой системы является сокращение времени на согласование служебной записки, повышение эффективности рассматриваемого процесса, избежание ошибок и утеря документа. Для получения положительного результата от поставленной цели можно достичь путем разработки автоматизации модуля согласования служебной записки при направлении студентов на мероприятия через корпоративный портал ФГБОУ ВО «ПГТУ».

При разработке автоматизированного модуля согласования служебных записок при направлении студентов на мероприятия через корпоративный портал необходимо учесть все проблемы, выявленные на этапе анализа деятельности управления бухгалтерского учета, отчетности и финансового контроля и ликвидировать их.

Чтобы описать разрабатываемый модуль, стоит учесть следующие функции, которые будут автоматизированы при внедрении данного проекта:

Формирование служебной записки о направлении студентов на мероприятия;

Согласование служебной записки о направлении студентов на мероприятия;

Разберем бизнес-процесс [3] автоматизированного модуля согласования служебных записок при направлении студентов на мероприятия ФГБОУ ВО «ПГТУ», используя методологию функционального моделирования IDEF0 (модель «как надо»). [4]

Входящим потоком процесса согласования СЗ являются сведения об обучающихся, которые будут направлены на мероприятия. На выходе процесса представлена утвержденная СЗ и приказ о направлении студентов на мероприятие. Управляющее воздействие на представленный процесс будет оказывать Приказ ФГБОУ ВО «ПГТУ» от 14 апреля 2017г. N 122-П «Об утверждении положения о направлении студентов на мероприятия», а также положение или информационное письмо о проведении мероприятия. Ресурсами же будут служить направляющее подразделение, управление финансов и экономикой, управление бухгалтерского учета, отёчности и финансовый контроль, проректор по образовательной деятельности, и вдобавок разрабатываемый модуль согласования служебной записки.

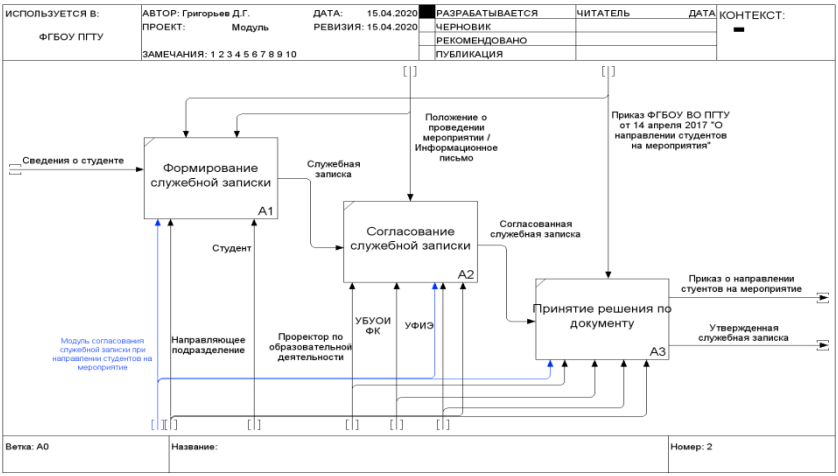


Рис. 1. Декомпозиция процесса согласования СЗ с учетом внедрения модуля согласования служебной записки при направлении студентов на мероприятие (модель как - надо)

В проектируемый модуль имеют доступ руководители направляющего подразделения (сотрудники ПГТУ).После того, как сотрудник авторизовался, ему присваивается уникальный идентификатор. Пользователь вносит данные о мероприятии, которое будет, данные о студентах, которые будут участвовать в этом мероприятии, смете расходов и источнике финансирования.

Пользователь, создавший служебную записку, отправляет данные лицам, которые согласуют СЗ. Согласующая сторона проверяет данные и после выносит свое решение. Если данная СЗ согласуется со всеми, то данная служебная записка считается согласованной.

После согласования СЗ со всеми лицами, согласившимися с документом, руководитель отправляющего подразделения формирует приказ отправлять студентов на мероприятие на основании утвержденной памятки.

Выводы

Разработанный автоматизированный модуль согласования служебных записок при направлении студентов на мероприятия через корпоративный портал ФГБОУ ВО «ПГТУ» содержит в себе следующие основные функции:

1) Создание служебной записки;
2) Согласование служебной записки;

3) Доработка документов, если требуется;

3) Формирование на основе служебной записки приказа о направлении студентов на мероприятия.

4) Печать готовых документов.

Данная разработка значительно улучшит бизнес-процесс по согласованию служебных записок за счет автоматизации

Спроектированный модуль может быть модернизирован, если понадобится.

Список литературы:

1. Хасенов Есиль Адикенович, СанкибаевАрманТемирханович Визуализация графических данных в приложении Asp. Net MVC // Проблемы науки. 2017. №4 (17).
2. Мирошниченко Марина Александровна, Останина Дарья Александровна Информационные технологии как средства обработки информации и автоматизации бизнес-процессов в крупных корпорациях // Научный журнал КубГАУ - ScientificJournalofKubSAU. 2016. №119.
3. Радченко Александр Васильевич Особенности бизнес-процессов на предприятии // Проблемы экономики и юридической практики. 2009. №3.
4. Чемисов С. Б. Применение методологии IDEF0 с целью моделирования бизнес-процессов на предприятии // ПСЭ. 2009. №4.

УДК 004.42

Данилов Роман Анатольевич
направление Информатика и вычислительная техника(магистратура),
гр.ИВТм-11

Научный руководитель
Васяева Наталья Семеновна,
канд. тех. наук, доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственных технологический университет», г. Йошкар-Ола

РАЗРАБОТКА СИСТЕМЫ ОБРАБОТКИ ИЗОБРАЖЕНИЙ НА RASPBERRYPI

Цель работы – разработать систему распознавания и анализа изображения шахматной доски для игры в шашки на базе одноплатного компьютера RaspberryPi.

Контроллер RaspberryPiобладает всеми атрибутами настоящего компьютера: выделенным процессором, памятью и графическим

драйвером для вывода через HDMI. На нем работает специальная версия операционной системы Linux. Поэтому на RaspberryPi легко установить большинство программ для Linux.Хотя в контроллере и отсутствует внутреннее хранилище данных, на нем можно использовать смарт-карты в качестве флэш-памяти, обслуживающей всю систему. Таким образом, можно быстро выгружать для отладки различные версии операционной системы или программных обновлений. Микрокомпьютеру для работы нужно постоянное напряжение 5V, более того, его работа завершается программным процессом — как и у обычного компьютера. RaspberryPi упрощает управление потоком операций в разных ситуациях: при подключении к Интернету для считывания или записи данных, воспроизведении какой-либо медиа-информации или подключении к внешнему дисплею.

Разработка программного обеспечения производится на языке Python 3 с использованием библиотекиOpenCV.Средидостоинств Python для написания программследует выделить такие, как:

- Простота для понимания и изучения. Если такие языки как C и Java используют в кодах много скобок и строк, то у Python строки кодов короче и понятны для прочтения.

- Наличие большого числа библиотек и готовых решений. Библиотеки Python- инструменты, решающие конкретные задачи: создание простых игр, работа с машинным обучением, работа с большими данными, базами данных.

- «Долговечность». Поскольку Pythonсчитается лучшим языком для работы с большими данными и машинного обучения, его «устаревание» не случится еще долго.

OpenCV — библиотека компьютерного зрения с лёгкими алгоритмами, которые могут использоваться в 3D-рендере, продвинутом редактировании изображений и видео, отслеживании и идентификации объектов и людей на видео, поиске идентичных изображений из набора и т.п.В неё входят более 2500 алгоритмов, в которых есть как классические, так и современные алгоритмы для компьютерного зрения и машинного обучения.

В разрабатываемом проекте действия на доске должен совершать робот-манипулятор. Принято допущение, что камера для получения изображения и RaspberryPi могут иметь как статичное расположение, так могут быть закреплены на «запястье» исполнительного механизмана некотором расстоянии и под углом относительно схвата, чтобы конструкция не загораживала игровое поле при получении изображения. Наиболее перспективнымвидится устройство в виде крана

мостового типа – на четырех ножках, со свободным перемещением «кисти» по плоскости. Разрабатываемая система в купе с роботом-манипулятором должна уметь определять расположение шашек на поле, «рубить» шашки соперника, проводить пешку в дамки, адекватно реагировать на действия оппонента.

Выводы

В результате данной работы будет разработана система, способная корректно оценить ситуацию на игровой доске и принять решение о наиболее эффективном перемещении шашки. Следует отметить, что подобный проект не потребует серьезных модификаций при использовании на определенных участках производственного процесса.

Список литературы:

1. Роберт Мартин. Чистая архитектура. Искусство разработки программного обеспечения.: Пер. с англ. – СПб.: Питер, 2018. – 352 с
2. Лутц М.Изучаем Python, 4-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2011. – 1280 с.
3. Характеристики одноплатного компьютера Raspberry Pi[Электронный ресурс]. – Режим доступа: https://myraspberry.ru/xarakteristiki-odnoplatnogo-kompyutera-raspberry-pi.html.
4. OpenCV[Электронныйресурс]. – Режимдоступа: https://opencv.org/.

УДК 004.42

Денисов Сергей Алексеевич
Направление «Информатика и вычислительная техника» (магистратура),
гр. ИВТМ-01-19

Научный руководитель
Галанина Наталия Андреевна,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения информационных систем
ФГБОУ ВО «Чувашский государственный университет им. И.Н. Ульянова», г. Чебоксары

АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО ЦИФРОВОЙ ПОДСТАНЦИИ

Цель работы – проектирование автоматизированных рабочих мест(АРМ) в системе цифровой подстанции [1].

Актуальность темыобусловлена высоким уровнем цифровизации современных подстанций, необходимостью удаленного управления, считывания и обработки больших массивов данных [4]. Возможность удаленного управлениядля каждого пользователя АРМ важна в виду современных реалий и перехода части персонала на дистанционную работу.

Ознакомление с АРМ. АРМ — специализированная ячейка в программной и аппаратной среде для автоматизации работы специалиста. Каждое такое автоматизированное место имеет строго заданный функционал в соответствии с назначением рабочего места.

Сама по себе концепция АРМ не нова, регламентируется ГОСТом 34.003-90 и имеет определенные правила и требования по эксплуатации.

Выбор средств разработки. Для разработки АРМ используются SCADA-системы, так как они обеспечивают работу в реальном времени, что базово необходимо в работе подстанций[7].

В комплекс SCADA-системы цифровой подстанции на нижнем уровне идет подключение дополнительного, зачастую стороннего,программного обеспечения от производителей датчиков, контроллеров, и прочего оборудования, необходимого для считывания данных с высокотехнологичных устройств[2].

Пользователи поделены на три группы согласно квалификации и АРМ, к которому принадлежит сотрудник:

– АРМ ОП – АРМ оперативного персонала;
– АРМ РЗА – АРМ инженера РЗА;
– АРМ АСУ – АРМ инженера АСУ[5].

Администратор комплекса, обладающий максимальным уровнем полномочий, назначает пользователю группу, соответствующую АРМ. При подключении к АРМ система проверяет уровень и соответствие допуска, и, если оба условия выполнены, рабочее место передается в управление оператору.

Для каждого АРМ существует перечень привилегий (рис.1) , права установки сигнала, просмотра схеми просмотра выполненных действий.

Заключение. Таким образом, задача проектирования АРМ для цифровых подстанций выполнена успешно. Реализованный функционал программы позволяет оператору АРМ выполнять весь перечень работ в соответствии с допуском и квалификацией.

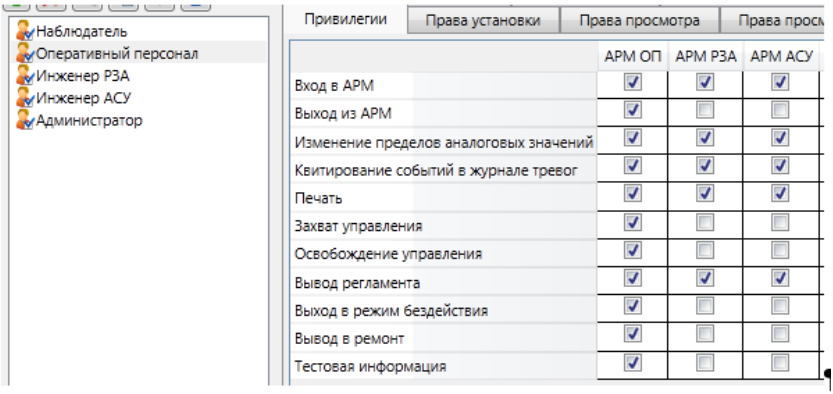


Рис.1. Привилегии пользователя с ролью «Оперативный персонал»

Список литературы:

1. Денисов С.А. Цифровая подстанция / С.А. Денисов, Н.А. Галанина // Информатика и вычислительная техника: сб. науч. трудов. - Чебоксары: Изд-во Чуваш.ун-та, 2019.- С. 71-74.

2. Охоткин Г.П. Методика структурного синтеза релейного регулятора тока транзисторного электропривода / Охоткин Г.П., Угарин С.В., Галанина Н.А.. - Электротехника.- 2017.- № 7. - С. 15-19.

3. Чичёв С.И. Методология проектирования цифровой подстанции в формате новых технологий / С.И. Чичёв, В.Ф. Калинин, Е.И. Глинкин.- М.: Издательскийдом «Спектр», 2014. - 228 с.

4. Moiseev D.V. Conducting an express analysis of emergency events of the electrical system based on calculations of the algorithm for determining the location of fault / D.V.Moiseev, N.A.. Galanina, N.N.Ivanova // Proceedings of the 2nd 2020 International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), 2020.- С. 9059206.

5. АСУ ТП [Электронный ресурс] // Wikipedia: сайт. – Режим доступа https://ru.wikipedia.org/wiki/Автоматизированная_система_управления_технологическим_процессом.

6. АСКУЭ [Электронный ресурс] //Wikipedia: сайт. – Режим доступа https://ru.wikipedia.org/wiki/Автоматизированнная_система_контроля_и_учета_энергоресурсов.

7. SCADA [Электронный ресурс] //Wikipedia: сайт. – Режим доступа: https://ru.wikipedia.org/wiki/SCADA..

УДК 004.42

Дмитриева Кристина Юрьевна
студент ФГБОУ ВО ПГТУ

Научный руководитель
Анисимов Павел Николаевич
доцент кафедры энергообеспечения предприятий
ФГБОУ ВО «Поволжский государственных технологический университет», г. Йошкар-Ола

ТЕХНИКО-ЭКОНОМИЧЕСКИЙ АНАЛИЗ ВАРИАНТОВ ЦЕНТРАЛИЗОВАННОГО И ИНДИВИДУАЛЬНОГО ПОКВАРТИРНОГО ТЕПЛОСНАБЖЕНИЯ ДЛЯ ГОРОДА ЙОШКАР-ОЛА

В статье авторы пытаются рассчитать технико-экономический анализ вариантов централизованного и индивидуального поквартирного теплоснабжения

В последнее время жители многоквартирных домов все чаще решают отказаться от централизованного отопления и перейти на индивидуальное отопление.

Централизованное теплоснабжение можно назвать сложной инженерной системой, занимающей значительную площадь. В системах централизованного теплоснабжения тепло вырабатывается за пределами отапливаемых зданий и затем передается по длинным разветвленным трубопроводам в целевые помещения. Такой вид отопления характерен для городов, особенно для многоэтажных домов и нежилых помещений.

Индивидуальное отопление-отопление квартиры за счет газового котла. Источник тепла устанавливается непосредственно у потребителя – жильца жилого дома, что позволяет значительно снизить потери тепла при его производстве и избежать их при транспортировке их от удаленного источника. В качестве теплогенератора в системе поквартирного теплоснабжения используется двухконтурный газовый котел с закрытой

топкой, принудительным удалением дымовых газов, забором воздуха для горения снаружи здания, регулирующими термостатами выработки и отпуска тепла на отопление и ГВС. Котел снабжен необходимыми блокировками и автоматикой безопасности.его размеры едва превышают размеры газовой колонки.

Значительная часть населения проживает в квартирах с центральным отоплением. А это, как правило, произвольное начало и окончание отопительного сезона, невозможность регулировать температуру в доме

–кратко говоря, отопление, которое часто приносит дискомфорт. Если раньше установка индивидуальной системы отопления в квартире казалась фантастикой, то сегодня это уже вполне осязаемая реальность. Владельцы собственного отопления не зависят от наличия воды в системе центрального отопления, ее температуры, возможных перебоев в теплоснабжении и прочих неприятностей. В их системах вода, которая первоначально поступала из центральной системы водоснабжения, циркулирует, не тратя ее впустую. Помимо удобства, как показывает практика, автономная система позволяет значительно снизить затраты на отопление. При этом межквартирное отопление может быть, как изначально планировалось при строительстве дома, так и использоваться вместо центрального отопления.

Преимущества централизованной системы отопления

• * возможность использования недорогих видов топлива;

• более низкая стоимость при покупке квартиры;

* отсутствие эксплуатационных расходов;

• безопасность.

Недостатки централизованной системы отопления:

• система работает по строгому сезонному графику;

* невозможность индивидуального контроля температуры нагревательных приборов;

* теплопотери при транспортировке и отоплении в многоквартирном доме;

• износ сетей приводит к частым авариям и перебоям в подаче электроэнергии.

Преимущества индивидуального внутриквартирного отопления:

* возможность контролировать температуру в квартире вплоть до полного отключения;

* при постоянном внимании к газовому оборудованию, соблюдении всех правил эксплуатации и точном учете можно добиться экономии средств;

* гарантия стабильного теплоснабжения.

Недостатки индивидуального квартирного отопления:

• более высокая покупная цена;

• высокие затраты на ремонт или замену газового оборудования;

• необходимость постоянного контроля исправности используемого газового оборудования;;

• необходимость самостоятельной организации ремонтно-эксплуатационных работ, связанных с эксплуатацией газового оборудования и дымохода;

* подъезды и подвалы не отапливаются, так как некоторые застройщики не оборудуют места общего пользования системами отопления;

• при отсутствии постоянных соседей их квартиры не отапливаются, а следовательно, увеличиваются теплопотери в вашей квартире;

* повышенный расход воды: требуется время, чтобы нагреть горячую воду в контуре, поэтому вы будете сливать часть объема, ожидая горячей воды из крана;

* повышенный риск несчастных случаев из-за неправильной эксплуатации оборудования (одним из жильцов).

Основной целью данной работы является оценка реальных затрат на теплоснабжение потребителей от реконструированных систем НТС и индивидуальных систем теплоснабжения на базе многоквартирных теплогенераторов. Предполагается рассматривать площади жилой застройки с различной преобладающей этажностью и разной численностью населения с учетом климатических различий (расчетной температуры теплосетей, продолжительности отопительного сезона и др.), а также тепловых свойств жилых зданий.

Показатели	Централизованная система отопления	Индивидуальное поквартирное отопление
Количество установленных котельных и индивидуальных котлов	0	300
Установленная мощность, МВт	15	7,15
Размер инвестиций в источники теплоты, тыс. руб.	52150	25180
Стоимость затрат на переоборудование поквартирного теплоснабжения, тыс. руб.	0	85
Количество потребителей тепла, ЖКХ	45	300

Показатели	Централизованная система отопления	Индивидуальное поквартирное отопление
Протяженность трубопроводов, м	30000	0
Размер инвестиций в модернизации тепловых сетей, тыс. руб.	0	0
Размер инвестиций в модернизации гаховых сетей, тыс. руб.	0	0
Суммарные инвестиции, тыс. руб.	52150	25180
Коэффициент энергетической эффективности	0,68	0,92
Годовое потребление тепловой энергии, МВт-ч/год	22480	3480
Годовой расход тепловой энергии, МВт-ч/год	33520	410
Эксплуатационные затраты, тыс. р./год	6700	875
Годовой расход газа, тыс. м3/год	3550,7	2520,5
Общекотельные и прочие затраты, тыс. р/год	2220	0
Итого затрат, тыс. р./ год	33189,5	2062,8
Себестоимость реализованного тепла, р./Гкал	1678	678,5

Список литературы:

1. В.В. Барановский, Т.Ю. Короткова Технико - экономическое обоснование создания тепловых электрических станций, 2018
2. Р.И. Эстеркин Котельные установки, 1989
3. file:///C:/Users/%D0%90%D0%BB%D0%B5%D0%BA%D1%81%D0%B0%D0%BD%D0%B4%D1%80/Downloads/PZE_2011_1_7.pdf
4. https://cyberleninka.ru/article/n/razvitie-perspektivy-i-sostoyanie-detsentralizovannyh-sistem-teplosnabzheniya-v-rf-1

УДК 004.056.57

Жаркова Мария Владиславовна
направление Информационная безопасность автоматизированных систем(специалитет), гр. БИ-41

Научный руководитель
Бородин Андрей Викторович
канд. экон. наук, зав. кафедрой информатики и системного программирования
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ТЕХНОЛОГИЙ РАЗРУШАЮЩИХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ

Цель работы– рассмотреть основные характеристики разрушающих программных воздействий (РПВ), сделать акценты на ихклассификационных признаках, и, наконец,исследовать тенденции развития соответствующих технологий.

Начнем с общего понятия РПВ. Разрушающие программные воздействия – программные средства деструктивного характера, которые носят разрушительный, вредоносный характер, а последствия активизации и применения которых могут привести к значительному или даже непоправимому ущербу[4].

Заметим, информационные технологии постоянно совершенствуются, и, таким образом, конечный пользователь все больше отстраняется от процессов, происходящих в "глубинах" компьютера. Понятно, что программы становятся все более сложными, увеличивается их размер, а вместе с этим увеличивается количество алгоритмических ошибок, ошибок реализации, и, как следствие, возникает все больше возможностей присутствия недокументированных возможностей, заложенных изначально, или внедренных в процессе эксплуатации.

Все это создает благоприятные условия для развития и распространения РПВ и, соответственно,для роста причиняемого ими вреда. Таким образом, можно говорить о значительной **актуальности** поднятой проблемы и, соответственно, данного исследования.

В основном различают следующие виды РПВ[3]:

Компьютерные вирусы.Особенностью является направленность на самодублирование и деструктивные функции. Задача сокрытия своего присутствия реализуется либо в течение латентного периода существования, либо не ставится вообще.

Вирусы можно разделить на классы по ряду признаков. По среде обитания:*сетевые* вирусы распространяются по компьютерной сети.*Файловые* внедряются в выполняемые файлы.З*агрузочные* –в загрузочный сектор диска или сектор, содержащий системный загрузчик винчестера.*Специальные*– ориентированы на конкретные особенности программного обеспечения, например,макровирусы, заражающие документы MicrosoftOffice.

По способу заражения среды обитания:*резидентный* вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения к операционной системе в части доступа к объектам заражения и тем самым скрывает факты внедрения в них;*нерезидентные* вирусы не заражают память компьютера и являются активными ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус.

По деструктивным возможностям:безвредные, неопасные, опасные вирусы, очень опасные вирусы.

«Черви».Основной функцией является самодублирование путем распространения в сетях, используя уязвимости прикладных систем и сетевых сервисов.Копии передаются на удаленный компьютер, исполняются и распространяются по доступным файловым системам.В отличие от вируса, червь никак не задевает файлы, существующие, в системе. Он просто размножается, копируя самого себя и заполняя свободное место на диске.

«Троянские программы».Данный класс РПВ часто относят к вирусам, однако это не всегда верно, основной функцией РПВ данного класса, заключается в краже информации, например, номеров кредитных карт, либо в имитации сбоя ЭВМ, чтобы под видом ремонта злоумышленник мог получить к ней доступ. Основная особенность – ассоциирование (выдача себя за часто используемое ПО или сервисы).

Виды троянских программ разделяются в зависимости от типа действий, выполняемых в компьютерной системе:

- *Trojan-Downloader*:загрузчик, который устанавливает на персональный компьютер(ПК) жертвы новые версии опасных утилит, включая рекламные модули.
- *Trojan-Dropper*:деактиватор программ безопасности. Используется хакерами для блокировки обнаружения вирусов.
- *Trojan-Ransom*:атака на ПК для нарушения работоспособности. Пользователь не может осуществлять работу на удаленном доступе без оплаты злоумышленнику требуемой денежной суммы;

- *Эксплойт*:содержит код, способный воспользоваться уязвимостью ПО на удаленном или локальном компьютере;

- *Бэкдор*:предоставляет мошенникам удаленно управлять зараженной компьютерной системой, включая закачивание, открытие, отправку, изменение файлов, распространение неверной информации, регистрацию нажатий клавиш, перезагрузку. Используется для ПК, планшета, смартфона;

- *Рутким*:предназначен для сокрытия нужных действий или объектов в системе. Основная цель – увеличить время несанкционированной работы.

Программные закладки.Для того чтобы закладка смогла выполнить какие-либо функции по отношению к другой прикладной программе, она должна получить управление, то есть процессор должен начать выполнять инструкции, относящиеся к коду закладки. Можно рассматривать три основные группы деструктивных функций, которые могут выполняться закладками: сохранение фрагментов информации, возникающей при работе пользователей; изменение алгоритмов функционирования прикладных программ;навязывание некоторого режима работы, либо замена записываемой информации информацией, навязанной закладкой.

Если на заре создания РПВ, вообще, и компьютерных вирусов, в частности, главной целью разработчиков было своего рода самоутверждение, то современный этап развития этого вида программного обеспечения характеризуется, с одной стороны, глубокой теневой коммерциализацией, а с другой стороны, постепенной миграцией в сферу систем вооружений. Первый фактор включает в себя средства атак на розничную банковскую сеть, на предприятия малого и среднего бизнеса, активно использующие электронные платежные системы, и, в какой-то степени, на крупный бизнес, наиболее уязвимый с точки зрения утечек в системах электронного документооборота. Второй фактор – это, по-видимому, будущее РПВ.

Реализация первого фактора развития РПВ предполагает, во многом обеспечение максимальной скрытности жизненного цикла РПВ, в том числе и с точки зрения средств эвристического анализа программного обеспечения, а также инструментов, использующих для анализа кодов методы искусственного интеллекта. При этом для противодействия средствам обнаружения РПВ, последние могут использовать методы интеграции вредоносного кода в удаленные от корня участки графа потока управления программ-мишеней [2].

С точки зрения эволюции РПВ, как систем вооружений (второй фактор), на первый план выходит задача сокрытия функциональности целевой компоненты РПВ. Атакуемая сторона не должна, не при каких обстоятельствах, узнать назначение вредоносных программ и программных компонент вплоть до реализации атаки. В этой связи главенствующую роль начинают приобретать технологии стойкой обфускации кода при заданных ограничениях применения [1]. При этом основой, автоматизированной обфускациикода, могут стать технологии эквивалентных преобразований программ, управляемых псевдослучайными процессами [5], как с секретом, так и без.

Реализацию обоих указанных факторов эволюции РПВ можно считать основными современными тенденциями развития технологий вредоносного программного обеспечения.

Выводы. Появление новых компьютерных технологий дают в руки нарушителей и создателей различного рода вредоносных программ всё новые и новые возможности.Чтобы выявить и предотвратить будущие потенциальные угрозы, специалисты по информационной безопасности должны быть осведомлены о текущих тенденциях развития вредоносных программ, и работать над созданием средств для их обезвреживания.

Список литературы:

1. Бородин, А. В. Вариант постановки задачи противодействия реверс-инжинирингу кода в рамках императивной парадигмы программирования / А. В. Бородин // Инженерные кадры – будущее инновационной экономики России. – 2019. – № 4. – С. 8-12.

2. Бородин, А. В. О задаче классификации на окрестности корня графа потока управления программы в контексте процесса размножения файловых компьютерных вирусов / А. В. Бородин, М. А. Юдина, М. А. Васильева // Современные наукоемкие технологии. – 2019. – № 1. – С. 31-35.

3. Бородин, А. В. Феномен компьютерных вирусов: элементы теории и экономика существования / А. В. Бородин. – Йошкар-Ола: Марийский государственный технический университет, 2004. – 144 с.

4. Вавренюк,А.Б. Разрушающие программные воздействия/ А.Б. Вавренюк, Н.П. Васильев,под ред. М.А. Иванова. –М.: НИЯУ МИФИ, 2011. – 328 с.

5. Львович, И. Я. Перспективные тренды развития науки: техника и технологии. Т. 1 / И. Я. Львович, В. А. Некрасов, А. П. Преображенский и др. – Одесса: КУПРИЕНКО СВ, 2016. – 197 с.

УДК 004.056.53

Жаркова Мария Владиславовна
специальность Информационная безопасность автоматизированных систем,
гр. БИ-41

Научный руководитель **Ч**
екулаева Елена Николаевна
к-т экон. наук, доцент кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г.Йошкар-Ола

ОСНОВНАЯ ХАРАКТЕРИСТИКА ЗАЩИТЫ КРИПТОВАЛЮТЫ В СОВРЕМЕННОМ МИРЕ

Цель работы - рассмотреть основную характеристику криптовалюты, выделить отличия её от других цифровых монет в электронном пространстве, и изучить популярные способы защиты цифровых монет.

Впервые термин «Криптовалюта», а точнее оригинальная англоязычная формулировка «CryptoCurrency» появилась в 2011 году в одной из статей в журнале Forbes. С того момента это слово начало все чаще встречаться в новостях, в газетах и просто в разговорах людей.

Криптовалюта – это разновидность платежного средства в электронном виде. Реализована она в виде математического кода, а название свое она получила по принципу действия: все транзакции проводятся с помощью криптографических элементов и электронной подписи.

Единица измерения в системе криптовалют – coin, что в переводе означает «монета». Какого-либо реального выражения наподобие ценных бумаг или золота у этой валюты нет, то есть все активы существуют только в цифровом виде.

Одним из ключевых отличий цифровых монет от реальных денежных средств является способ их попадания в цифровое пространство. Реальные деньги для перевода нужно загружать на счет или вносить на электронный кошелек, а коины сразу появляются в электронном формате без какого-либо реального обеспечения.

Все только и говорят о том, как заработать на криптовалюте. Но не многие задумываются о самом важном, а именно о том, как не потерять заработанный капитал. Безопасность криптовалюты — очень важный вопрос, к сожалению, многие думают о ней в последнюю очередь.

Стоит подумать о сохранности своих сбережений заранее и не допускать ошибок, из-за которых вы можете потерять свои деньги.

Рассмотрим поподробнее особенности крптовалюты:

- Криптовалюта - это цифровая платежная система, которая не использует банки для проверки транзакций.

- Это одноранговая система, которая позволяет любому человеку в любом месте отправлять и получать платежи.

- Платежи с использованием криптовалюты существуют исключительно в виде цифровых записей в онлайн-базе данных, которые описывают конкретные транзакции.

- При переводе средств в криптовалютах транзакции записываются в открытые регистры.

- Хранится криптовалюта в цифровых кошельках пользователей.

Криптовалюта получила свое название, потому что для проверки транзакций с ее использованием применяется шифрование. Это означает, что для хранения и передачи данных о криптовалюте между кошельками и в открытые регистры используется расширенное кодирование. Целью шифрования является обеспечение безопасности.

Криптовалюты обычно создаются с использованием технологии блокчейн (blockchain). Блокчейн описывает способ записи транзакций в «блоки» и отметки времени. Это довольно сложный технический процесс, но в результате получается цифровой регистр криптовалютных транзакций, который хакерам сложно взломать.

Кроме того, транзакции требуют двухфакторной аутентификации. Например, пользователя могут попросить ввести имя и пароль в начале транзакции. Затем, может потребоваться введение кода аутентификации, который отправляется в виде смс на личный мобильный телефон.

Использование цифрового кошелька является самым популярным способом хранения цифровых монет. Такие кошельки очень просты в использовании и довольно удобны. В случае если криптовалюта хранится на персональном компьютере, то уровень безопасности напрямую зависит от технических характеристик данного устройства.

В целом защита виртуального кошелька на ПК похожа на защиту любой конфиденциальной информации. Нужно быть предельно осторожным при использовании Интернета и хранить пароли в зашифрованных файлах на внешних устройствах. В идеале, пароли должны храниться только в памяти владельца. Рекомендуется устанавливать кошельки на ПК, которые не используются для интернет-серфинга на ежедневной основе.

Одно из популярных решений проблемы защиты криптовалют основано на использовании Linux, который считается практически непробиваемым для вирусов и хакерских атак.

Также стоит упомянуть о холодном кошельке, позволяющем повысить безопасность на несколько уровней. В целом это предполагает размещение криптовалюты на оффлайн-кошельке, что ограничивает любые попытки несанкционированного доступа. Холодный кошелек — это физическое устройство, которое безопасно генерирует закрытые ключи для криптовалют.

В большинстве случаев холодный кошелек создается на устройстве, которое никогда не было подключено к Интернету, например, на старом ноутбуке. Но мало кто знает, что такое хранилище может быть создано за пределами Интернета. Этот аспект также имеет большое значение. Пользователю не нужно подключать Интернет, устанавливать "кошелек", и генерировать ключи.

Из всего обилия онлайн кошельков, аппаратные кошельки являются наиболее удобными и имеют самый высокий уровень безопасности. Это портативные устройства, специально предназначенные для хранения криптовалют. Такой кошелек является флэш-накопителем с безопасным и простым программным обеспечением и многоуровневой защитой криптографии.

Холодный кошелек незаменим для безопасного хранения активов в виде виртуальной валюты. Но в тот момент, когда вам понадобится перевести свои деньги через Интернет, вы обязательно наткнетесь на другие проблемы безопасности, успешное решение которых повлияет на безопасность онлайн-денег.

Активно развивающаяся торговля криптовалютами ставит перед пользователями новую задачу поиска безопасного способа хранения активов, т.е. постоянное наличие онлайн-доступа к кошельку. Некоторые нишевые участники создают «горячий кошелек», с помощью которого они проводят ежедневные операции, и еще один холодный кошелек, где они держат свои основные активы. Такой подход был успешно реализован на большинстве фондовых бирж. Связь с фондовыми биржами и услугами обмена валюты является неотъемлемой частью всех участников домена даже для тех, кто не считает себя криптотрейдерами.

Криптотрейдер - это специалист в области криптотрейдинга действующий по собственной инициативе, который осуществляет торговлю цифровыми активами при помощи криптовалютных бирж, с целью получения прибыли из процесса торговли. Задачей

криптотрейдера является анализ текущей ситуации на рынке криптовалют, чтобы выгодно заключать торговые сделки.

Криптотрейдинг - это способ доступа к торговле цифровыми активами на криптобиржах, с целью извлечения прибыли.

Все онлайн-кошельки, фондовые биржи и системы обработки данных должны соответствовать конкретным требованиям безопасности. При выборе онлайн-ресурса для проведения транзакций, каждый пользователь должен самостоятельно принять меры предосторожности при работе с криптовалютой.

Во-первых, пользователь должен внимательно следить за безопасностью своей электронной почты, так как, более 90% хакерских атак осуществляется через доступ к ней. Смартфон на системе Android, с установленным идентификатором Google представляет с собой опасность для онлайн-кошелька его владельца. Поэтому, рекомендуется использовать простой телефон, который будет использоваться исключительно для финансовой деятельности. Кто-то может рассматривать такие рекомендации как просто банальность, но как показывает практика, это позволяет увеличить уровень безопасности активов.

Удобство, безопасность и надежность биржи является ключевым аспектом в случае постоянной торговли на ней или простого хранения существующих там активов. Фондовые биржи, большая часть которых представляет централизованные услуги, часто подвержены хакерским атакам. К сожалению, такие случаи встречаются всё чаще. Общая оценка ресурсов, прямо или косвенно связанных с криптовалютным рынком, позволила определить некоторые случаи биржевой ненадежности, хотя не всем удается заметить их с первого взгляда.

Список литературы:

1. Д. Приходько «Криптовалюта. Учебное пособие по работе с цифровыми активами»,2020.- 340 с.
2. https://bcm-center.com/useful-articles/cryptocurrency-protection
3. https://sozd.duma.gov.ru/bill/419059-7#bh_histras
4. И. Башир «Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты».2020. – 540с.
5. https://xakep.ru/2016/01/18/cryptsy-face-bankruptcy/

УДК 004.056

Иванов Григорий Вячеславович
направление «Информатика ивычислительная техника» (магистратура),
гр. ИВТМ-01-19

Научный руководитель
Галанина Наталия Андреевна,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения информационных систем
ФГБОУ ВО «Чувашский государственный университет им. И. Н. Ульянова», г. Чебоксары

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ НА ОСНОВЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

Цель работы. Описаниеосновных этапов при создании мобильного приложения на основе искусственной нейросети.

Актуальность работы.Развитие искусственных нейросетей на текущий момент набирает стремительные обороты. Программные продукты на их основе помогают специалистам в решении сложных задач.Примерами таких продуктов являются мобильные приложенияShazam, Prisma, SwiftKey и др.

Основная часть.Мобильное приложение – это программма, которая разрабатывается под определённую платформу смартфонов (iOS, Android, Windows Phone и т. д.). Для разработки была выбрана операционная система Android[1].

Искусственная нейронная сеть – математическая модель, которая является упрощенной формой биологической нейронной сети, состоящая из нейронов и связей между ними. Основными типами архитектур искусственных нейронных сетей являются: свёрточные и рекуррентные исскуственные нейросети [2].

Основные этапы создания мобильного приложения на основе искусственной нейросети. Первый этап – разработка концепциимобильного приложения[4-5].На этом этапе необходимо коротко описать основные функции приложения, которые оно будет выполнять.

Второй этап - проектирование и дизайн.Необходимо создать прототипы будущего мобильного приложения и определить навигацию между ними. Далее необходимо определить цвет иразмер компонентов, то есть создать визуальный шаблон мобильного приложения.

Третий этап - процесс разработки. На этом этапе решаются следующие задачи:

- разработка клиентской части: вёрстка прототипов и анимации, настройка логики и переходов, подключение функционала и API (программный интерфейс приложения);

- разработка искусственной нейросети (ИНС): сбор данных, анализ и обработка данных, создание архитектуры ИНС, обучение ИНС [3];

- разработка серверной части: формирование архитектуры клиент-серверного взаимодействия, создание базы данных, проектирование структуры взаимодействия между сущностями, внедрение ИНС, разработка серверных скриптов с применением REST-архитектуры.

Четвертый этап - тестирование.

Тестирование включает в себя ручное тестирование и проверку на наличие программных ошибок. К процессу тестирования необходимо отнестись очень серьезно, ведь от него зависит качество мобильного приложения.

Выводы. В целом, процесс создания мобильного приложения на основе искусственных нейронных сетей является достаточно сложной, но интересной задачей, для решения которой требуются профессиональные навыки в области информационных технологий.

Список литературы:

1. Мобильное приложение [Электронный ресурс]. -Режим доступа : https://ru.wikipedia.org/wiki/Мобильное приложение.

2. Нейроннаясеть [Электронный ресурс]. - Режим доступа : https://ru.wikipedia.org/wiki/Нейронная_сеть.

3. Запуск нейросети на Android [Видеозапись]/ Наталья Кухарчик. - Режим доступа : https://www.youtube.com/watch?v=BYpiet2swrI&t=184s.

4. Этапы разработки мобильных приложений [Электронный ресурс] / ООО “АППсСтудио”. - Режим доступа : https://appsstudio.ru/etapy-razrabotki-mobilnogo-prilozheniya.

5. Разработка мобильных приложений: с чего начать[Электронный ресурс] / Mail.ruGroup. -Режим доступа : https://habr.com/ru/company/mailru/blog/179113/.

УДК 681.5

Иванов Артем Владимирович, Иванов Роман Андреевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-21

Научный руководитель
Мясников Владимир Иванович
к.т.н., доцент кафедры информационно вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ОСОБЕННОСТИ ВИЗУАЛИЗАЦИИ В CODESYS 2.3

Цель работы – анализ ошибок, возникающих при построении визуализации с элементом *Таблица* в CodeSys 2.3, пути преодоления данных трудностей.

В настоящее время программируемые логические контроллеры (ПЛК) повсеместно внедряются в промышленность, особенно широко используются в задачах автоматизации производства и автоматического управления техническими объектами.

Обеспечение надежного, удобного и понятного человеко-машинного интерфейса – одна из главных задач проектирования автоматической системы управления производством. Визуализация отображения информации об объекте в текстовом или графическом виде позволят пользователю осуществлять управление им. Часто применяются обновляющиеся графики (тренды), таблицы и т.д.

Для разработки таких приложений применяются специальные среды разработки. Одной из популярных сред является среда программирования «CodeSys». Данная среда является свободно распространяемой. В качестве ПЛК в нашей стране широко используются изделия российской фирмы «ОВЕН».

Рассмотрим особенности построения визуализации для ПЛК110[M02] фирмы «ОВЕН». Для программирования ПЛК в среде CodeSys необходима специальная программа, так называемый target-файл – профиль целевой платформы. Для ПЛК110[M02] фирмой разработантarget-файл под среду CodeSys 2.3. Это не последняя версия среды, однако, под среду CodeSys 3.5 target-файла для ПЛК110[M02] нет.

Рассмотрим создание в качестве визуализации *Таблицу*, в которую периодически или по определенному событию выводится следующая информация:

- время совершения события;
- данные режимов работы узлов, путем отображения перечисляемых типов.

В качестве языка программирования будем использовать язык ST, широко применяемый при программировании ПЛК в среде CodeSys.

Задача: вывести на экран таблицу. В таблице выводятся моменты свершения некоторых событий: время свершения (тип DT – дата и время), аварийные ситуации (перечисляемый тип), смена режима работы (перечисляемый тип) и включение/выключение агрегата (перечисляемый тип).

Для работы с таблицами объявим для каждой таблицы структуру – пользовательский тип данных, который содержит набор переменных разных типов.

```
TYPE strucTab :
STRUCT
    Out_agreg : enum_out ;
    regime_agreg :  enum_tabl2_regim ;
    avar_agreg :enum_avar ;
    T_Time : DT;
END_STRUCT
END_TYPE
```

На рис.1 представлена таблица, соответствующая объявлению.

Как видно из рисунка, особенность визуализации таблицы – заполнение всех строк начальными значениями переменных (для времени начало отсчета с 1970 г., если не изменено текущее время). Данное представление оказывается не наглядным, одним из способов исправления ситуации – вывод переменных после преобразования их в тип STRING, который имеет начальное значение ' '.

Объявив структуру:

```
TYPE strucTab :
STRUCT
    Out_agreg : STRING ;
    regime_agreg :  STRING;
    avar_agreg : STRING;
    T_Time :STRING;
END_STRUCT
```

и выполнив преобразования переменных в строковый тип, должны получить начальный вид таблицы без лишних символов.

	Time	Regime	Agregats	Avar
1	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
2	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
3	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
4	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
5	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
6	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
7	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
8	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
9	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
10	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
11	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
12	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
13	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
14	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
15	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
16	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
17	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
18	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
19	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar
20	DT#1970-01-01-00:00	No_Regim	no_agreg	no_avar

Рис.1. Инициализация таблицы

Откомпилируем программу и запустим ее в режиме эмуляции. Даже до старта программы, сразу при ее подключении на экране всплывает надпись (рис. 2).

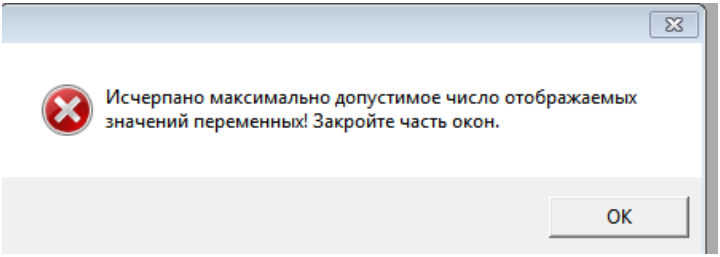


Рис.2. Предупреждение после подключения

Как оказалось, CodeSys 2.3 не может выводить в визуализацию несколько переменных строкового типа. В версии CodeSys 3.5 это устранено.

Попытаемся как-то выйти из этой ситуации. После ряда экспериментов пришли к выводу, что одна переменная типа STRING может быть помещена в таблицу. Если объявить время строковой переменной, то по моментам появления временных отсчетов можно

будет ориентироваться в значениях других переменных. Что касается перечисляемых типов данных, то пришлось ввести начальное значение в виде подчеркивания, двойного подчеркивания и т.д. Небольшая сложность – нельзя использовать одно и то же начальное значение в разных переменных. На рис. 3 приведен пример таблицы при использовании предложенного приема.

	Time	Regime	Agregats	Avar
1	2017-04-03-00:00:00	Stop_	__	___
2	2017-04-03-00:00:00	Stop_stop_	__	___
3	2017-04-03-00:00:00	_	__	No_calibr_
4		_	__	___
5		_	__	___
6		_	__	___
7		_	__	___
8		_	__	___
9		_	__	___
10		_	__	___
11		_	__	___
12		_	__	___

Рис.3. Пример вывода таблицы

Выводы

Приведенные приемы программирования позволяют сделать визуализацию проекта более наглядной для CodeSys 2.3.

Список литературы:

1. Визуализация CodeSys/. Дополнение к руководству пользователя по программированию ПЛКв CodeSys 2.3. 3S – Smart Software SolutionsGmbH Memminger Strabe 151 - 2008.

2. Минаев, И. Г. Программируемые логические контроллеры: практическое руководство для начинающего инженера / И. Г. Минаев, В. В. Самойленко. – Ставрополь: АРГУС, 2009. – 100 с.

УДК 004.42

Карташев Роман Александрович, Сидуков Дмитрий Александрович
направление Информатика и вычислительная техника (бакалавриат),
гр. ИВТ-21

Научный руководитель
Васяева Елена Семёновна,
канд. техн. наук, доцент кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА АЛГОРИТМА ОБЪЕЗДА ПРЕПЯТСВИЙ

Цель работы – разработка алгоритма объезда препятствий колёсным роботом.

Применение мобильных роботов с каждым годом становится всё шире и шире. Они постепенно входят в наш мир, появляясь в разных областях повседневной жизни: военная отрасль, медицинское дело, космические исследования, даже повседневный быт. Так, машины с алгоритмом распознавания препятствий используются для проведения работ в неизвестной местности: путём анализа окружающей среды робот получает информацию о том, в каком направлении ему двигаться. Подобное применение такая технология находит в военной технике. С помощью специального сенсора (например, ультразвукового дальномера) определяется расстояние до препятствий и выстраивается маршрут. Основная цель данной области – определение препятствий и создание автономной системы с использованием пар датчиков/сенсоров и измерение их эффективности.

В задачах ориентации в замкнутом пространстве используют следующие алгоритмы:

- алгоритм Дейкстры – алгоритм нахождения кратчайшего пути от одной вершины графа до всех остальных;
- очередь с приоритетом – алгоритм, основанный на алгоритме Дейкстры. Наиболее подходит для работы с небольшим количеством входных данных (таким, как положение в пространстве);
- A* алгоритм - алгоритм поиска по первому наилучшему совпадению на графе, который находит маршрут с наименьшей стоимостью от одной вершины к другой. Порядок обхода вершин определяется эвристической функцией «расстояние + стоимость».

В данной работе алгоритм управления роботом (рис. 1) основан на анализе размеров препятствия, что позволит сократить время

прохождения роботом маршрута. Для этого робот должен быть оснащён либо 3-мя дальномерами, расположенными спереди и по бокам робота, либо широкоугольной лидарной системой. Для уменьшения вероятности невозврата роботом на линию после объезда препятствия необходимо сохранять информацию об удалении от линии следования при объезде.

Движение робота осуществляется с помощью подачи ШИМ-сигнала на двигатели, при движении вперед/назад подается одинаковый уровень сигнала, при повороте подается разное значения, одно колесо начинает вращается медленнее другого в соответствии с ПИД-регулятором.

Определение расстояния до препятствия производится на основе значений центрального дальномера. Алгоритм объезда препятствия основан на алгоритме Дейкстры (рис. 2).

В коде программы функции и процедуры разделены на отдельные файлы по признаку принадлежности к аппаратным ресурсам. Для увеличения скорости выполнения программы код написан на основе методов процедурного программирования.

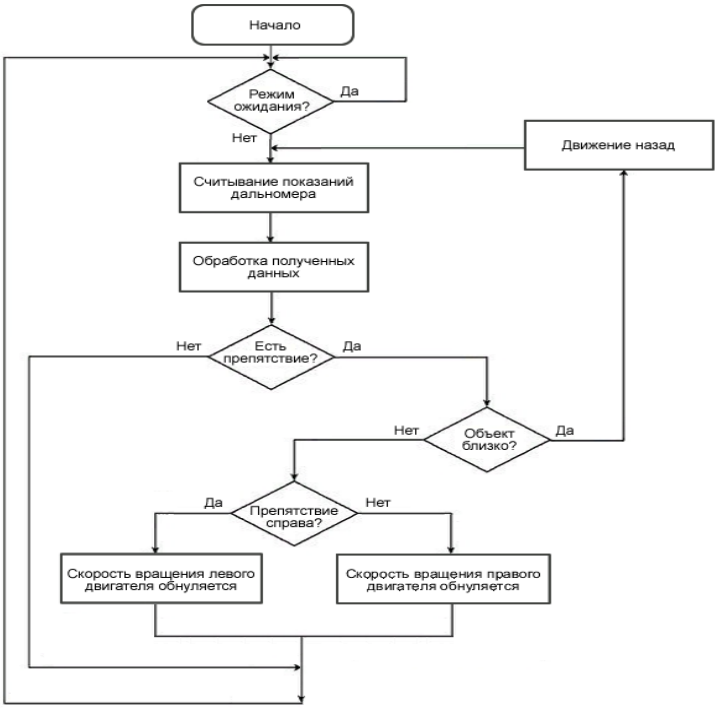


Рис. 1. Алгоритм объезда препятствия

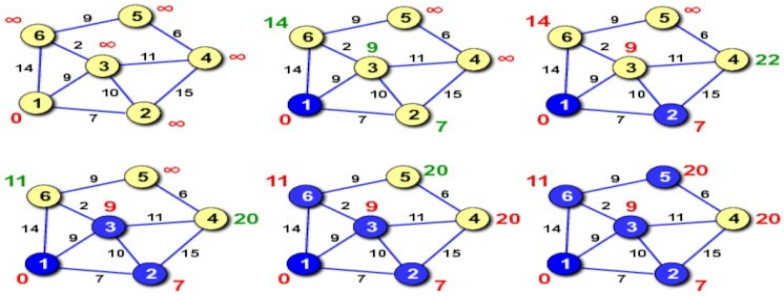


Рис. 2. Алгоритм Дейкстры

Список литературы:

1. Бачинин, Н. В. Основы программирования микроконтроллеров: учебник / Н. В. Бачинин, В. Л. Панкратов, В. И. Накоряков. – М.: Форум: Инфра-М, 2010. – 512 с.
2. Конехи, Дж. Реализация методов ориентирования для продвинутых автономных роботов. [Электронный ресурс]/ Дж. Конехи, М. Прозек - WCECS 2013, 23-25 October, 2013. Режим доступа: http://www.iaeng.org/publication/WCECS2013/WCECS2013_pp378-82.pdf.
3. Инженерные алгоритмы построения маршрутов. [Электронный ресурс]/Д. Деллинг, П. Сандерс, Д. Скульт, Д. Вагнер - : Algorithmics, LNCS 5515, pp. 117–139, 2009. Режим доступа: https://i11www.iti.kit.edu/extra/publications/dssw-erpa-09.pdf.

УДК 004.891.2

Кладовикова Елена Андреевна
направление Прикладная информатика
(магистратура), гр. ПИм-21

Научный руководитель
Уразаева Татьяна Альфредовна,
канд. техн. наук, доцент кафедры информационных систем в экономике
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Олы

МОДЕРНИЗАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ НАЛОГОВЫХ ОРГАНОВ РОССИЙСКОЙ ФЕДЕРАЦИИ.

Аннотация: В статье приведен анализ автоматизированной информационной системы «Налог», которая применяется налоговыми

органами для решения задач, связанных с функциями и полномочиями Федеральной налоговой службы России. Автоматизация процессов, осуществляемых налоговыми органами, направлена на: повышение эффективности функционирования налоговой системы за счет: быстродействия и принятия более качественных решений; оперативность работы налоговых инспекторов и рост производительности их труда; обеспечение налоговых служб всех уровней полной и актуальной информацией о всех изменениях, происходящих в налоговом законодательстве; предоставление достоверных данных об эффективности системы контроля за соблюдением норм налогового законодательства. В статье предложены направления и принципы модернизации автоматизированной информационной системы «Налог», рас- крыты основные направления построения новой автоматизированной системы и предложены параметры контроля уровня достижения целей в результате модернизации существующей.

Ключевые слова: Цифровая экономика, информационные технологии, государственное управление, Федеральная налоговая служба, налоговое администрирование, модернизация налоговой системы.

На всех этапах развития государства от налоговой системы требуется решение проблем обеспечения своевременного поступления налоговых доходов в бюджеты на федеральном, региональном и муниципальном уровнях, сбалансированности бюджетов по доходам и расходам, сокращения дефицита, внешнего и внутреннего долга. При этом повышение эффективности и уровня собираемости налоговых платежей и обеспечение налоговых поступлений во все бюджеты бюджетной системы Российской Федерации является одной из приоритетных задач для налоговых органов. В свою очередь, с развитием и внедрением информационных и цифровых технологий во все сферы жизнедеятельности, возникла необходимость автоматизации деятельности и органов государственного и муниципального управления, в том числе, налоговых органов.

Применение информационных технологий, включая создание автоматизированных систем и баз данных для эффективного функционирования налоговых органов, является одной из приоритетных задач ФНС России.

АИС «Налог» – автоматизированная информационная система, призванная облегчить работу налоговых органов и повысить ее

эффективность в части осуществления учетно-аналитических функций, а также вопросов взаимоотношения налоговых органов и налогоплательщиков.

Основными направлениями автоматизации налоговых органов являются следующие:

– совершенствование информационной системы налоговой службы;

– разработка и внедрение современных и эффективных информационных технологий;

– совершенствование телекоммуникационной сети, в рамках которой происходит обмен данными между подразделениями налоговой службы, а также информационное взаимодействие с внешними контрагентами;

– подготовка квалифицированных кадров для работы с информационными системами.

Для эффективной работы по администрированию налогов, проведению результативных проверок и обеспечению поступлений в бюджет ФНС выполняет обработку очень больших объемов информации. Для удовлетворения потребности в обработке все возрастающих объемов данных возможно использование новейшего программного обеспечения АИС «Налог-new», которое разрабатывается в рамках модернизации ФНС и ее территориальных органов. АИС «Налог-new» представляет собой единую информационную систему, которая подразумевает комплексную перестройку организационной структуры ФНС, выстраивание новых бизнес-процессов. Она создает механизмы интеграции баз данных федерального и регионального уровня и таким образом может использовать всю накопленную в налоговой службе информацию.

Создание АИС «Налог-new» должно привести к следующим результатам:

1. Значительный рост автоматизации рутинных операций за счет внедрения технологии «Налоговый автомат». Налоговый автомат – технология, которая позволяет обеспечить своевременную обработку поступающих документов и автоматизацию формализованных процедур налогового администрирования. В рамках этой технологии предполагается автоматизация процессов начисления, проводки платежей, взыскания недоимок и др. Внедрение технологии «Налоговый автомат» позволит передать целый ряд рутинных функций и принятия формализованных решений из инспекций в информационные системы более высокого уровня.

2. Развитие сервиса «Личный кабинет», который даст возможность вывести на новый уровень процессы взаимодействия налогоплательщиков и налоговой службы. Новая парадигма информационных систем пред- полагает, что налогоплательщики станут не просто пользователями информационной системы, а партнера- ми, а фискальный орган будет выполнять в том числе сервисные функции. В связи с этим важной задачей становится широкое предоставление информационных сервисов как внешним (налогоплательщики, органы власти), так и внутренним пользователям информационной системы.

3. Повышение эффективности деятельности налоговых органов путем использования более прогрессивной системы оценки их работы. Это станет возможно благодаря максимальной автоматизации процессов, консолидации внутренней и внешней информации о деятельности налоговой службы на федеральном уровне, что позволит оценить те аспекты деятельности налоговых органов, которые на сегодняшний день оценить крайне затруднительно.

Основные задачи проекта модернизации налоговых органов АИС «Налог» представлены на рисунке 1.

Рис. 1. Задачи модернизации автоматизированной информационной системы «Налог»

Таким образом, задача модернизации и увеличения эффективности функционирования АИС «Налог» является актуальной и необходимой и ведёт к повышению уровня централизации, консолидации и интеграции налоговой информации, развитию системы анализа и прогнозирования

и обеспечению оперативности принятия решений налоговыми органами, оптимизации процесса электронного взаимодействия с налогоплательщиками, повышению эффективности контрольной работы.

Список литературы:

1. Абхалимова Р.С., Шарафутдинов А.Г. (2014). Информационные технологии XXI века//Экономика и социум. № 2−5 (11). С. 234−236.
2. Лебедева Ю.А. (2017). Роль потребительских бюджетов в стратегии развития Российской Федерации//Государственное и муниципальное управление в Российской Федерации: современные проблемы и перспективы развития. Сборник научных трудов преподавателей, аспирантов и студентов кафедры государственного и муниципального управления. Москва. С. 35−41.
3. Милькина И.В., Косарин С.П. (2017). Искусственный интеллект в системе управления городом//Шаг в будущее: искусственный интеллект и цифровая экономика: Материалы 1-й Международной научно-практической конференции. Государственный университет управления. С. 258−264.
4. Милькина И.В., Косарин С.П., Ходанова Н.А. (2016). Построение информационно-аналитической системы управления жилищно-коммунальным комплексом//Вестник Университета. № 20. С. 80.
5. ХмелякА.С. (2014). Информационные технологии как метод совершенствования работы налоговых органов//Наука и современность. № 30. С. 199–203.

УДК 004

Кокшев Павел Андреевич
направление 09.06.01 «Информатика и вычислительная техника» профиль «Элементы и устройства вычислительной техники и систем управления» (аспирантура), группа А-05.13.05-20

Научный руководитель
Галанина Наталия Андреевна,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения,
ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова», г. Чебоксары

ИССЛЕДОВАНИЕ И РАЗРАБОТКА НЕЙРОСЕТЕВЫХ АЛГОРИТМОВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ДЛЯ СЕТЕВОГО АНАЛИЗАТОРА ДАННЫХ ЦИФРОВОЙ ПОДСТАНЦИИ

Цель работы – разработка нейросетевых алгоритмов обнаружения вторжений для сетевого анализатора данных для цифровой подстанции.

Когда речь заходит о цифровизации в энергетике, не обходится без упоминания относительно новой коммуникационной технологии МЭК 61850. Подстанции, разработанные с применением стандарта МЭК 61850, называются цифровыми подстанциями. Следовательно, объектом исследования являются данные, передающиеся в сети цифровой подстанции.

Защита информации в автоматизированной системе управления технологическими процессами является составной частью работ по созданию (модернизации) и эксплуатации автоматизированных систем управления технологическими процессами и должна обеспечиваться на всех стадиях ее жизненного цикла[5].

С внедрением стандарта МЭК 61850 для цифровых подстанций появилась возможность и необходимость внедрения систем диагностики и анализа трафика цифровых подстанций [4,6]. В связи с этим необходимо использовать требования к аудиту безопасности, аименно АУД.5 «Контроль и анализ сетевого трафика». Даннаямера позволит исключить подачу несанкционированных управляющих команд, которые выходят за рамки цифрового проекта(файла описания конфигурации подстанции SCD). Кроме того,появится возможность диагностировать пропадание связи, как сцелыми сегментами сети, так и с отдельными устройствами[1].

Анализатор сетевых пакетов – это программа, работающая на уровне сетевого адаптера и перехватывающая весь трафик[2].

Анализ данных представляет собой процесс сбора всех данных, проходящих через определенный сетевой интерфейс. Благодаря этому появляется возможность мониторинга сети и перехват пакетов, проходящих через эту сеть. Это дает широкие возможности для контроля состояния сети в части информационной безопасности.

С помощью разработки анализатора сети можно предупредить два из этих трех основных типов угроз безопасности. К ним относятся нарушение целостности информации и нарушение работоспособности информационной системы, то есть отказ в обслуживании.

Задача сетевого анализатора состоит в идентификации и реагировании на подозрительную деятельность внутри сети. Для этих целей разумно применять алгоритмы нейронных сетей, что позволит не только выявить сетевые атаки в режиме реального времени, но и по набору признаков определить ее тип и характеристики.

Основное преимущество в применении нейронной сети в выявлении вторжений — это гибкость, которую предоставляет эта сеть. Нейронная сеть может анализировать данные из сети, даже если данные являются

неполными или искаженными. Кроме того, сеть сможет выполнять анализ с данными в нелинейном виде. Обе эти характеристики важны в сетевой среде, где получаемая информация подвержена случайным системным ошибкам. Кроме того, поскольку некоторые атаки на сеть могут быть осуществлены скоординированным вторжением нескольких злоумышленников, особенно важно уметь обрабатывать данные из нескольких источников в нелинейном виде [4].

Выводы

Применение нейросетевых алгоритмов в сетевом анализаторе данных открывает широкие возможности в плане обнаружения вторжений и противодействия им. Это повышает надежность функционирования цифровой подстанции и целостность передачи данных внутри ее сети.

Список литературы:

1. Кокшев, П.А. Оценка угроз информационной безопасности в цифровой подстанции / П.А. Кокшев, А.А. Андреева // Состояние и перспективы развития IT-образования: сб. докл. и науч. ст. Всерос. науч.-практ конф. – Чебоксары: Изд-во Чуваш.ун-та, 2019. – С. 225-231.
2. Анализатор сетевых пакетов. [Электронный ресурс] Режим доступа: http://teacherbox.ru/kompseti/sniffer/.html (Дата обращения 04.03.2020).
3. Фимичев Н.Н. Применение нейронных сетей в обнаружении вторжений // Современные научные исследования и инновации. 2015. № 10 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2015/10/58404 (дата обращения: 10.11.2020).
4. Moiseev D.V. Conducting an express analysis of emergency events of the electrical system based on calculations of the algorithm for determining the location of fault / D.V.Moiseev, N.A.. Galanina, N.N. Ivanova // Proceedings of the 2nd 2020 International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), 2020.- С. 9059206.
5. Охоткин Г.П. Методика структурного синтеза релейного регулятора тока транзисторного электропривода / Охоткин Г.П., Угарин С.В., Галанина Н.А.. - Электротехника.- 2017.- № 7. - С. 15-19.
6. МоисеевД.В. Разработка программного комплекса диагностики централизованной системы РЗА /Д.В. Моисеев, Н.А. Галанина, Н.Н. Иванова //Информационные технологии в электротехнике и электроэнергетике:материалы XII-й Всеросс. научн.-техн. конф. – Чебоксары: Изд-во Чуваш.ун-та, 2020. - С.383-385.

УДК 004.42

Кошкин Егор Николаевич, Корнилов Артём Сергеевич
направление Информатика и вычислительная техника, гр. ИВТ-21

Научный руководитель
Васяева Наталья Семёновна,
канд. техн. наук, кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА ДВУХАГЕНТНОЙ АВТОМАТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ УСТРАНЕНИЯ ПРЕПЯТСТВИЙ НА ЛИНИИ

Цель работы – разработка двухагентной автоматизированной транспортной системы с устранением препятствий на линии.

Применение двухагентной автоматизированной транспортной системы (АТС) может стать решением проблемы многих производственных предприятий, которым необходима слаженная работа двух и более автономных устройств, которые бы выполняли поставленные задачи не смотря на возникающие внештатные ситуации. Примером такой системы могут послужить роботы погрузчики, которые автономно выполняют транспортировочные задачи, передавая друг другу информацию о выполнении какой-либо задачи или о возникновении препятствия на линии движения погрузчиков.

Задачу двухагентного АТС можно рассмотреть, как последовательность двух подзадач: 1) движение одного робота по маршруту (линии) и обнаружение препятствий; 2) устранение вторым роботом обнаруженного препятствия.

Первый робот состоит из каркаса на котором крепятся все датчики, платы, моторы и источники питания. В качестве питания используются два литий-ионых аккумулятора 18650 соединённых последовательно для увеличения напряжения. Основным управляющим контроллером выступает плата ArduinoMEGA 2560, поскольку именно эта плата обладает необходимым количеством пинов для подключения большого числа устройств. В движение робота приводят два коллекторных электродвигателей с колёсами. Управляет двигателями драйвер L298, поскольку он способен корректно управлять данными электродвигателями и не потребляет много энергии.

Обмен информацией между роботами осуществляется при помощи модулей Bluetooth HC-06 с дальностью связи до 30 метров. Для задачи

создания прототипа двухагентной системы дальности действия протокола IEEE 802.15.1 вполне достаточно.

Движение по линии обеспечивается инфракрасным сенсором Line Follower Module, который имеет на борту 8 датчиков и общается с Arduino по линии I^2C. Он позволяет наиболее точно отслеживать заданную линию. Сенсор закреплён в передней нижней части робота.

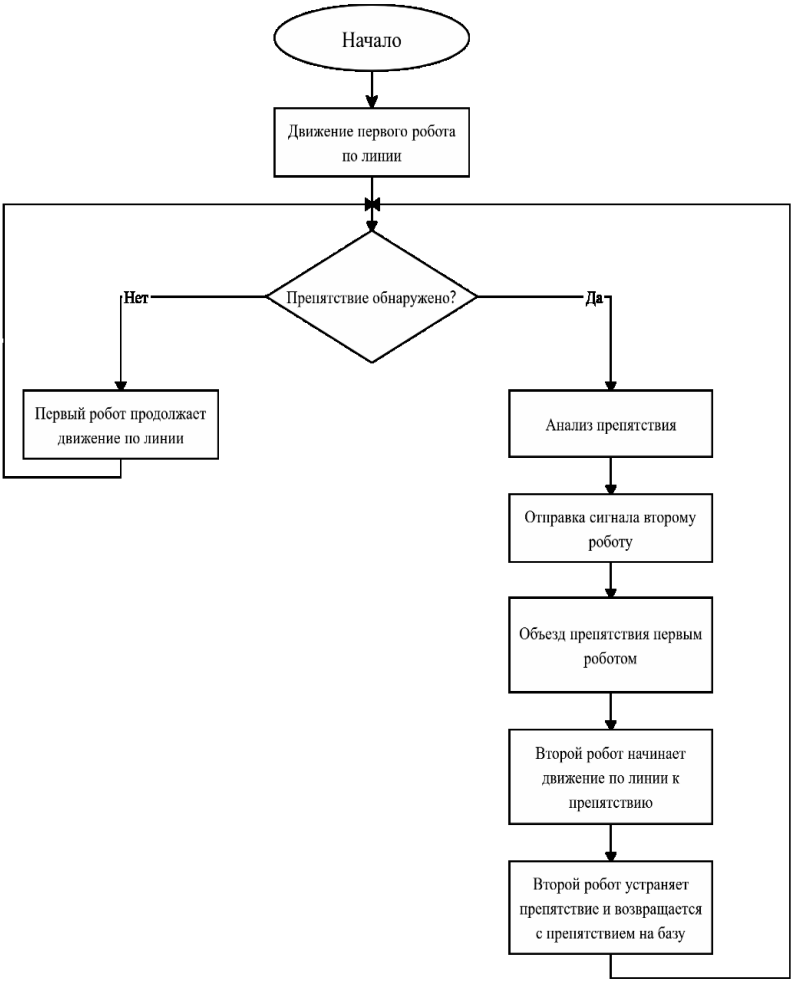


Рис. 1 Обобщенный алгоритм взаимодействия двух роботов

Для ориентации в пространстве используются три инфракрасных дальномера, расположенные на передней и боковых частях робота. Они нужны для обнаружения препятствия и объезда их.

Алгоритм передвижение по линии второго робота полностью аналогичен алгоритму первого робота. Роль второго робота заключается в том, чтобы при обнаружении роботом №1 препятствия, при помощи захвата убрать препятствие с линии, доставив его к месту разгрузки. Механизм захвата представляет собой систему тяг, которые приводятся в движение сервомоторами. Манипулятор закреплен на верхней части конструкции робота. На рис. 1 приведён обобщённый алгоритм взаимодействия двух роботов.

Отдельной задачей является определение габаритов препятствий вторым роботом. Это требуется для принятия решения о том, как реализовывать устранение препятствий в зависимости от их размеров. Возможны три варианта: 1) сдвиг препятствия с линии так, чтобы оно не мешало прохождению маршрута, в случае невозможности захватить его; 2) захват препятствия и доставка его к месту разгрузки без погрузки в контейнер робота №2; погрузка препятствия в контейнер и доставка его к месту разгрузки.

Список литературы:

1. Блум, Дж. Изучаем Arduino. Инструменты и методы технического волшебства / Дж. Блум. – БХВ - Петербург, 2015. – 336 с.
2. Программирование микроконтроллерных плат Arduino/Freeduino / Улли Соммер - БХВ-Петербург 2012. – 256 с.
3. Проекты с использованием контроллера Arduino, 2-е издание / Виктор Петин - БХВ-Петербург 2015. – 448 с.
4. Делаем сенсоры. Проекты сенсорных устройств на базе Arduino и Raspberry Pi / Теро Карвинен, Киммо Карвинен, Вилле Валтокари – Вильямс 2015. – 445 с.
5. Arduino Essentials / Francis Perea - Packt Publishing 2015. – 206 с.Аандрэ, Ф. Микроконтроллеры семейства SX фирмы Ubicom / Ф. Аандрэ. - М.: ДМК, 2016. – 272 с.
6. http://arduino-projects.ru/
7. https://www.cyberforum.ru
8. https://atmel.ucoz.ru/publ/spravochnik_po_jazyku/1-1-0-1

УДК 004.42

Кузовов Н.Д.
группа БТСм-11

Научный руководитель
Дубровин Василий Николаевич
доктор медицинских наук, профессор
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ КЛАССИФИКАЦИИ ВЫЗВАННЫХ ПОТЕНЦИАЛОВ В СИСТЕМЕ НЕЙРОКОМПЬЮТЕРНОГО ИНТЕРФЕЙСА

Предлагается применение нейронных сетей и глубокого обучения для классификации вызванных потенциалов головного мозга в системе нейрокомпьютерного интерфейса с последующим формированием базы классификаций.

Введение. Нейрокомпьютерные интерфейсы стремительно развивающееся направление медицины и биоинженерии, одним из сдерживающих факторов которого является отсутствие обобщённых баз классификации вызванных потенциалов, а имеющиеся узконаправленны и являются предметом коммерческой тайны. Наилучшим способом классификации больших объёмов данных в современном мире являются нейронные сети, которые во многих аспектах анализа и классификации превосходят классические алгоритмы и даже человека.

Цель работы. Разработка программы для классификации вызванных потенциалов в системе нейрокомпьютерного интерфейса и формирование базы классификации вызванных потенциалов.

Решаемые задачи.Для достижения поставленной цели необходимо:

1. провести анализ существующих методов классификации вызванных потенциалов, с целью выделения их недостатков и основных характеристик определяющих их преимущества;
2. определить основные признаки и структуру будущей нейронной сети, метод и характеристики обучения, формат выходных нейронов;
3. создать окружение для обучения нейронной сети, сформировать базы данных для её обучения;
4. разработать программу нейронной сети, произвести её обучение;
5. произвести испытание обученной нейронной сети.

Техника решения. Процесс подбора параметров для обучения нейронной сети, подразумевает экспериментальный подбор

«гиперпараметров» - значений, которые подбираются вручную, методом проб и ошибок, например момент, скорость обучения. То же самое можно сказать и про структуру нейронной сети, количество слоёв, количество нейронов в каждом слое подбираются экспериментально, до достижения оптимальных показателей.

Поэтому одной из ключевых задач является формирование базы для обучения нейронной сети и её окружения, без которых невозможно начать процесс обучения, и определить оптимальную структуру для конкретной задачи и выбрать гиперпараметры. Так же формирования базы для обучения нейронной сети является наиболее трудоёмким процессом, необходимо собрать обширные данные снейроинтерфейсов, разбить их на тестовые, группы обучения и сгруппировать по выбранным признакам (например, состояние покоя, зрительная концентрация, аудио-концентрация, движения отдельных конечностей, изолированные движения в суставах).

Программа будет разрабатываться на языке высокого уровня Python, с использование googleTensorFlow.

Выводы. В результате работы планируется сформировать базу классификации вызванных потенциалов головного мозга в системе нейрокомпьютерного интерфейса, для этого будет использоваться программа на основе нейронной сети. Одним из ключевых моментов является формирование баз для обучения нейронной сети, и разработка её окружения. Вторым по трудоёмкости процессом является непосредственно этап обучения и формирования оптимальных «настроек» и структуры нейронной сети. В дальнейшем наличие такой базы классификаций будет способствовать развитию нейрокомпьютерных интерфейсов.

Список литературы:

1. Каллан, Роберт. Основные концепции нейронных сетей/ А.Г. Сивока – Пер. с англ. – М.: Издательский дом «Вильямс», 2001г. – 287с.
2. Шолле, Франсуа. Глубокое обучение на Python – СПб.: Питер, 2018г. – 400с.

УДК 253.5

Кулаков Владимир Андреевич
направление Информационная Безопасность (специалитет), гр. БИ-51

Научный руководитель
Гуринович Юрий Федорович,
доцент кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологически университет», г. Йошкар-Ола

ВИЗУАЛИЗАЦИЯ ТОПОЛОГИИ КОМПЬЮТЕРНОЙ СЕТИ ДЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ

С внедрением цифровых технологий в бизнес-процессы государства, различных организаций возрастает необходимость в интеллектуальных системах мониторинга безопасности.

Существуют различные инструменты для анализа состояния всей сети в целом, мониторинга портов, выявления аномалий в «сетевом поведении» пользователя. К таким инструментам относятся и средства визуализации топологии компьютерной сети.

В компьютерных сетях под визуализацией понимается процесс объединения данных в визуальные диаграммы и графики для определения закономерностей, тенденций и корреляций между сетевыми данными.

Модели визуализации базируются на элементах визуальной грамматики: абстрактном (точка, линия, плоскость, измерение, формат), конкретном (цвет, прозрачность, тон, фигура), действии (масштаб, движение, отражение) и сравнении (симметрия, соотношение, баланс, кластерность).

Классическим представлением модели визуализации компьютерной сети является связанный граф (рис. 1). Под узлами графа понимаются хосты сети (компьютерное и сетевое оборудование), а дугами обозначаются связи между хостами (физические или информационные).

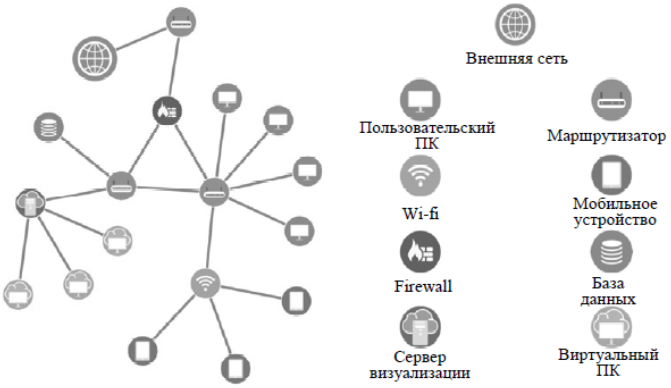


Рис. 1. Демонстрация топологии сети типы устройств и связи между устройствами, представленные при помощи графа

Сценарий использования графической модели предполагает визуализацию для анализа топологии сети и получение значений нескольких метрик для каждого хоста и связей между хостами.

Качество работы системы визуализации зависит от того, насколько эффективно пользователь воспринимает информацию при анализе изображений, предоставляемых системой, и от того насколько эти изображения информативны. Информативность визуализации зависит от детализации собранных агрегированных и корректированных данных и от графических моделей, отображающих эти данные.

Процесс визуализации топологии компьютерной сети состоит из шести этапов:

Этап 1. Выбор источников данных. Для визуализации топологии и параметров сети наиболее важны физические источники информации, например, могут использоваться активные и пассивные средства сбора информации о компьютерной сети: Nmap и Wireshark.

Этап 2. Выбор алгоритмов агрегации и корреляции. С использованием определенной последовательности выбранных алгоритмов происходит анализ данных, их объединение и формирование непосредственно для отображения.

Этап 3. Формирование списка графических моделей. На этом этапе выбираются модели, которые позволяют визуализировать полученные данные. В большинстве систем для визуализации данных компьютерной сети используются графы – при визуализации небольших компьютерных сетей или сетей, хосты которых не содержат много связей.

Этап 4. Изменение графических моделей для обеспечения необходимого соотношения «эффективность-информативность».

Этап 5. Добавление инструментов. Для дополнительной корректировки соотношения «эффективность-информативность».

Этап 6. Создание информационной панели. На заключительном этапе производится объединение графических моделей, инструментов для работы с ними, с модулями сбора и анализа данных в единую систему визуализации.

Таким образом, решение по визуализации сети – это важный набор полезных инструментов, которые обеспечивают критический обзор всей сетевой инфраструктуры. Использование в IT-среде такого решения может повысить эффективность, помочь в выявлении реальных угроз и их устранении.

Во многих случаях визуализация сети относится к отображению топологии сети, чтобы определить физическое расположение и текущее состояние сети. Система визуализации позволяет оценить уровень защищенности системы и может быть использована для формирования полного понимания состояния защищенности системы.

Необходимо учитывать соотношение эффективности восприятия данных пользователем и информативности данных визуализации с целью визуализации топологии компьютерной сети для мониторинга данных безопасности.

Список литературы:

1. Гуз Александр. СправочноеруководствоNmap (ManPage). // SPecialiSTRePack. – 2017.

2. Сандер Крис. Анализ пакетов. Практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях. // Вильямс. – 2019.

3. М. В. Коломеец, А. А. Чечулин, И. В. Котенко. Методика визуализации топологии компьютерной сети для мониторинга безопасности. // Изв. вузов. Приборостроение. - 2016. - №10. С. – 807-811.

4. Сергеев А.Н. Основы локальных компьютерных сетей. Учебное пособие. // Лань. – 2016.

УДК 339.138

Лебедев Михаил Алексеевич
направление Информатика и вычислительная техника(магистратура),
гр.ИВТм-13

Научный руководитель
Зыкова Надежда Николаевна,
канд.соц. наук, кафедра социальных наук и технологий
ФГБОУ ВО «Поволжский государственных технологический университет»,
г. Йошкар-Ола

СОЦИАЛЬНАЯ РЕКЛАМА –ИНСТРУМЕНТ В СОВРЕМЕННЫХ УСЛОВИЯ ИНЖЕНЕРНОЙ ДЕЯТЕЛЬНОСТИ

Цель работы–раскрыть в данной статье понятие социальной рекламы, раскрыть основанное назначение социальной рекламы, показать актуальные развития рынка в плане рекламы. Выполнить сравнительный анализ социальной рекламы от государственной. Раскрасть значимость предпринимательской деятельности в сфере социальной рекламы.

В настоящеевремя реклама представляет собой новый востребованный инструмент в современные условия деятельности.Подтверждение этого - проведение фестивалей и конкурсов социальной рекламы: Московский фестиваль социальной рекламы, Международный фестиваль социальной рекламы «МЫ! /WE!», Фестиваль наружной социальной рекламы, Первый фестиваль социальной интернет рекламы и много других ежегодно организуемых мероприятий ...).

Реклама необходима в сфере современной деятельности для наглядной демонстрациииположительных аспектов и привлечения заинтересованных лиц путём интеграции интересной и актуальной информации в неё.

Основной задачей социальной рекламы — является изменение отношения людей,к проблемам, которые существуют в настоящее время, в долгосрочной перспективе — предложение новых социальных ценностей и идей, необходимых обществу.

Для определения понятия социальной рекламы и дальнейшего разбора её воздействия на различные группы в социуме я хочу обратиться к ФЗ « О рекламе» от 13.03.2006N38«социальная реклама - информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу

лиц и направленная на достижение благотворительных и иных общественно полезных целей, а также обеспечение интересов государства»[1].

Используемый в России термин «социальная реклама» является переводом с английского publicadvertising. В других странах ему соответствуют понятия «некоммерческая реклама» и «общественная реклама». Рассмотрим их определения.

1.Некоммерческая реклама – реклама, распространяемая некоммерческими организациями в их интересах, целью которой является сбор пожертвований, призыв голосовать за определённого кандидата, привлечение внимания человека в обществе к определённой информации (университету, институту и т.п.).

2.Общественная (социальная) реклама распространяет материалы, связанные с пропагандой позитивных явлений, создаётся бесплатно, с предоставлением места в СМИ и времени выхода на некоммерческой основе.[2].

Статус социальной рекламы в России пока ещё невысокий посравнению с аналогичной рекламой на Западе или в США. У нас этой деятельностью подчас занимаются непрофессионалы, что обуславливает низкий уровень качества рекламного продукта и, как следствие, низкую эффективность воздействия на социум. Но проблема состоит не только в качестве, но и в количестве такой рекламы. «Заключение договора на распространение социальной рекламы является обязательным для реклам распространителя в пределах пяти процентов годового объема распространяемой им рекламы».

Как видно из статьи закона, юридическое лицо, профессионально занимающееся рекламной деятельностью, обязано отводить на социальную рекламу лишь 5% площадей или эфирного времени, выделяемого им на распространение рекламных сообщений. Нет ничего удивительного в том, что этот небольшой объем теряется на фоне огромного количества коммерческой рекламы, особенно с учетом того, что фирмы-реклам распространители выделяют для размещения социальной рекламы наименее привлекательные для коммерческих рекламодателей, то есть наименее эффективные места.[1].

Как бы странно и парадоксально это не «звучало», но толчком к развитию социальной рекламы послужил экономический кризис, из-за которого рекламная деятельность многих компаний приостановлена, а рекламные пространства пустуют, и для того, чтобы заполнить так называемые «пробелы» государство предлагает им заполнять

образовавшиеся «ниши» социальной рекламой, не терпя убытков и принося пользу стране.

На рынке социальной рекламы действуют три основных участника:

государство, некоммерческие организации и бизнес.

Государство - основной участник, от него ждут рационального регулирования деятельности на этом рынке, реализации программ развития социальной рекламы. Здесь различают два вида рекламы: государственная реклама (МЧС «Потому что мы первые приходим на помощь», ГИБДД «Безопасность на дорогах», МНС «Пора выйти из тени») и социальная. Несмотря на то, что государственная реклама выражает интересы государства и отражает морально-нравственные ценности народа, она имеет свои признаки и отличия от социальной рекламы. Эти отличия в первую очередь состоят в том, что социальная реклама направлена на достижение социально-значимых целей, тогда как государственная реклама ориентируется на продвижение государственных сервисов и ее цель – повышение эффективности выполнения государством своих функций и улучшение имиджа государства как провайдера разного рода государственных сервисов, сервисных продуктов и услуг. [5]

Ко второму типу (т. е. к социальной рекламе в узком смысле слова) относятся образцы социальной рекламы такие как: «Все у нас получится», «Позвоните родителям», «Не гони на дороге, тебя дома ждут…» и пр.

Социальная реклама духовно обогащает общество, пробуждает в людях лучшие качества. В одной из социальных реклам звучит призыв «Не гони на дороге, тебя ждут дома!», который может восприниматься каждымчеловекомпо-своему, но только действительно сознательный человек осознаёт свою ответственность за будущее не только своё, но и отцов и матерей. В этом случае возможности социальной рекламы неоценимы и государство активно этим пользуется.

Некоммерческие и общественные организации являются одними из основных и постоянных заказчиков социальной рекламы, которая для подобных организаций является инструментом для реализации их деятельности, связанной с достижением социальных, благотворительных, культурных, образовательных и научных целей. Она распространяется в целях охраны здоровья граждан, развития физической культуры и спорта, удовлетворения духовных и других нематериальных потребностей граждан. Социальная реклама некоммерческих организаций направлена на привлечение средств для

пожертвований неимущим, на строительство храмов, покупку еды и одежды для бедных и т.д. Основную часть социальной рекламы, размещаемой в средствах массовой информации, занимает именно реклама некоммерческих организаций. Последним участником на данном рынке, который все больше осознает свою потребность в этой деятельности, является бизнес.

Для предпринимателя социальная реклама - это инструмент для создания образа социально ответственного бизнеса. Заставить вести предпринимателя социально ответственный бизнес никто не в силах, к этому призывает лишь внутренний этический принцип, основанный на морально-нравственных ценностях, принятых в обществе. Некоторые коммерческие компании создают одноименные общественные и некоммерческие организации, открывая для себя широкие возможности для заполнения рекламных площадей социальной рекламой, близкой по звучанию с названиями известных коммерческих брендов и марок. Здесь поводом для создания социально-направленной рекламы становится общественная активность коммерческого предприятия. [2].

В современном государстве приняты законы, постановления, нормативно правовые акты, регулирующие деятельность бизнеса. Но помимо них существуют негласные, никем не закрепленные правила. К одному из них относится обращение к корпоративно социальной ответственности (КСО) бизнеса. Само понятие КСО подразумевает ответственность субъектов бизнеса за соблюдение норм и правил, неявно определенных или неопределенных законодательством (в области этики, экологии, милосердия, человеколюбия, сострадания и т. д.) влияющих на качество жизни отдельных социальных групп и общества в целом.[2].

Социальная ответственность бизнеса это, прежде всего, влияние на общество. Эта ответственность проявляется не только в осуществлении благотворительных программ, специальных программ социального назначения и т.д., а так же в том, чтобы производить безопасные качественные товары, устанавливать доступные цены, предоставлять правдивую информацию о своей продукции, способствовать улучшению социального климата в своей организации, а затем и в государстве.

Важным является тот факт, что бизнесмены, владеющие крупными компаниями, начинают вкладывать средства в создание социальной рекламы не только для поддержания имиджа и косвенной рекламы собственной продукции, а также потому, что им не безразлично, в какой стране будут расти и воспитываться их дети. Это указывает на

начавшийся переход российских предпринимателей от получения прибыли в максимально короткий срок без оценки негативных последствий своей деятельности для общества к осуществлению этической оценки своего бизнеса и к участию в решении общественно значимых задач, не сулящих экономической выгоды в краткосрочной перспективе (или вообще не связанных с получением дохода). Это имеет большое значение для социально-экономического развития нашей страны и для повышения качества жизни.[2].

Выводы

В настоящее время социальная реклама играет важную роль для всех, не только для предпринимателей или узко заинтересованной группы лиц. Я бы сказал, что основная деятельность социальной рекламы направленна для поднятия острых проблем и агитации ЗОЖ, правильного питания, улучшения качества жизни и прочих социальных проблем.

Наша страна в настоящее время находится на стадии осознания роли бизнеса и общества в развитии социальной рекламы, которая является способом воздействия общественных объединений, преследующих духовные, нравственные или социальные цели, либо государства на социум в целом или на отдельные слои населения, также она способствует социальной поддержке населения, восстановлению доброжелательных отношений между людьми и развитию на этих принципах новых экономических отношений и построению современного гражданского общества.

Актуальность и вектор направления рассмотрен в данной статье.

Список литературы:

1. Федеральный закон № 38-ФЗ «О рекламе» от 13 марта 2006 года. URL: http://www.consultant.ru/popular/advert/ (дата обращения 6.11.2020).
2. Социальный маркетинг и социальная реклама. URL: http://socialmarket.ru/ (дата обращения 7.11.2020).
3. Пчелина О.В., Тарбушкин А.Ю.Предпринимательство, управление проектами и реклама в социальной сфере: учебное пособие. URL: https://e.lanbook.com/book/93213 (дата обращения 7.11.2020).
4. Николашвили Г. Краткая история социальной рекламы. URL: http://www.socreklama.ru/analytics/list.php?ELEMENT_ID=390&SECTION_ID=122(дата обращения 8.11.2020).
5. Котляров И.Д. Применение аутсорсинга в государственной деятельности в Российской Федерации // Вопросы государственного и муниципального управления. 2012. № 2. С. 112-120. URL:https://vgmu.hse.ru/data/2013/01/14/1303209807/%D0%9A%D0%BE%D1%82

%D0%BB%D1%8F%D1%80%D0%BE%D0%B2%20112-120.pdf (дата обращения 8.11.2020)

УДК 004.056.5

Лежнина Анна Сергеевна
студентка группы ИВТ-11

Научный руководитель
Глозштейн Даниил Александрович
аспирант кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИССЛЕДОВАНИЕ ПОДХОДОВ К ОЦЕНКЕ УГРОЗ И РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Деятельность организаций, функционирующих в современных условиях, обязательно включает в себя информационную составляющую, которой так же, как и любой другой из составляющих экономической безопасности, присущи определенные риски и угрозы.

С развитием IT-технологий и ввиду увеличения числа угроз безопасности, актуальной является задача по разработке универсального методического подхода к оценке рисков информационной безопасности.

Под информационной угрозой понимают «вероятное событие, которое с помощью воздействия на информацию или другие компоненты информационной системы предприятия может привести к нанесению ущерба».

Угрозы информационным активам предприятия могут быть вызваны внутренними (программные и аппаратные сбои в работе оборудования, халатность сотрудников службы экономической безопасности, использование незащищенных каналов связи и т.д.) и внешними (стихийные бедствия, хакерские атаки, обострение конкуренция и т.д.) факторами [3].

Необходимо отметить, что информационные риски могут переходить в категорию информационных угроз при определенных условиях, что позволяет рассматривать их как потенциальные угрозы для экономической безопасности предприятия.

Таким образом, «риск» является более широким понятием, в отличие от понятия «угроза», и вследствие этого можно с уверенностью сказать, что система экономической безопасности предприятия должна быть

риск-ориентированной, направленной на выявление, анализ и оценку рисков, в том числе связанных с ее информационной составляющей.

Изучение термина «риск» применительно к информационной составляющей экономической безопасности предприятия позволило раскрыть особенности управления рисками данной сферы. На рис. 1 представлена схема процесса управления информационными рисками предприятия.

Рис.1. Процессы управления информационными рисками

Управление информационными рисками предприятия основывается на результатах оценки рисков. В свою очередь, оценка рисков информационной безопасности состоит из трех основных элементов, а именно из идентификации угроз, уязвимостей и активов.

Особенностью процесса управления рисками в области информационной безопасности является то, что, несмотря на актуальность проблем, решаемых с его помощью, он не может существовать отдельно и должен быть интегрирован в общую систему обеспечения экономической безопасности предприятия.

Существует огромное количество актуальных для предприятия или организации потенциальных угроз. Вследствие этого процедура их определения и автоматизация процесса моделирования угроз становится достаточно сложной. Методики составления модели угроз сложны, особенно для средних и малых организаций, у которых возможно не хватает ресурсов, чтобы разбираться в методиках и проводить длительные расчеты. Упрощение методик - это потенциальное снижение защищенности ИС. В текущих условиях это может привести к компрометации данных и финансовым потерям. Имеющиеся на рынке решения либо могут быть применены лишь в процессе разработки ПО,

либо являются внутренними решениями, либо нацелены на отдельные области. Универсального решения, соответствующего требованиям наших методик, пока не существует.

Задача управления рисками заключается в выборе обоснованного набора контрмер, позволяющих снизить уровни рисков до приемлемой величины. Стоимость реализации контрмер должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть обратно пропорциональна вероятности причинения ущерба. При моделировании угроз специалистам необходимо знать помимо описания защищаемого объекта сами угрозы. Составление списка актуальных идентифицированных угроз на каждый идентифицируемый актив или группу активов реализуется после завершения анализа этих угроз. Список актуальных угроз формируется на основе теории графов.

Применение графов атак позволяет несколько упростить задачу аналитиков при исследовании проблемы безопасности и защищённости. Деревья атак обладают высокой наглядностью и позволяют хорошо структурировать всевозможные варианты потенциальных проблем для каждого из активов [6]. Деревья атак имеют высокую степень демонстративности и обеспечивают качественное структурирование полного спектра вариантов возникающих потенциальных проблем для всех выделенных активов.Построение дерева для каждого актива следует выполнять таким образом, чтобы в нем были перечислены все потенциальные маршруты реализации атак. Актив (если быть точным, один из его компонентов безопасности - конфиденциальность, целостность, доступность, аутентичность и т. д.) является основой дерева, а в нем самом перечисляются способы и, если достаточно информации, инструменты нарушения этого свойства безопасности. Этот способ также весьма удобен для выявления наиболее критичных и необходимых к исключению вариантов реализации атак и разработки ответных действий на них. Все разновидности атак необходимо закрыть контрмерой (на рис. 1 контрмеры представлены кругами с метками C1 ...C4). Какие-то контрмеры могут закрывать сразу несколько вариантов (например, для подцели G4 контрмера C2), а для некоторых вариантов, возможно, потребуется сразу несколько контрмер (для подцели G5 - контрмеры C2 и C3). Штриховая линия на рис. 1 обозначает, что узлы G4 и G5 маловероятны в случае организации атаки.

Дерево атак создается описанием всех возможных реализаций атак злоумышленником с учетом первоначальной конфигурации ИС. Также учитывается уровень знаний злоумышленника и его финансовые

средства. На основе этого производится анализ защищенности ИС (определение узких мест), формируются рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности. Все объекты графа атак можно подразделить на активы уязвимости и угрозы. Активы задаются вершинами графа. Все возможные последовательности действий нарушителя представляются дугами, связывающими вершины графа [1].

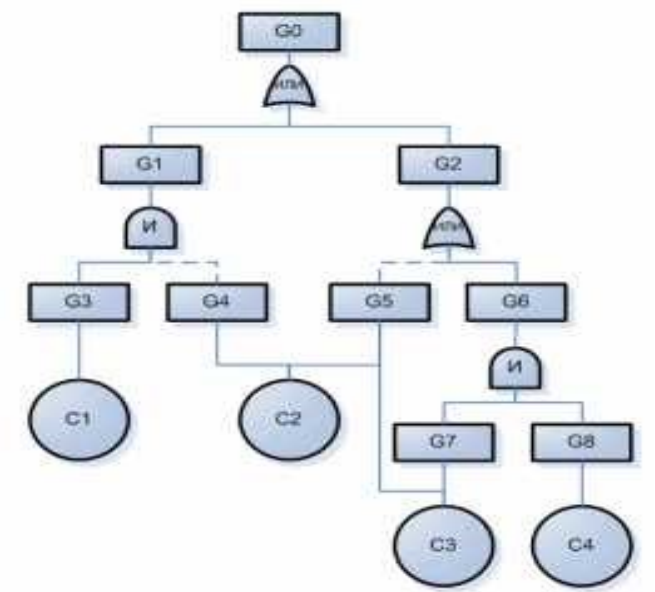


Рис. 2. Дерево атак с определением контрмер для всех вариантов реализации атаки

На сегодняшний день перед каждым предприятием, обеспокоенного вопросами безопасности своих информационных ресурсов, встает вопрос об организации системы защиты информации, которая бы позволила в полной мере обеспечит безопасность функционирования телекоммуникационного оборудования и циркулирующей информации в информационной системе предприятия. Эффективность защиты информации зависит от подхода к ее организации и правильного выбора методов расчета рисков информационной безопасности.

На данный момент разработано значительное количество подходов к оценке и обработке рисков, абсолютно универсальных для любой информационной системы, независимо от того, насколько

конфиденциальна циркулирующая в ней информация. Тем не менее, для корректного конструирования систем защиты информации с использованием этих подходов необходим значительный объем сведений как о реализованных нарушениях безопасности, так и о возможных и неудачных вторжениях, для определения самых актуальных угроз информационной безопасности. Таким образом, требуется некий пункт отсчета, с которой необходимо начинать создавать систему защиты, однако её практическая реализация не всегда допустима из-за ограничения во временном и экономическом вопросах

Одним из наиболее перспективных направлений научной деятельности в сфере информационной безопасности является разработка новых подходов к оценке и обработке рисков конкретных организаций, а также обобщение существующих методик в единую универсальную систему. Динамическое изменение внешних и внутренних условий существования организации, а также отсутствие определенного способа разрешения проблем сохранения ИБ может спровоцировать появление рисков нарушения ИБ. Поэтому особую важность приобретает процесс оценки рисков и выбор соответствующих управленческих подходов. Попытки решения этих проблем производились в серии российских и зарубежных авторов, но значительная часть вопросов до сих пор не определена в достаточной мере.По результатам анализа существующих работ [1-6] было определено, что большая часть рисков нарушения ИБ заключена в ИС организации.

Невозможно полностью устранить все риски ИБ, однако возможно предсказать частоту их появления и уменьшить оказываемое ими воздействие на организацию [2, 5]. Управление рисками должно производиться в строгом соответствии с определенным подходом, алгоритмом или комплексом мер управления. Анализ рисков представляет собой совокупность действий по выявлению уязвимостей и оценке возможного ущерба в случае реализации нарушений ИБ ИС. Риски ИС можно отобразить в виде пирамидальной диаграммы, представленной на рис. 2 (ЛВС - локальная вычислительная сеть; ИТ - информационные технологии).

Рис. 3. Диаграмма рисков информационной системы.

Подобное представление дает возможность позволяет классифицировать риски ИС на бизнес-риски, технические риски и риски нарушения ИБ.

Бизнес-риски имеют прямую связь с функционалом ИС. Они требуют тщательного изучения и прогноза на стадии формулирования задач деятельности организации, подбора инструментов автоматизации производства и мер по оптимизации бизнеса.

Технические риски напрямую связаны с жизненным циклом ИС. Риск, который касается архитектуры данных, формируется из-за того, что используемая топология данных не подпадает под требования общепринятых стандартов. Риск на уровне программного обеспечения (ПО) возникает из-за отсутствия необходимого ПО или когда ПО не совместимо с модулями ИС. Техническое обеспечение и аппаратная архитектура могут осложнять управленческие процессы, это связано с наличием систем хранения данных, кластерами и другими составляющими, что создает необходимость приобретения и внедрения дополнительных средств управления, а также их интеграции в ИС.

Риски нарушения ИБ связаны с архитектурой системы защиты информации (СЗИ) – появление уязвимостей в которой провоцирует формирование риска утечки критически важной информации.

Образование рисков ИС, описанных на рис. 2, формирует экономические и управленческие риски, что является крайне критичным фактором в масштабе всего предприятия. Реализация любого риска ИС

может спровоцировать инвестиционные, экономические и репутационные потери, а их комплекс может остановить непрерывный управленческий процесс, в результате чего снизится качество менеджмента производственной и бизнес-деятельности организации. Чаще всего условия риска вызывают производственные задержки и возникновение ситуаций с высокой степенью неопределенности, что затрудняет принятие оптимального решения по управлению рисками и непрерывностью бизнес-процессов.

Существует несколько общепринятых методологий, используемых для управления информационными рисками и рисками нарушения ИБ. Эти методологии можно разбить на два класса: стандартизированные и качественно-количественные. Первый класс включает в себя меры и процедуры управления, основанные на модели PDCA«Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)», используемую для выстраивания архитектуры управленческих процессов. Качественно-количественные методологии определяют процедуру управления рисками на основе частной методики, направленной на особенности системы.

На базе существующих исследований и стандартизированных требований в области оценки рисков были проанализированы методы управления рисками. Результаты анализа представлены в таблице 1 (выполнение условия критерия оценки обозначено «1», невыполнение условия критерия оценки принято обозначать «0»).

Таб. 1. Анализ методов и подходов к управлению рисками

Метод или подход	Идентификация рисков	Оценка рисков	Анализ рисков	Определение степени	Возможность построения отчета о	Общая оценка
FERMA:2002	1	1	0	0	0	2
COSO:2004	0	1	0	0	0	1
ISO 31000:2009	1	1	1	0	0	3
CRAMM	1	1	0	1	1	4
BS 7799-3:2006	0	1	1	0	1	3
OCTAVE	0	1	1	1	0	3
RiskWatch	0	1	0	1	1	3
CORAS	1	1	1	0	1	4
ГОСТ Р ИСО/ МЭК	1	1	1	0	1	4
Экспертный	0	1	1	0	0	2
Процессный подход	1	0	1	0	0	2

В итоге оценки результативности различных методов максимальный балл получили CRAMM, CORAS, ГОСТ Р ИСО/МЭК. Общим слабым местом этих подходов является узкий диапазон их возможного применения и отсутствие возможности для надежного предсказания и превентивной оценки рисков. Кроме того, весьма значимой при применении зарубежных подходов и методик становится специфика отечественного документооборота и архитектура взаимодействия ИС как между собой, так и со средствами защиты информации.

Список литературы:

1. Гаранжа А. В., Губенко Н. Е. Применение метода построения деревьев атак для защиты интернет - магазинов // Инновации в науке: материалы научно-технич. конф. Донецк, ДонНТУ. 2017

2. Финогеев А. А., Финогеев А. Г., Нефёдова И. С., Финогеев Е. А., Камаев В. А. Анализ информационных рисков в системах обработки данных на основе «туманных» вычислений // Вестн. Астрахан.гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2018. № 4. С. 38-46.

3. Крыжановский О. А., Попова Л. К. Анализ современных подходов к пониманию терминов «риск» и «финансовый риск» // Молодой ученый. — 2016. — №19. — С. 467-471.

4. Вахрамеев Я. М., Богатенков Д. С. Управления рисками и проблемами на проектах по внедрению отечественных ERP-систем // Науч.-метод. электрон. журн. «Концепт». 2016. Т. 17. С. 103-108.

5. Kravets A. The Risk Management Model of Design Department’s PDM Information System // Creativity in Intelligent Technologies and Data Science. Second Conference, CIT&DS 2017 (Volgograd, Russia, September 12-14, 2017). P. 490-500.

6. Lippmann R. P., Ingols K. W., Piwowarski K. Practical Attack Graph Generation for Network Defense.

УДК 004.5

Лоскутова Светлана Сергеевна
направление Прикладная математика иинформатика (магистратура), гр. 4299

Научный руководитель:
Валитова Наталья Львовна,
канд.техн. наук, доцент кафедры прикладной математики и информатики
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ», г. Казань

РАЗРАБОТКА АЛГОРИТМА ЧУВСТВИТЕЛЬНОСТИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РЕШЕНИЯ ОБРАТНЫХ ЗАДАЧ ПРОЧНОСТИ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Цель работы – разработать программное обеспечение для определения ошибки измерений деформации жесткости продольных ребер на растяжение-сжатие в сечениях и разработка алгоритма чувствительности, используя данные, полученные экспериментальным путем.

Перед нами стоит**актуальная** задача – построить адекватную математическую модель, которая позволит решить вопрос о разработке методики измерения деформаций жесткости материалов не для прообразов конструкций, а для реальных элементов.

Математическая часть задачи:

Для применения численных методов решения рассмотрим дискретнуюзадачуприменив метод интегрирующих матриц. Таким образом, имеем:

$$J = \left(\{f'_{exp}\} - \{f'\}\right)\left(\{f'_{exp}\} - \{f'\}\right)^T \to min$$

$$[C + H]\{f'\} = \{P - S\}$$

Здесь $\{f'_{exp}\}$, $\{f'\}$ - столбцы размера nk, экспериментальные и модельные значения деформаций каждого ребра по сечениям конструкции (n – количество ребер, k – количество сечений).

[C] – диагональная матрица порядка nk×nkжесткостей продольных ребер конструкции по сечениям.

[H] – матрица порядка nk×nk коэффициентов, зависящих от формы и жесткости поперечных сечений конструкции.

{P} – столбец размера nk осевых сил, прикладываемых к ребрам на свободном торце конструкции (z=l),

{S} – столбец размера nk, определяемый нагружением конструкции.

Алгоритм чувствительности для решения поставленной задачи:

1) Задаются начальные значения искомой жесткости ребер $\{C^0\}$. Задается шаг метода e и погрешность решения ε. Номер итерации k=0.

2) Пусть выполнено k итераций алгоритма и найдено k-е приближение вектора изгибной жесткости $\{C^k\}$. Решается СЛАУ, и находятся модельные деформации $\{f'\}$.

3) Вычисляется значение целевой функции J.

4) Проверяется правило останова. Если целевая функция J<ε, то алгоритм останавливается и оптимальным считается $\{C^k\}$. Иначе выполняется переход к следующему пункту.

5) Вычисляется матрица чувствительности $[\psi]$ по следующим формулам, полученным дифференцированием СЛАУ:

$$[\psi] = -[C + H]^{-1} \begin{bmatrix} \lceil f'_0 \rfloor & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & \lceil f'_{n-1} \rfloor \end{bmatrix}$$

6) Следующее (k+1)-е приближение изгибной жесткости находится по формуле:

$$\{C^{k+1}\} = \{C^k\} + e\{\partial C\}$$

где $\{\partial C\}$ – вектор-столбец приращения, вычисляемого как решение СЛАУ.

7) Номер итерации k увеличивается на 1 и осуществляется переход к п. 2.

Решением задачи является восстановление жесткости продольных ребер на растяжение-сжатие в сечениях.

Разработка рабочей программы основана на языке программирования C# и базы данных MicrosoftSQL, предварительные расчеты производятся в пакете прикладных программ для решения задач технических вычислений - matlab.

Модули, которые должны присутствовать в программной части:

1) Расчетный, в котором отображается расчет формул.

2) Графический, в котором отображаются графики приближений.

3) Информационный, в котором отображается информация о взаимодействии с программой и справочная информация по математической части программы.

База данных при взаимодействии спрограммной частью должна сохранять и выгружать при необходимости расчетные данные для дальнейшего их использования.

Программа дает возможность получать экспериментальные результаты расчетов, помогает получать графические результаты измерений и сохранять или выгружать данные из единой базы данных.

Выводы

Программа с подобным алгоритмом вычисления деформаций поможет получить экспериментальный результат и уменьшить объем трудозатрат на подобные измерения в реальном времени.

Список литературы:

1. Баничук Н.В. Введение в оптимизацию конструкций. М.: Наука, 1986. 302 с.
2. Дегтярев Г.Л., Сиразетдинов Т.К. Теоретические основы оптимального управления упругими космическими аппаратами. М.: Машиностроение,1986. 214с.
3. Костин В.А., Валитова Н.Л. Идентификация изгибной жесткости балки с использованием функции чувствительности // Новые технологии, материалы и оборудование российской авиакосмической отрасли: Сб. докл. Всерос. науч.-практ. конф. с международным участием. Казань: АН РТ, 2016. Т.1. С. 86–91.
4. Костин В.А., Хуан Ш., Валитова Н.Л. Применение дискретно-континуальной модели расчета на прочность для решения задачи идентификации теплонагруженной конструкции // Изв. вузов. Авиационная техника. 2017. №3. С. 3–7.
5. Костин В.А., Хуан Ш., Валитова Н.Л. Численные методы анализа чувствительности в задачах идентификации конструкций // Вестник КГТУ им. А.Н. Туполева. 2017. Т. 73. №1. С. 78–83.
6. Костин В.А., Хуан Ш., Валитова Н.Л. Решение обратной задачи прочности тонкостенных конструкций с использованием алгоритма чувствительности // Изв. вузов. Авиационная техника. 2018. №1. С. 123–127.
7. Костин В.А., Торопов М.Ю., Снегуренко А.П. Обратные задачи прочности летательных аппаратов // Казань: Изд-во Казан.гос. техн. ун-та, 2002. 284 с.

УДК 633/635

Мишин Сергей Александрович
направление 09.06.01 «Информатика и вычислительная техника» профиль «Элементы и устройства вычислительной техники и систем управления» (аспирантура), группа А-05.13.05-18

Научный руководитель
Галанина Наталия Андреевна,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения
ФГБОУ ВО «ЧГУ им. И.Н. Ульянова», г. Чебоксары

PID РЕГУЛЯТОР В УЗЛЕ РУЛЕВОГО УПРАВЛЕНИЯ

Цель работы – исследование алгоритмов автоматической настройки коэффициентов PID регуляторадля управления коллекторным двигателем.

Одной из проблем мехатронных систем, работающих в агрессивных средах, является недолговечность систем обратной связи [1,2]. Одной из таких систем является система обратной связи в рулевом механизме. Выход ее из строя влечет за собой потерю возможностей управления поворотом рулевого колеса и определения направления движения [4,5].Решением этой проблемы является использование электродвигателей с энкодером, основанным на эффекте Холла.

Слабым звеном управления такой системой является поворотвала двигателя в требуемый угол и удержание этого угла[3]. Для решения этой проблемы необходимо использовать PID регулятор. Функция, описывающая работу PID регулятора, состоит из трех составляющих – пропорциональной, интегральнойи дифференциальной частей (формула 1).

$$U(n) = K_p E(n) + K_i^{discr} \sum_{k=0}^{n} E(k) + K_d^{discr} (E(n) - E(n-1)) \quad (1)$$

Математический смысл пропорциональной части $E(n)$заключается в пропорциональной зависимости выходного значения регулятора и отклонения системы; интегральной части $\sum_{k=0}^{n} E(k)$ - в сумме всех отклонений системы от требуемого значения; дифференциальной части $\big(E(n) - E(n-1)\big)$- в разнице двух соседних отклонений системы[6].

У PID регулятора имеются три коэффициента, которые влияют на «силу» воздействия той или иной части регулятора. Для упрощения подбора коэффициентов можно воспользоваться авто-подбором коэффициентов. Существует несколько методов, используемых в

алгоритмах авто-подбора коэффициентов. Один из таких методов – метод «реле»[4], имеющий следующий алгоритм работы (рис.1):

- подаём управляющий сигнал и ожидаем стабилизации значения с датчика;
- сигнал изменяем на некоторую величину («ступеньку»);
- ожидаем заданное время, затем меняем сигнал на ту же «ступеньку», но в другую сторону;
- начинаем«раскачивать» систему;при прохождении значения с датчика через значение стабилизации сигнал снова переключается;
- производим анализ периода «раскачки» и её амплитуды; на основании этих данных вычисляем рекомендуемые коэффициенты.

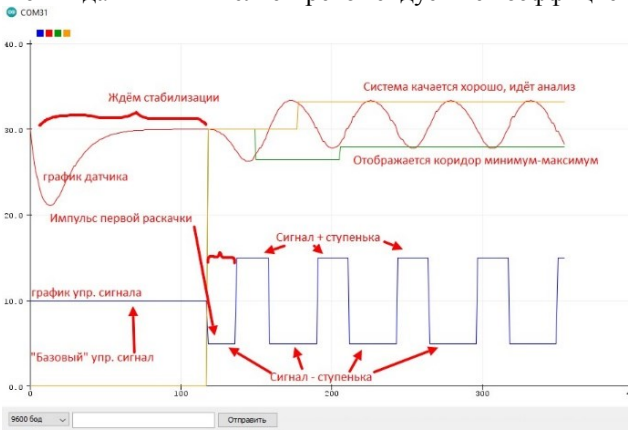


Рис. 1. Иллюстрация алгоритма авто-настройки

Полученные результаты работы алгоритма автоматического вычисления коэффициентов: Kp = 0.1;Ki = 0.05; Kd = 0.01.

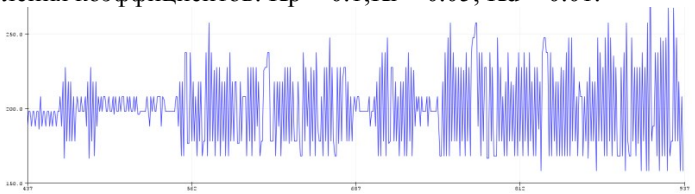


Рис. 2. Показания реальной угловой скоростипри заданном значении 200 градусов/сек

Из анализа графика(рис. 2) следует, что дифференциальный коэффициент необходимо снизить, чтобы убрать паразитное раскачивание системы.

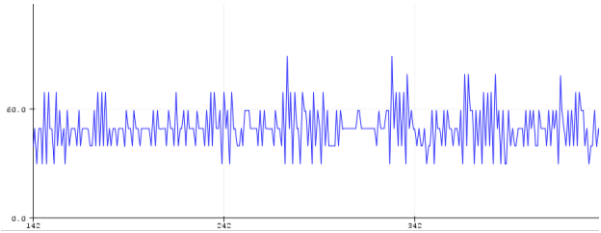


Рис. 3. Показания реальной угловой скорости при заданном значении 50 градусов/сек

На графике (рис. 3) видно, что раскачивание системы пропало. Следующим шагом является проверка системы на большое изменение установки. Этот шаг позволит проанализировать коэффициент интегральной части.

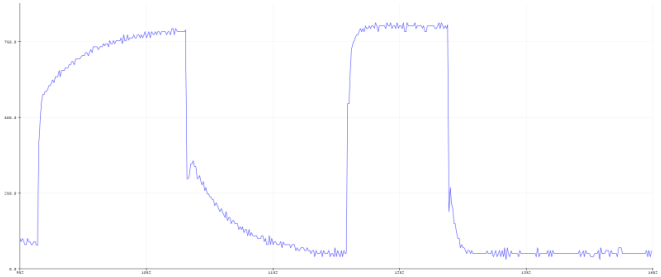


Рис. 4. Сравнение показания реальной угловой скорости при изменении установки с 50 до 800 градусов/сек с разным коэффициентом Ki

Из графика (рис. 4) видно, что увеличение коэффициента интегральной части с Ki = 0.05 до Ki = 0.03 значительно улучшило отклик системы на большое изменение установки.

Выводы. Разработана модель управления коллекторным двигателем на основе изучения реальных данных с датчика положения вала; в результате былореализовано управление электродвигателем с обратной связью. На практике данную систему можно использовать, например, в рулевом управлении трактора для правильного регулирования положениярулевого вала в режиме реального времени.Следует отметить, что результаты погрешности регулирования угловой скорости составили менее 2%.

Список литературы:

1. Leea, D., Yia, K., Changb, S., Leeb, B., Jangc, B. Robust steering-assist torque control of electric-power-assisted-steering systems for target steering wheel torque tracking // School of Mechanical and Aerospace Engineering, Seoul National University. 2018. P. 20 – 32.

2. J. E. Naranjo, C. González, R. García, T. de Pedro Electric Power Steering Automation for Autonomous Driving // Lecture Notes in Computer Science. 2015. P. 113-119.
3. PID Controllers Auto Tuning - Relay Feedback // URL: http://auto-controls.blogspot.com/2009/10/pid-controllers-auto-tuning-relay.html
4. Мишин С. А., Галанина Н. А. Разработка диспетчера задач // Информационные технологии в электротехнике и электроэнергетике. - Чебоксары: Чувашский государственный университет имени И.Н. Ульянова, 2020. - С. 481-483.
5. Мишин С. А., Галанина Н. А. Разработка алгоритма управления автономными группами роботов на основе анализа возможных подходов // Состояние и перспективы развития ИТ-образования. - Чебоксары: Чувашский государственный университет имени И.Н. Ульянова, 2019. - С. 174-180.
6. Мишин С. А., Борисов М. А. Разработка меню устройства для автоматического управления потоком жидкости // Современные технологии в машиностроении и литейном производстве. - Чебоксары: Чувашский государственный университет имени И.Н. Ульянова, 2018. - С. 498-502.

УДК 004.42

Морохина Дарья Дмитриевна
направление Информатика и вычислительная техника (магистратура),
гр. ИВТ-21

Научный руководитель
Васяева Елена Семёновна,
канд. техн. наук, кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА СИСТЕМЫ РАСПОЗНАВАНИЯ ШАШЕК КАМЕРОЙ OPENMVH7

Цель работы – разработка алгоритма распознавания шашек камерой машинного зрения OpenMVH7.

Платформа с интегрированным модулем видеокамеры OpenMV H7 состоит из светочувствительной КМОП-матрицы OV7725, 32-битного микроконтроллера STM32F765VIT6, понижающего DC-DC регулятора напряжения PAM2305AAB330 и светоиндикации (рис. 1) [3].

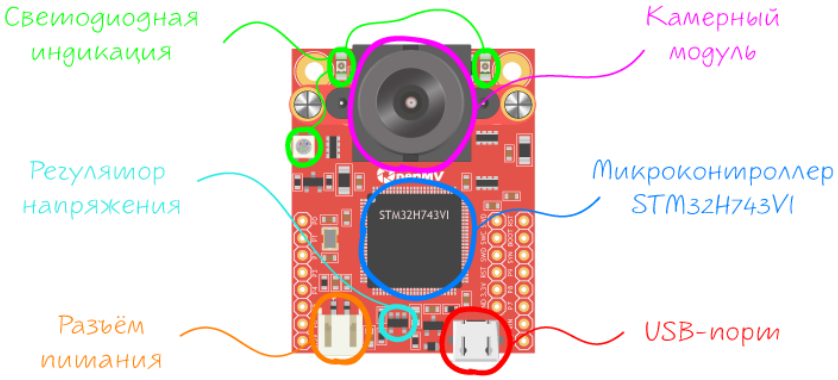


Рис. 1. Элементы платформы OpenMV H7

При помощи КМОП-матрицы осуществляется захват изображения. Размер матрицы 1/3″ с максимальным разрешением 640×480 (VGA). Камера позволяет снимать видео в 8-битном режиме оттенков серого или цветном 16-битном формате RGB565 с частотой 75 кадров в секунду. Поддерживаются форматы сжатия MJPEG, GIF и несжатое видео RAW. Объектив с фокусным расстоянием 2,8 мм и диафрагмой F2.0 крепится через байонет со стандартной резьбой M12 с шагом 0,5 мм, поэтому к OpenMV H7 подходят сменные объективы от GoPro и других портативных камер. На обратной стороне объектива установлен ИК-фильтр на 650 нм, который можно снять для съёмок в темноте.

Мозгом платы выступает 32-битный процессор STM32H743VI} от компании STMicroelectronics с вычислительным ядром ARM Cortex-M7. Контроллер отвечает за обработку изображения с камерного модуля OV7725, а также предоставляет доступ к 10 пинам ввода-вывода общего назначения (GPIO) для коммуникации с внешними устройствами. Микроконтроллер предоставляет 2 МБ Flash-памяти и 1 МБ RAM-памяти.

Светоиндикация представлена одним RGB светодиодом и двумя обычными, которые включаются при заданных пользователем значениях.

Камера может подсоединяться к компьютеру через разъём micro-USB либо на какую-либо автономную установку. Например, квадрокоптер или манипулятор.

На платформе также присутствует слот для карты памяти формата microSD. Внешняя память используется для записи и хранения тяжёлых медиафайлов. Объём памяти может быть до 64 ГБ.

Система распознавания шашек состоит из камеры машинного зрения OpenMVH7, которая подсоединена к компьютеру при помощи USB кабеля, и неподвижной стойки, которая фиксирует камеру ровно над центром шахматной доски на высоте (h, см.), позволяющей камере захватить всё поле без лишних предметов (рис.2).

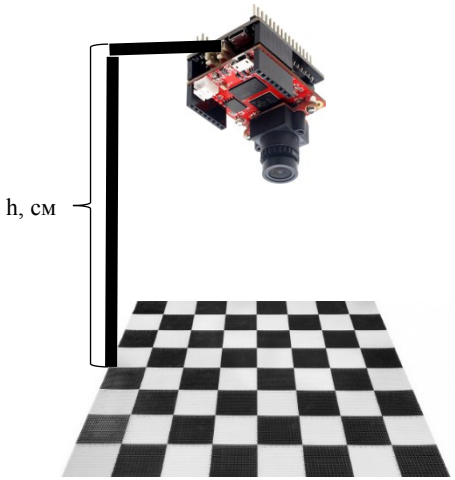


Рис. 2. Система распознавания шашек

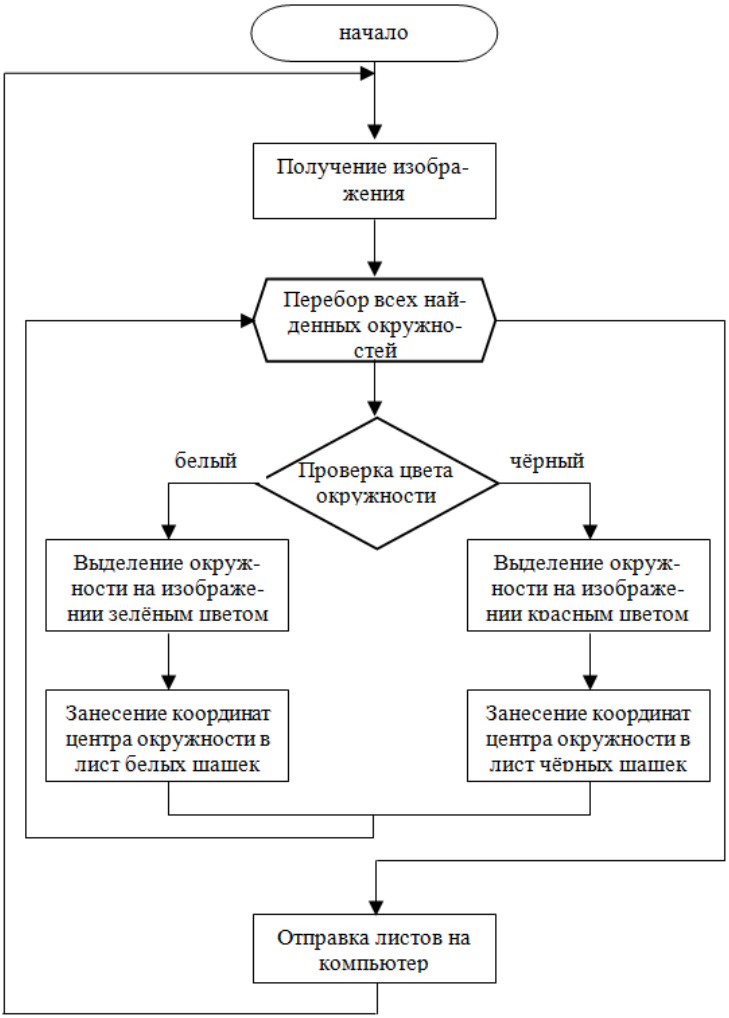


Рис. 3. Блок-схема алгоритма определения координат черно-белых шашек

Данная платформа программируется в среде OpenMV IDE на языке MicroPython.

Задачу распознавания шашек можно условно разделить на две подзадачи: распознавание окружностей на изображении и разделении их по цветам.

Частота опроса камеры процессором составляет 30 раз в секунду. Для начала на полученном изображении находятся окружности всех радиусов. В данном случае в объектив попадают только сами шашки, которые имеют равные между собой размеры. Лишние круги могут быть обнаружены только при слишком ярком освещении, когда на доске или шашках возникают блики. А таком случае необходимо в программе задать дополнительную проверку на допустимый радиус, что уменьшит вероятность ошибки.

Следующий шаг включает в себя перебор всех найденных на изображении окружностей, которые содержатся в некотором временном архиве, и определение цвета каждой из них.

Алгоритм определения цвета некоторого объекта заключается в переборе каждого пикселя объекта и проверке его на принадлежность нужному цвету по модели RGB. Учитывая, что шашки могут иметь только белый и чёрный цвета, эту же процедуру можно реализовать на цветовой модели HSV.

На промежуточном изображении все пиксели нужного цвета окрашиваются в белый, остальные в чёрный, после чего проводится сравнение полученных областей и ранее выделенных окружностей. Первой проходит проверка на белый цвет и все совпадающие области обводятся на изображении зелёным, а координаты центра (x,y) заносятся в соответствующий лист. При проверке на чёрный цвет окружности выделяются красным.

После окончания цикла, где были перебраны все найденные окружности, оба сформированных листа посылаются по проводу на компьютер. Там с их помощью можно восстановить расположение шашек на доске. Данный алгоритм описан в блок-схеме на рис.3.

Данная установка может являться частью большей системы, состоящей помимо неподвижной машинного зрения OpenMVH7 из манипулятора, который будет передвигать шашки по полю в соответствие с полученной командой либо по Bluetooth модулю от пользователя, либо по проводу от шашечной программы.

Список литературы:

1. Клетте, Р. Компьютерное зрение. Теория и алгоритмы/ Р. Клетте. – Пер. с англ. – М.: ДМК Пресс, 2019. – 506 с.

2. Лутц, М. Изучаем Python, 4-е издание. / М. – Пер. с англ. – СПб.: Символ-Плюс, 2011. – 1280 с.

3. Камера машинного зрения OpenMVH7: техническая документация [Электронный ресурс]. Режим доступа: http://wiki.amperka.ru/products:openmv-cam-h7.

УДК 004.056.5

Морохина Дарья Дмитриена
студентка группы ИВТ-21
Дегаев Максим Николаевич
аспирант кафедры информационно-вычислительных систем

Научный руководитель
Глозштейн Даниил Александрович
аспирант кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИССЛЕДОВАНИЕ МЕТОДИК ОПИСАНИЯ И КЛАССИФИКАЦИИ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исследование проблем оценки реального уровня защищенности критически важных информационных систем (далее - ИС) в процессе их эксплуатации является одним из приоритетных направлений в развитии информационной безопасности (далее - ИБ). Оценка реального уровня защищенности ИС является основой построения всей системы защиты информации для каждой конкретной организации, а также определяет вектор развития уже существующей системы защиты, акцентируя её уязвимые стороны.

Под защищенностью понимается состояние информации, при котором становится невозможным или затруднено воздействия случайного или преднамеренного характера, влияющие на конфиденциальность, целостность и доступность информационных активов и инфраструктуры организации. В целях достижения такого состояния применяются различные меры и средства по защите информации в ИС. Для того, чтобы определить, насколько эффективными являются предпринятые меры и средства необходимо постоянно проводить оценку защищенности ИС. Проблема оценки защищенности ИС прежде всего связана со сложностью определения качественных и количественных показателей применяемых мер. Стандартный подход к оценке заключается в декомпозиции системы защиты информации на отдельные элементы - активы, угрозы и уязвимости, взаимодействия между которыми порождают систему определенных рисков, способных нанести разного рода ущерб организации. Так как активы могут быть весьма разнообразными в зависимости от формы бизнеса и жизнедеятельности предприятия, а кроме того являются, в большинство случаев, статичной частью общей

системы взаимодействия, основной задачей при оценке уровня защищенности информации является идентификация и систематизация угроз и уязвимостей ИБ.

Классификация угроз ИБ

Видом реализации угрозыИБ является одиночное или взаимосвязанное осуществление одного или нескольких событий и инцидентов ИБ, которые ведут к воздействию на конфиденциальность, целостность и доступность объектов защиты организации.[1]

Основными элементами канала реализации угроз ИБ являются:

- источник угроз ИБ - объект, создающий угрозы;
- среда, в которой носители могут распространяться и воздействовать на защищаемые информации;
- носитель –объект который переносит в себе информацию в любом доступном к дальнейшей расшифровке формате.

Основными классификационными признаками угроз ИБ являются:

- источник угроз;
- форма реализации;
- вид нарушаемого свойства;
- особенности уязвимости, которую реализует конкретная угроза;
- объект действия угрозы;
- тип актива, уязвимых к данной угрозе ИБ.

Реализация угрозы может быть направлена на нарушение конфиденциальности, актуальности, целостности и доступности информации (в том числе на нарушение работоспособности ИС или ее элементов). Процесс в общем случае состоит из четырех этапов:

- сбор информации;
- вторжение;
- осуществление несанкционированного доступа;
- ликвидация следов несанкционированного доступа.

Связь уязвимостей и угроз ИБ

Условием реализации угрозы безопасности, обрабатываемой в системе информации, может быть недостаток или слабое место в информационной системе. Угроза характеризуется наличием уязвимостей. Уязвимость информационной системы - свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Необходимо своевременно предпринимать действия по обнаружению и устранению уязвимостей ИС на всех уровнях защиты информации. Если уязвимость соответствует угрозе, то существует риск нарушения информационной безопасности.

Источники угроз используют уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны действия источников угроз по активизации тех или иных уязвимостей, не связанные со злым умыслом.

Каждой угрозе могут быть сопоставлены различные уязвимости, устранение или существенное ослабление которых влияет на вероятность реализации угроз ИБ.

Подходы к классификации уязвимостей ИБ

Уязвимости ИБ можно разделить на объективные, субъективные и случайные.[2]

Объективные уязвимости основываются на особенностях построения и технических характеристиках оборудования и ПО, применяемых на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз ИБ.

Субъективные уязвимости зависят от действий субъектов (например, разработчиков оборудования и ПО, системных администраторов и пользователей организации). Уязвимости данного типа в большинстве случаев устраняются организационными и программно-аппаратными методами.

Случайные уязвимости обуславливаются особенностями окружающей объект информатизации среды и непредвиденными обстоятельствами. Многие из факторов, обеспечивающих наличие таких уязвимостей ИС, в целом предсказуемы, но полное их устранение либо невозможно, либо затруднено и достижимо только при проведении целого комплекса организационных и инженерно-технических мероприятий.В любом случае, уязвимости могут появиться в информационной системе на одном из некоторых этапов её жизненного цикла, один из способов классификации уязвимостей построен по этому признаку. Эта классификация выделяет уязвимости проектирования, уязвимости реализации и уязвимости эксплуатации [3].

Первый тип предполагает уязвимость, заложенную в самом проекте объекта, и не существует способов его реализации и эксплуатации, исправляющих данную уязвимость, например неспособность протокола TCP/IP обрабатывать количество запросов, превышающее определенный предел, приводит к отказу в обслуживании целевого сервера.

Второй тип предполагает уязвимость, появившуюся при некорректном исполнении объекта, например, программная ошибка или некачественное исполнение аппаратной части, банальный брак.

Уязвимости третьего типа появляются, когда должным образом не осуществляется обслуживание объекта.

Чаще всего обнаруживаются и используются уязвимости второго и третьего типов. Первый тип сложен для обнаружения и сложен (порой невозможен) для устранения. Второй тип довольно сложен для обнаружения и прост для устранения. Третий тип прост для обнаружения и устранения.

Методическими документами установлено, что любая угроза в общем виде описывается через возможности нарушителя, используемые нарушителем уязвимости, а также предполагаемый результат реализации угрозы, выраженный в нарушении свойств информационной безопасности.

При этом угроза признается актуальной при наличии возможностей у злоумышленника путей осуществления этой угрозы с использованием слабых мест в системе защиты информации. Таким образом, качество и полнота выявления угроз безопасности информации зависят от качества оценки возможностей нарушителя по реализации этой угрозы и полноты оценки и анализа уязвимостей.

Оценка возможностей нарушителя осуществляется в соответствии с базовыми моделями угроз безопасности информации, утвержденными ФСТЭК России. В основе классификации уязвимостей ИС используются следующие классификационные признаки [4]:

- область происхождения уязвимости;
- типы недостатков ИС;
- место возникновения (проявления) уязвимости ИС.

К уязвимостям ИС по области происхождения относятся:

- уязвимости архитектуры;
- уязвимости кода;
- уязвимости конфигурации;
- многофакторные уязвимости;
- организационные уязвимости.

Среди уязвимостей ИС по типам недостатков ИС можно выделить уязвимости, связанные:

- с неправильной настройкой параметров ПО;
- с неполнотой проверки вводимых (входных) данных;
- с возможностью внедрения команд операционных систем;
- с внедрением произвольного кода;
- с переполнением буфера памяти и др.

Уязвимости ИС по месту возникновения (проявления) подразделяются на следующие типы:

- в общем (общесистемном) программном обеспечении;
- в прикладном программном обеспечении;
- в специальном программном обеспечении;
- в технических средствах;
- в сетевом (коммуникационном, телекоммуникационном) оборудовании;
- в средствах защиты.

В настоящее время наиболее полный перечень уязвимостей хранится в базе данных уязвимостей ФСТЭК России. В данном документе используется следующая система классификации (табл.1):

Таблица 1. Порядок описания уязвимостей базы данных ФСТЭК России

Элемент описания уязвимости	Содержание
Наименование уязвимости	Текстовая информация об уязвимости, на основе которой возможно установить причину и (или) последствия уязвимости.
Идентификатор уязвимости	Номенклатурное значение, включающее код базы данных уязвимостей, год выявления уязвимости и порядковый номер уязвимости, выявленной в текущем году.
Краткое описание уязвимости	Текстовая информация об уязвимости и возможностях ее использования.
Наименование ПО и его характеристики	Текстовая информация о наименовании ПО, его версии, вендоре
Операционные системы и аппаратные платформы	Операционная система, под управлением которой функционирует программное обеспечение с обнаруженной уязвимостью
Тип ошибки и его идентификатор	Описание ошибки в соответствии с общим перечнем ошибок CWE
Класс уязвимости	Определяется один из принятых классов: уязвимость кода, уязвимость архитектуры или многофакторная уязвимость
Оценка уязвимости	Определение общего вектора и уровня опасности уязвимости в соответствии с общей системой оценки уязвимостей (CVSS)

Возможные меры по устранению уязвимости	Рекомендации по устранению уязвимости. Чаще всего предлагаются производителем ПО
Статус уязвимости	Для корректной оценки требуется подтверждение наличия уязвимости производителем ПО
Способ эксплуатации	Каким образом будет использована уязвимость и какие действия можно производить с ПО при её использовании
Способ устранения и информация об устранении	Актуальный путь решения указанной проблемы. Чаще всего уязвимость устраняется разработчиком и способ устранения сводится к обновлению программного обеспечения
Ссылки на источники	Ресурсы, на которых указана информация об уязвимости и способах её устранения
Идентификаторы других систем описаний уязвимостей	Идентификаторы уязвимости в других системах описаний.
Прочая информация	Текстовая информация, которая позволяет дополнить общую информацию об уязвимости:

Способы оценки угроз и уязвимостей.

Методы, которые могут применяться для оценки уровня защищенности, реализуют как качественные, так и количественные подходы к оценке защищенности ИС. Применение количественных и/или качественных методов зависит от конкретной ситуации, доступности достоверных данных и потребностей организации, связанных с принятием решений по защите информации.

Особенно актуальна задача оценки уровня защищенности ИС на этапе эксплуатации ИС. На этапе эксплуатации количественные методы реализуются на основе получения соответствующих данных о текущей конфигурации и реализуемой политике безопасности. Качественные требуют привлечения экспертных решений. В случае применения качественных методов требуется разработки определенного набора показателей и критериев, позволяющих с достаточной степенью достоверности оценить реальный уровень текущего состояния безопасности ИС.

Наиболее эффективным является подход, обобщающий определенные группы угроз и уязвимостей по ущербу, наносимому ими активам организации. Такой способ реализуется в подавляющем большинстве существующих методик оценки риска.В настоящее время наиболее применимыми являются следующие методики анализа и оценки рисков информационной безопасности[5]:

CCTARiskAnalysisandManagementMethod (CRAMM) появилась одной из первых на рынке анализа уязвимостей. В ее основе заложены процедуры определения как качественного анализа рисков, так и количественного. В данной методике имеется два способа проведения оценки анализа рисков: обеспечение базового уровня информационной безопасности и полный анализ рисков.

Facilitated Risk Analysis Process (FRAP) представляет собой методику для качественной оценки рисков. Поиск и анализ уязвимостей состоит из определения списка активов, которые являются наиболее уязвимыми, идентификации угроз, анализ риска для каждого из активов. Под анализом имеется ввидучастота возникновения риска, а также масштаб ущерба, который понесет организация в случае реализации этого риска. На основе этих параметров, задается матрица определения уровня риска.

RiskAdvisor - ПО, представленное компанией MethodWare.Данная методика состоит из пяти этапов:описание контекста, описание рисков, описание угроз, оценка ущерба, анализ проделанной работы. На завершающем этапе методики формируется детализированный отчет, составляется граф рисков.

RiskWatch - решение, реализующее оценку рисков в четыре итерации. На первом шаге происходит определение предмета исследования.На втором шаге происходит детальное описание всех составляющих системы. Для количественной оценки рисков на третьем шаге необходимо сопоставить угрозы и уязвимости с возможными потерями. Составление отчетности завершает цикл алгоритма, происходит сбор информации, полученной на первом, втором и третьем шаге.

ГРИФ представляет собой средство для комплексного анализа уязвимостей и выявления рисков. В основе данной методики лежит два различных приема, позволяющих оценивать риски ИБ: «модель угроз и уязвимостей» и «модель информационных потоков».На начальном этапе происходит подробное описание информационной системы. Определяются элементы системы, которые оперируют ценной информацией, а также защитные средства и группы пользователей с различными правами доступа. Собрав всю необходимую информацию, можно построить подробную архитектурную модель ИС компании. На основе этой модели уже можно проводить анализ уязвимости информации и составлять оценку рисков.

Особо нужно отметить, что для получения максимально достоверной картины, отражающей реальное положение вещей, разумно использовать

сразу несколько методов оценки. Выбор метода оценки защищенности будет зависеть от возможностей организации и целей защиты информации. Результатом проведения оценки реального уровня защищенности будет информация, которая является основой для принятия решения по обеспечению заданного уровня безопасности информации.

Список литературы:

1. Методика определения угроз безопасности информации в информационных системах. - ФСТЭК России, 2015
2. ГОСТ Р 56545 - 2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. Введ. 2016-04-01. М.: Стандартинформ, 2015. 22 с.
3. Муханова А., Ревнивых А.В., Федотов А.М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестник НГУ. Серия: Информационные технологии. 2018. №2.
4. Зубарев И.В., Жидков И. В., Кадушкин И.В., Медовщикова С. Алексеевна Уязвимости информационных систем // Информационные и математические технологии в науке и управлении. 2016. №3.
5. Баранова Елена Константиновна. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. №1 (9)

УДК 004.896

Москвичев Михаил Евгеньевич
направление Информатика и вычислительная техника(магистратура),
гр.ИВТм-11

Научный руководитель
Васяева Наталья Семеновна,
канд.тех. наук, кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственных технологический университет», г. Йошкар-Ола

РАСПОЗНАВАНИЕ ЛИЦ УЧАСТНИКОВ ДЛЯ РЕГИСТРАЦИИ И АВТОРИЗАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ СОРЕВНОВАНИЙ КОМПЛЕКСА «ГТО»

Цель работы – повышение эффективности всей информационной системы организации и проведения фестивалей соревнований комплекса «ГТО» за счёт ускорения процесса регистрации и авторизации спортсменов с помощью сервиса распознавания лиц, который будет использоваться в общей совокупности всей системы.

Принять участие в фестивале “ГТО” может совершенно любой человек, всего есть 11 возрастных ступеней: начиная с 1, в которую входят дети от 6 лет, и заканчивая 11, в которую входят люди от 70 лет и старше. В данный момент все соревнования проводятся вручную: судьи должны следить за огромным количеством спортсменов, записывать их результаты, секретари - зарегистрировать всех, а в дальнейшем и перевести значения каждого из спортсменов по каждому соревнованию в 100-бальную шкалу, подсчитать результаты и присвоить знак: бронзовый, серебряный или золотой. В большинстве случаев на таких соревнованиях есть несколько судей и пара-тройка секретарей и сотни спортсменов. Так как вся работа бумажная и зависит только от людей - часто возникновение ошибки при регистрации неизбежно: например, неправильные инициалы, возраст или принадлежность к команде, в результатах многих видов спорта, при пересчете в 100-бальную шкалу. Если выбирать между увеличением количества секретарей, судей, следовательно увеличением количества расходов и выплат на их содержание, и разработкой сервиса проведения фестивалей “ГТО”, то выгода очевидна. Освободившиеся средства станут отличной возможностью сохранения бюджета и направление его в сторону развития и быстродействия проведения фестивалей.

Как уже упоминалось, количество участников может достигать тысячи и более человек, каждый из них должен пройти регистрацию перед сдачей нормативов по видам спорта. Чтобы ускорить этот процесс для самих спортсменов, а также исключить возможность возникновения ошибок при регистрации для секретарей было придумано решение автоматизировать этот процесс. Проще говоря, данный микросервис распознавания лиц позволяет выполнять две основные задачи: регистрацию спортсменов, участвующих в мероприятии, а также оперативный доступ к редактированию результатов каждого участника, что значительно экономит затрачиваемое время выполнения этих операций секретарём и снижает риск возникновения ошибок и конфликтов до минимума.

Весь микросервис представляет из себяbackend-сервер, к которому обращаются браузерный сайт и мобильное приложение через route (маршруты).

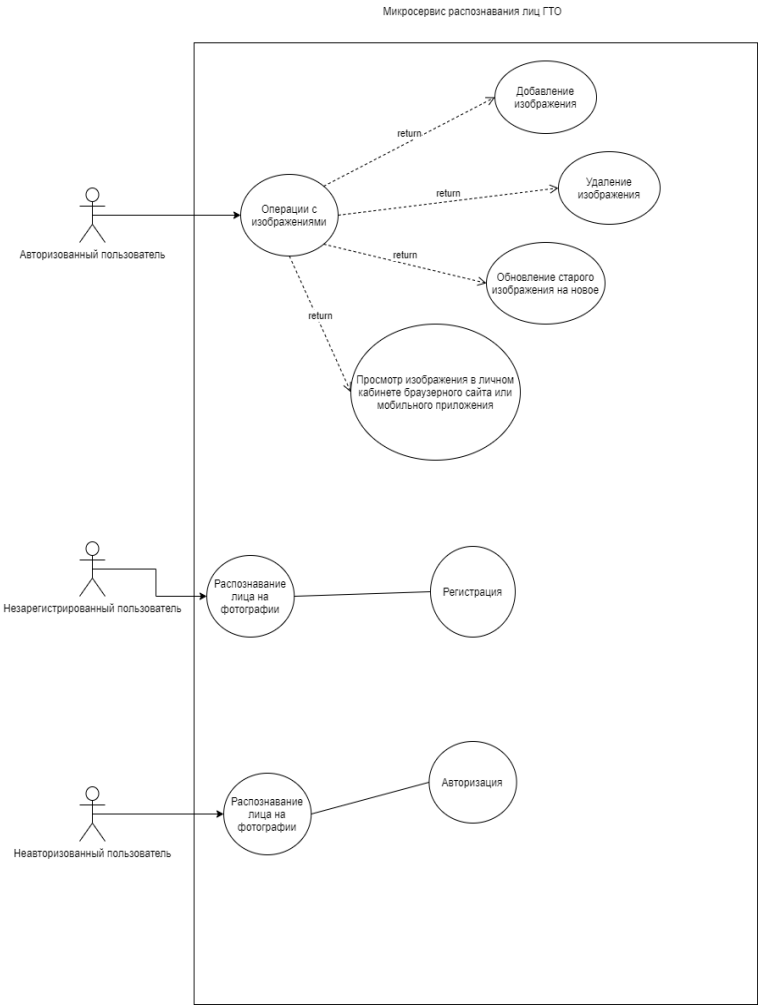


Рис. 1. Диаграмма использования системы распознавания лиц

При входе в систему делается фотография пользователя через браузерный сайт или мобильное приложение, далее происходит распознавание пользователя. Если пользователь не зарегистрирован, то ему предлагается зарегистрироваться с последующей авторизацией и входом в систему. Если же пользователь уже зарегистрирован в системе, то он авторизуется и ему становятся доступны следующие

операции с фотографиями: просмотр установленной фотографии в личном кабинете, добавление фотографии, обновление старой на новую или же вовсе удаление фотографии.

На рисунке 1 представлены все варианты использования системы.

Выводы

Использование технологии распознавания лиц в проведении и организации фестивалей «ГТО» вполне оправданно. Во-первых, вся система в общем не имеет аналогов на рынке программ и является единственной в цифровом сегменте по предоставляемому функционалу. Во-вторых, регистрация участников на основе распознавания лиц также уникальна и не внедрялась ранее в категории спорта в целом.

Список литературы:

1. Роберт Мартин. Чистая архитектура. Искусство разработки программного обеспечения.: Пер. с англ. – СПб.: Питер, 2018. – 352 с
2. Роберт Мартин. Чистый код: создание, анализ и рефакторинг. Библиотека программиста.: Пер. с англ. – СПб.: Питер, 2010. – 464 с
3. Описание REST системы, принципы и методы [Электронный ресурс]. - Режим доступа: https://restfullapi.net/
4. Описание всей процедуры проведения соревнований ГТО, а также общие положения [Электронный ресурс]. - Режим доступа: https://www.gto.ru/

УДК 004.896

Мошкин Никита Андреевич
направление Конструирование и технология электронных средств(магистратура), гр. ЭВСм-21

Научный руководитель
Петухов Игорь Валерьевич,
д-р технических наук, профессор
ФГБОУ ВО «Поволжский государственный технологический университет»,
г. Йошкар-Ола

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СПОСОБОВ ОПТИМИЗАЦИИ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

Цель работы – обзор существующих подходов к поискуоптимальных наборовгиперпараметровглубоких нейронных сетей.

В настоящее время, глубокие нейронные сети решают широкий спектр задач, которые в отдельных случаях показывают результат выше, чем человек. Практическая реализация ГНС стала возможна из-за снижения стоимости вычислительного оборудования, повышения эффективности оптимизационных алгоритмов и появления больших объемов данных для обучения ГНС. Но, в то же время, остаются сложности в части тонкой настройки ГНС, в частности, подбора оптимальных гиперпараметров: **количество нейронов**, **количество слоёв**, **количество слоёв для обучения, функция активации** и **скорость обучения**. В основном, сам подбор осуществляется на основе опыта разработки или обычного перебора. Можно отметить то, что оптимальный набор гиперпараметров весьма существенно влияет на эффективность модели машинного обучения[1]. Для подбора гиперпараметров существует набор эвристических алгоритмов,таких как**поиск по решетке**, **случайный поиск (метод Монте-Карло)**и **генетический алгоритм**. Рассмотрим данные методы по отдельности.

ПОИСК ПО РЕШЕТКЕ

Традиционным методом осуществления оптимизации гиперпарамеров является поиск по решётке (или вариация параметров), который просто делает полный перебор по заданному вручнуюподмножеству пространства гиперпараметров обучающего алгоритма. Поиск по сетке является очень традиционной техникой для реализации гиперпараметров. Это грубая сила всех комбинаций. Поиск по решётке должен сопровождаться некоторым измерениемпроизводительности, обычно измеряемой посредством перекрёстной проверки на тренировочном множестве, или прогонкой алгоритма на устоявшемся проверочном наборе.

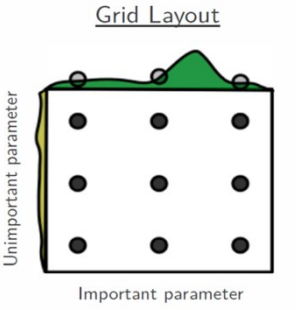


Рис 1. Поиск по решетке

Преимущества:

- Относительно простая реализация
- Проход по решетке легко параллелизуем
- Надежен при проходе в пространстве поиска малой размерности

Недостатки:

- “Решение в лоб”
- Для прохода по пространству поиска большой размерности появляется необходимость в мощном аппаратном обеспечении

СЛУЧАЙНЫЙ ПОИСК (МЕТОД МОНТЕ-КАРЛО)

Данный алгоритм произвольно выбирает пространство поиска и оценивает наборы из заданного распределения вероятностей. Например, вместо того, чтобы пытаться проверить все 100 000 выборок, мы можем проверить 1000 случайных параметров. Случайный поиск может превзойти поиск по решётке, особенно в случае, если только малое число гиперпараметров оказывает влияние на производительность алгоритма обучения машины [2]. В этом случае говорят, что задача оптимизации имеет низкую внутреннюю размерность. Случайный поиск также легко параллелизуем и, кроме того, позволяет использовать предварительные данные путём указания распределения для выборки случайных параметров

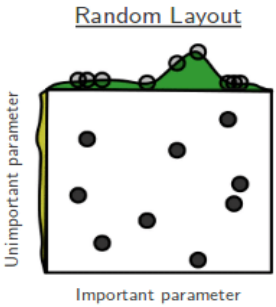


Рис 2. Случайный поиск

Преимущества:

- По аналогии с поиском по решетке, случайный поиск также прост в реализации и легко параллелизуем.
- Превосходит поиск по решетке в случаях, если не все гиперпараметры одинаково важны для производительности модели ГНС.

Недостатки:

- В классической версии алгоритма не использует информацию из предыдущих экспериментов для выбора следующего набора гиперпараметров.
- Трудно предсказать результаты поиска в последующих экспериментах.

ГЕНЕТИЧЕСКИЙАЛГОРИТМ

Эволюционная оптимизация — это методология для глобальной оптимизации неизвестных функций с шумом.Эволюционная оптимизация используется для оптимизации гиперпараметров для статистических алгоритмов обучения машин, автоматического обучения машин, для поиска архитектуры глубоких нейронных сетей, а также для формирования весов в глубоких нейронных сетях. При оптимизации гиперпараметров эволюционная оптимизация использует эволюционные алгоритмы для поиска гиперпараметров для ГНС, в состав которых входит генетический алгоритм. Данный алгоритм работает следующим образом: создаетсяначальная подпопуляция

(список случайно сгенерированных кортежей гиперпараметров), далее происходит оценивание данных кортежей (расчет функции их пригодности), затем кортежи ранжируются по их относительной пригодности, по итогу кортежигиперпараметровс наихудшей производительностью меняются на новые, образованные путем скрещивания и мутации. Повторяем эти шаги, пока не добьемся удовлетворительной производительности модели ГНС, или до тех пор, пока производительность не перестанет улучшаться.

Преимущества:

- Простота реализации
- ГА не требует информации о поведении функции
- ГА относительно стоек к попаданию в локальные минимумы функций
- Эффективное распараллеливание
- Работает заведомо не хуже абсолютно случайного поиска

Недостатки:

- Непросто смоделировать ГА для нахождения всех решений задачи
- Не для всех задач удается найти оптимально кодирование параметров
- Неэффективно применять ГА в случае оптимизации функции, требующей большого времени на вычисление [3]

Выводы

Из проведенного аналитического обзора можно сделать вывод, что каждый из перечисленных методов обладает своими преимуществами и недостатками.Но, в то же время, для дальнейшего изучения и применения для решения задачи оптимизации подбора гиперпараметров ГНС, генетический алгоритм кажется более перспективным, ввиду простотыего реализации, стойкости к попаданию в локальные минимумы функций оптимизации, а также пригодности к решению крупномасштабных проблем оптимизации.

Список литературы:

1. Li, L., Jamieson, K., DeSalvo, G., Rostamizadeh, A., & Talwalkar, A. (2017). Hyperband: A Novel Bandit-Based Approach to Hyperparameter Optimization. J. Mach. Learn. Res., 18, 185:1-185:52.
2. Bergstra, J., &Bengio, Y. (2012). Random Search for Hyper-Parameter Optimization. J. Mach. Learn. Res., 13, 281-305.
3. Панченко, Т. В. Генетические алгоритмы [Текст]: учебно-методическое пособие / под ред. Ю. Ю. Тарасевича. — Астрахань: Издательский дом «Астраханский университет», 2007. — 87 [3] с.

УДК 004.031.2

Осокина Екатерина Владимировна
направление Информатика и вычислительная техника(магистратура),
гр.ИВТм-13

Научный руководитель
Смирнов Алексей Владимирович,
канд.тех. наук, доцент, кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственных технологический университет»,
г. Йошкар-Ола

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АКУСТИЧЕСКОГО ТРАКТА ЭХОЛОТА

Цель работы – Разработать методику и соответствующий программный модуль для определения передаточной характеристики эхолотов методом площадей (метод Симою).

Эхометрирование - это один из методов определения уровня жидкости в затрубном пространстве скважины. Схематическое изображение скважины показано на Рис 1.

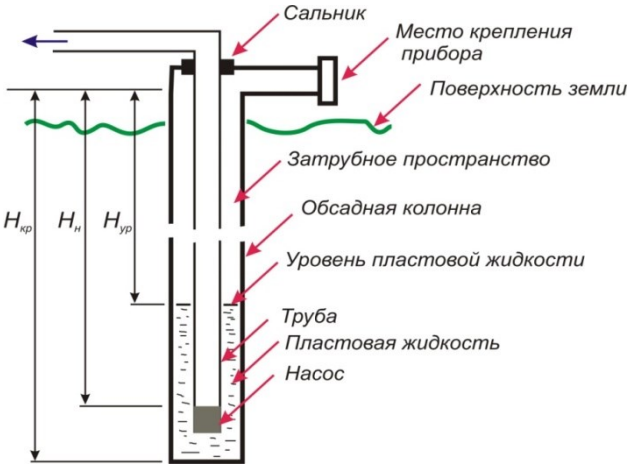


Рис 1. Схематическое изображение нефтедобывающей скважины
$H_{ур}$ – текущий уровень затрубной жидкости
$H_{н} и H_{кр}$ - уровни подвеса насоса и кровли скважины

Исследование производится с помощью эхолота - прибора для измерения положения уровня жидкости в скважине. В настоящее время

применяются различные типы эхолотов, но принцип работы всех приборов идентичен.

Определение уровня жидкости осуществляется акустическим методом путем измерения времени прохождения акустического сигнала от устья скважины до границы раздела фаз «газ-жидкость». По величине измеренного времени и введенному значению скорости распространения акустического сигнала производится вычисление уровня. Устройство приема акустических сигналов присоединяется к патрубку затрубного пространства исследуемой скважины, и в газовую среду скважины генерируется акустический сигнал.

Сгенерированный и отраженный акустический сигналы регистрируются в виде эхограммы и запоминаются в оперативной памяти блока регистрации, соединенного с устройством приема акустического сигнала. По зарегистрированной эхограмме микропроцессор блока регистрации выделяет отраженные акустические сигналы и определяет время прихода отраженного сигнала [1].

В результате анализа микрофонного узла и усилительного тракта эхолотов можно выделить следующие характерные области эхограммы (Рис. 2)

- область акустического шума (1);
- область нарастания стартового импульса, вызванного резким изменением давления при срабатывании клапана (2);
- область резонансных явлений системы при окончании возмущения, вызванного изменением давления при срабатывании клапана (3);
- область нахождения отклика (4).

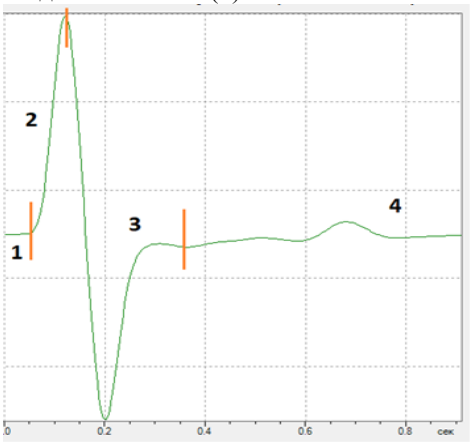


Рис. 2. Характерные области эхограммы.

Учитывая особенности работы микрофонного тракта и усилителя заряда, а также учитывая, что резонансные явления акустического тракта эхолота много ниже по временным характеристикам, эквивалентным резонансной частоте, относительно времени срабатывания клапана, можно предположить следующие допущения:

- акустический тракт эхолота представляет собой полосовой фильтр[2];
- изменение давления при срабатывании клапана можно считать эквивалентом функции Хевисайда (функции включения);
- область 2 эхограммы можно считать переходной характеристикой эхолота.

Таким образом, область нарастания стартового импульса (область эхограммы 2) может быть выбрана в качестве рабочей области переходной характеристики акустического тракта эхолота при решении задачи построения передаточной характеристики акустического тракта эхолота.

При аналитическом исследовании систем автоматического регулирования составление дифференциального уравнения объекта регулирования связано со значительными трудностями. В ряде случаев сложность полученного уравнения делает неудобным его практическое использование. В то же время обычно имеется возможность экспериментального определения реакции системы на заданное возмущение и возникает задача определения передаточной функции системы по экспериментальным кривым [3].

Метод «площадей» (Метод Симою) позволяет определить коэффициенты передаточной функции регулируемого объекта (или любого другого линейного элемента системы автоматического регулирования) [4].

Методика определения передаточной характеристики эхолотов сводится к следующему порядку действий:

1. Регистрация эхограммы эхолотом определенной модификации при определенных режимах работы (давление, температура).
2. Выделение области стартового импульса эхограммы в качестве данных переходной характеристики эхолота.
3. Определение коэффициентов передаточной характеристики эхолота методом «площадей».
4. Определение достоверности полученных результатов.

Выводы

Произведенные теоретические и практические исследования могут дать полное представление результатов и выводов математической

модели акустического тракта эхолотов. Рассмотрено построение передаточной характеристики методом площадей (Симою). Разработана методика определения передаточной характеристики методом площадей (Симою). Разработан программный модуль определения математической модели акустического тракта эхолота.

Список литературы:

1. Оператор по исследованию скважин: учебное пособие / Санду С.Ф. – Томск: Изд-во Томского политехнический университета, 2015. - 120 с. URL.: https://studref.com/465211/geografiya/opredelenie_staticheskogo_dinamicheskogo_urovnya_zhidkosti_dobyvayuschey_skvazhine.
2. Полосовой фильтр и режекторный фильтр [Электронный ресурс]. – URL.: https://lib.qrz.ru/node/4553
3. Симою М.П. Определение коэффициентов передаточных функции линеаризованных звеньев и систем авторегулирования, Автомат.и телемех. / М.П. Симою. - 1957, том 18 выпуск 6, 514 528.
4. Стефани Е.П. Сборник задач по основам автоматического регулирования теплоэнергетических процессов : учебное пособие для ВУЗов / Е.П. Стефани. – М., “Энергия” , 1973. – 336с.

УДК 004

Павлова Диана Дмитриевна
направление Информационная безопасность автоматизированных систем (специалитет), гр. БИ-51

Научный руководитель
Александров Александр Петрович
доцент кафедры Информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Трудно представить современный мир без системы электронных платежей. Только в нашей стране за последние три года число электронных платежей выросло более чем на 80%.Электронные платежные системы служат для расчетов между пользователями и организациями при покупке или продажи товаров и услуг в Интернете.

Идея электронных платежных систем впервые появилась в 80-е годы XX века. Её основой послужили изобретения Дэвида Шаума, который основал в США компанию "DigiCash". Основной задачей этой компании

было внедрение технологий обращения электронных денег. Замысел был довольно прост. В системе осуществляются операции с электронными монетами, представляющими собой файлы-обязательства эмитента с его электронной подписью. Предназначение подписи было аналогично предназначению элементов защиты бумажных купюр

Термин электронная платежная система можно расшифровать как технологию (если говорить о реализации, то сервис), представляющая собой совокупность методов, договоренностей и подтехнологий,позволяющая производить расчеты между финансовыми организациями, бизнес-организациями и интернет-пользователями при покупке-продаже товаров и за различные услуги через Интернет.[1]

Безопасность — это одна из самых серьезных проблем, если говорить об электронной коммерции. Такие случаи, как кража личных данных и мошенничество с платежами, по-видимому, растут с каждым днем в сегменте электронной коммерции. Для владельцев магазинов крайне важно обеспечить своим покупателям безопасную и безопасную среду для покупок. Несанкционированные действия в сфере систем электронных платежей могут повлечь за собой нарушения в работе электронно-вычислительных машин и привести систему электронных платежей, банк, а впоследствии и рыночную экономику к провалу. Проблемами защиты данных в системах электронных платежей, разработкой современных технических и клиентских средств защиты, а также усовершенствованием антивирусных систем сегодня занимаются многие отечественные и иностранные специалисты. Существует огромное количество исследований и разработок, в области защиты систем электронных платежей, но в то же время из-за постоянного развития технологий возникают новые проблемы, которые необходимо решать новыми способами.

По статистике, чаще всего подвергаются атакам следующие системы: сервера баз данных (30%), серверы приложений (12%),терминалы (32%), веб-серверы (10%). На рабочие станции, серверы аутентификации, серверы резервного копирования и прочее приходится около 10%. Из данной статистики можно увидеть, что именно с сайтов и приложения подвергаются атаке, так как через их уязвимости чаще всего становится возможным получение доступа к данным[2].

Безопасность платежных систем обеспечивают:

1) Безопасные интернет соединения (зашифрованные соединения). Для безопасного проведения интернет платежей наличие SSLсертификата не является достаточным условием. Лишь

комплексный подход, который сертифицирован по современным международным стандартам, позволяет обеспечить безопасность обработки интернет-платежей на самом высоком уровне.

2) Клиентская защита. Существуют меры безопасности для клиентской защиты:

- Логин и пароль доступа для входа в систему проходит тестирование на сложность;

- Комбинация номера банковской карты, срока действия, имени держателя карты, CVV/CVC кодов;

- Виртуальная карта. Возможность создания виртуальной карты, дублирующей основную, для проведения интернет-платежей;

3) Техническая защита.Привязка платежного сервиса к фиксированному IP-адресу и телефонному номеру клиента и осуществление клиентского доступа в систему по зашифрованному протоколу HTTPS/SSL помогают обеспечить безопасность платежных систем. Также возможность использования виртуальной клавиатуры для набора данных идентификации противодействуют перехвату личных данных.

4) Сертификация платежных систем. СтандартPaymentCardIndustryDataSecurityStandard (PCIDSS) былразработанСоветом по стандартам безопасности данных индустрии платежных карт, который был учрежден международными платежными системами Visa, MasterCard, AmericanExpress, JCB. Иными словами, это документация со списком критериев, которому должен удовлетворять сервис, если он как-то управляет такими вещами, как номер карты, срок её действия и CVV-код. Чтобы получить эту сертификацию компании/организации должны проходить каждый год[3].

В последние годы с увеличением преступности в сфере электронных платежных систем появляются все больше уязвимостей с помощью которых мошенники получают возможность доступа к вашим личным данным. С точки зрения информационной безопасности в системах электронных платежей существуют следующие уязвимые места:

- Пересылка платежных и других сообщений между банком и клиентом и между банками;

- Обработка информации внутри организаций отправителя и получателя сообщений;

- Доступ клиентов к средствам, аккумулированным на счетах.

- Одним из наиболее уязвимых мест в системе электронных платежей является пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом.

Для защиты при пересылке платежных систем сообщений внутренние системы организаций отправителя и получателя должны быть приспособлены для отправки и получения электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем), а также длявзаимодействие отправителя и получателя электронного документа должно осуществляться непосредовано – через канал связи.

Для обеспечения функций защиты информации на отдельных узлах системы электронных платежей должны быть реализованы следующие механизмы защиты:

- управление доступом на оконечных системах;
- контроль целостности сообщения;
- обеспечение конфиденциальности сообщения;
- взаимная аутентификация абонентов;
- невозможность отказа от авторства сообщения;
- гарантии доставки сообщения;
- невозможность отказа от принятия мер по сообщению;
- регистрация последовательности сообщений;
- контроль целостности последовательности сообщений.

Качество решения указанных выше проблем в значительной мере определяется рациональным выбором криптографических средств при реализации механизмов защиты.

Также для безопасного использования электронных платежных систем стоит соблюдать некоторые правила: никому не сообщайте ваш пароль, а лучше использовать одноразовые пароли(усиленную авторизацию); проверяйте, что соединение установлено именно с адресом платежной системы или интернет-банка; проверяйте, что соединения действительно происходит в защищенном режиме SSL; используйте программное обеспечение из проверенных и надежных источников, выполняйте регулярные обновления.[2]

Заключение

Цифровые платежи довольно просто и удобны в использовании. Но не стоит забывать, что интернет является целью для мошенничества и преступности, поэтому пользователь должен соблюдать меры предосторожности, прежде чем совершать покупки и разглашать личную и финансовую информацию.

Список литературы:
1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб: Питер,960 с, 2012;
2. ИвановМ.А., МихайловД.М., Защита информации в электронных платежных ситемах. Москва 2011;
3. Пилецкая А. В. Безопасность платежей в электронной коммерции // Молодой ученый. — 2019. — №51. — С. 254-255.

УДК 622.69

Перевозчикова Надежда Михайловна
направление Эксплуатация транспортно-технологических машин и комплексов (магистратура), гр. ЭТМ-22

Научный руководитель
Костромин Денис Владимирович
к.т.н., доцент каф. ЭМиО
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИСПОЛЬЗОВАНИЕ ZULU ГИС В ООО «ГАЗПРОМ ГАЗОРАСПРЕДЕЛЕНИЕ ЙОШКАР-ОЛА»

Цель работы:Организация поставки программного обеспечения для электронной карты и гидравлических расчетов.

Актуальность работы заключается в том, чтобы экономить рабочее время ИТР за счет исключения ручной обработки информации на бумажных носителях; получение собственных вероятностных оценок отказов оборудования при общей оценке надежности инженерных сетей;быстрая адаптация молодых специалистов; существенное сокращение времени на подготовку исходных данных для расчета режимов.

Использование Zulu ГИС в ООО «Газпром газораспределение Йошкар-Ола» ведется с июля 2008 года.

Для решения проблемы Общество на основе программы ГИС ZULU начало создавать свою геоинформационную систему.

Предполагалась сопоставить графические и семитические источникиинформации. Функционал ГИС ZULU оказалась намного шире, чем ожидалось:

-систематизацию на топографической основе информации об объектах сетей газоснабжения, застройке, дорожной сети, охранных зонах, полосах и участках землеотвода;

-совместное представление трасс трубопроводов и других инженерных коммуникаций на цифровой топооснове;

-удобный инструментарий для инвентаризации объектов газового хозяйства;

-оперативное получение информации об объектах сетей газоснабжения в любой части территории;

-информационную поддержку планирования работ по реконструкции и ремонту сетей газоснабжения с учетом других инженерных коммуникаций;

-ведение электронных паспортов на все объекты системы газораспределения и газопотребления;

-выполнение гидравлических расчетов по готовой модели газопроводов от ГРС (источника) до конечных потребителей, моделирование новых сетей;

-активное использование при технологическом присоединении на всех этапах (от выдачи ТУ до пуска газа);

-использование результатов ГИС для эксплуатации (маршрутные карты, планшеты АДС, карты в АДС и др.)

На данный момент с помощью ГИС создаются маршрутные карты и планшеты АДС, технологические схемы, выполняются гидравлическиерасчеты, расчеты пропускной способности газопроводов, а так же решаются коммутационные задачи по поиску отключающих устройств при повреждениях газопроводов с выводом количества отключенных абонентов, выполняются расчеты объема газа в баллоне. ГИС дает возможность вывести на печать любую часть карты с произвольным масштабом. Так же к ГИС привязаны базы данных газопроводов, потребителей, запорной арматуры, позволяющие просматривать данные простым кликом мыши на объекте карты.

ГИС активно используется многими службами и отдела Общества. На данный момент разработчиком системы выпущено приложение ZuluGIS для мобильных устройств, что является очень удобным для сотрудников, которые выезжают на места и могут видеть картину «в живую». Специалисты ООО «Политерм» оперативно решают возникающие вопросы, и, при необходимости, даже выпускают обновления программы. В некоторых случаях вопросы решаются в течение одного часа.

Сотрудниками Общества ведется работа по актуализации карт, баз данных газопроводов и потребителей. Кроме этого ведется работа по внесению в ГИС новых участков газопроводов.

Создание единого информационного пространства ООО "Газпром газораспределение Йошкар-Ола" сетей газоснабжения позволяет существенным образом повысить организованность и управляемость.

Выводы:

-поиск объектов по атрибутивным параметрам, "опросом" через карту в режиме реального времени многочисленных баз данных, содержащих изменяемую информацию;

-отображение паспортно-технологической информации об объектах газового хозяйства;

-контроль и согласование проведения ремонтных и диагностических работ на объектах;

-выявление участков с предельной загрузкой в системах газопроводов – используется руководителями для принятия решений о своевременном ремонте, замене, реконструкции трубопровода и т. д.;

-обеспечение доступа к единой базе данных ГИС ГС технического отдела, аварийной службы, центральной диспетчерской, группы режимов и т.п.;

-информационная поддержка при подготовке технических условий на подключение и согласование проектов;

-анализ и графическое отображение параметров сети при подключении (отключении) потребителей, проведении регламентных ремонтных и аварийно-восстановительных работ.

-планирование мероприятий по развитию газораспределительного комплекса региона, а также обеспечить высокий уровень диспетчеризации и автоматизации процесса транспортировки газа.

Область применения описываемой информационной системы охватывает газораспределительные сети всех категорий давления в масштабе области, района, населенного пункта, сети газораспределения предприятий и площадок.

Список литературы:

1. Бугаевский, Л.М. Геоинформационные системы - М.: Златоуст, 2000.
2. Официальный сайт ООО «Политерм» г. Санкт Петербург. politerm@politerm.com . Дата 23.10.2020 г.
3. Официальный сайт ООО «Газпром газораспределение Йошкар-Ола».https://www.marigaz.ru/. Дата 23.10.2020 г.

УДК 621.396

Порфирьев Александр Игоревич
Направление «Информационная безопасность» (специалитет), гр. БИ-51

Научный руководитель
Сидоркина Ирина Геннадьевна,
д-р техн. наук, профессор, кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ВОПРОСЫ ПРИМЕНЕНИЯ БАНКА ДАННЫХ УГРОЗ ДЛЯ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ

Цель работы – рассмотрение вопросов применения банка данных угроз для определения уровня защищенности.

Методика определения актуальных угроз от ФСТЭК 2008 года не слишком удобна. Но здесь ничего не поделаешь, что есть, с тем и работаем.

Свежие документы от ФСТЭК предписывают в качестве исходных данных для угроз безопасности информации использовать банка данных угроз (БДУ). Сейчас там 213 угроз и список может пополняться.

Здесь сразу же хотелось бы рассказать о плюсах и минусах БДУ. Несомненный плюс – это то, что теперь нет необходимости придумывать и формулировать угрозы самостоятельно, хотя дополнить модель угроз своими угрозами тоже ничего не запрещает. Еще один плюс это прописанный потенциал нарушителя и определенные нарушаемые характеристики безопасности информации для каждой угрозы.

Минусы. Первый минус это ограниченные возможности по сортировке угроз. Когда вы первый раз начинаете делать модель угроз по БДУ, то естественное желание это отсеять угрозы, которые не могут быть актуальны в вашей системе по структурно-функциональным характеристикам. Например, убрать угрозы для виртуальных контейнеров и гипервизоров, потому что в системе не применяется виртуализация или отобрать угрозы для BIOS/UEFI нужно по какой-то причине, а такой возможности нет. Не говоря уже о том, что в БДУ целый ряд достаточно экзотических угроз, связанных, например, с суперкомпьютерами или грид-системами.

Приходится вручную классифицировать эти угрозы, иначе работа очень затрудняется, особенно учитывая то, что угрозы даже по порядку никак не сгруппированы.

Второй минус – описание самих угроз. Нет, где-то все четко и понятно. Но бывает угроза так сформулирована, что нужно голову поломать, чтобы разобраться о чем вообще речь.[1]

Вернемся определению списка актуальных угроз.

Первое, что нужно определить это глобальный параметр – уровень исходной защищенности. Глобальный он потому, что определяется один раз и не меняется от угрозы к угрозе. Чтобы определить уровень исходной защищенности (он же коэффициент исходной защищенности Y1) нужно для семи показателей выбрать одно из значений, которое больше всего подходит для вашей системы.

Таблица 1. Пример списка характеристик и их значений:

технические и эксплуатационные характеристики испдн	Уровень защищенности		
	Высокий	средний	низкий
1. по территориальному размещению:			
Распределенная испдн, которая охватывает несколько областей, краев, округов или государство в целом	-	-	+

Каждому значению соответствует высокий, средний или низкий уровень защищенности. Считаем какой процент у нас получился для показателей с разными значениями. Про высокий уровень исходной защищенности – забудьте, его не бывает. Если «высокий» и «средний» набрали 70% и выше, то определяем средний уровень исходной защищенности (Y1 = 5), если нет, то – низкий (Y1 = 10).

Итак, опасность угроз может быть низкой, средней или высокой, в зависимости от того незначительные негативные, просто негативные или же значительные негативные последствия наступают при реализации угрозы соответственно.

Этот раздел называется «Определение последствий от нарушения свойств безопасности информации (опасность угроз)». Назвали его именно так, потому что, по сути, по определению опасности угроз это является определением последствий, но при согласовании модели угроз, проверяющие могут и не провести эту параллель, а поскольку «определение последствий» должно быть в модели угроз – пишут замечание. [3]

Итак, опасность угроз может быть низкой, средней или высокой, в зависимости от того незначительные негативные, просто негативные

или же значительные негативные последствия наступают при реализации угрозы соответственно.

По данной теме ведутся споры — должна ли опасность угроз определяться один раз и быть константой для всех угроз – или же нет. Методикой это не оговорено, поэтому можно и так и так. Данный подход промежуточный –определяется опасность угроз в зависимости от нарушения конфиденциальности, целостности или доступности при реализации конкретной угрозы.

Негативные последствия не зависят от способа нарушения конфиденциальности, целостности и доступности. Например, если ваши персональные данные утекут в какой-то базе, то вам скорее всего будет неважно каким образом это произошло – с помощью SQL-инъекции или с помощью физического доступа нарушителя к серверу (профессиональный интерес эксперта не в счет). Поэтому определяем три «опасности угроз», для нарушения конфиденциальности, целостности и доступности. Часто они могут совпадать, но все равно в модели угроз лучше отдельно проанализировать. К счастью, в БДУ для каждой угрозы нарушаемые характеристики тоже прописаны. [2]

Выводы

Банк данных сформирован с целью предоставления информационной и методической поддержки государственным структурам и организациям по определению и оценке угроз в информационных (автоматизированных) системах, а также обнаружению, анализу и устранению брешей в ходе создания и эксплуатации инфомационных систем, ПО и средств защиты информации.Банк данных угроз безопасности информации предназначен для заинтересованных органов власти и компаний, которые занимаются созданием и эксплуатацией информационных (автоматизированных) систем, а также разработкой программного обеспечения и средств защиты информационной безопасности.

Основной целью создания банка данных угроз была разработка некой методической базы данных, содержащей сведения об угрозах и уязвимостях. На текущий момент, помимо этой информации, в банке данных хранится методический инструмент, позволяющий операторам коммуникационных систем проводить работы по выявлению и анализу уязвимостей в таких системах.

Список литературы:

1. Банк данных угроз безопасности информации. Эл.ресурс: https://bdu.fstec.ru/threat.

2. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: "Инкомбук", 1997. – 540с
3. Дроботун Е.Б.— Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя. – 2016. – № 3. – С. 42 - 50.

УДК 378.147.88

Пуртов Д.Н.
аспирант ФИиВТ

Научный руководитель
Сидоркина Ирина Геннадьевна,
д-р техн. наук, профессор, кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СПОСОБ СОЗДАНИЯ ГРАММАТИКА ЛИНГВИСТИЧЕСКИХ ПРАВИЛ ДЛЯ ИЗВЛЕЧЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Введение

Поиск ключевой информации зачастую можно свести к поиску определённого слова или фрагмента текста. Именно в этой единице речи текста может содержатся нужная, ключевая информация[1]. Поиск такой единицы информации сводится к решению задачи поиска именованных сущностей (NamedEntityRecognition — NER) — частная задача извлечения информации, состоит в поиске единиц текста в слабоструктурированных текстах (как правило на естественных языках).Как правило подобную задачу решают различными методами,основанными на грамматиках лингвистических моделей языков и статистическими моделями. [2]

1. Грамматика лингвистические правил для извлечения ключевой информации

Для извлечения ключевой информации есть разные механизмы. Одним из подходов извлечения информации является поиск ее по грамматика лингвистических правил. Подобное правила могут использоваться для поиска информации, а узкоспециализированных текстах. Под узкоспециализированными текстами стоит понимать тексты одной тематики, которое зачастую имеют одинаковую структуру. Главной проблемой данного подходанеобходимость ручного создания подобных правил. Решением данной проблемы может служить

система, которая автоматически создает подобные правила. Ниже будет представлена схема для создания подобных грамматика лингвистических правил.

В общем виде процесс создания грамматика лингвистических правил можно разделить на 3 основные части (модули):

1. Подготовка данных для их дальнейшего анализа
2. Поиск в тексте ключевых слов
3. Автоматическое создание грамматика лингвистических правил

2. Подготовка входных данных

На входе подается обычный текст на естественном языке. Задача модуля подготовки входных данных учесть специфику представления текста на естественном языке и преобразовать ее в вид удобный для анализа. Удобным для анализа форматом является массив из слов. В массиве каждая строка представляет собой текст, а столбец слово из этого теста. Причем все слова должны быть обработаны, а именно, представлены в формате токенов. [3]

3. Поиск в тексте ключевых слов

Под поиском ключевых слов тут понимается нахождение в нашем массиве слов, которые максимально характеризуют суть всего текста. Для решения подобной задачи можно использовать линейные модели машинного обучения на базе TF-IDF.[4]При обработке таким образом узкоспециализированных текстов можно заметить необычное поведение модели. Под необычным поведением понимаются скачки весов. На рисунке 1 можно увидеть, что веса некоторых слов имеют настолько высокие показатели, что их можно отнести ключевым словам.

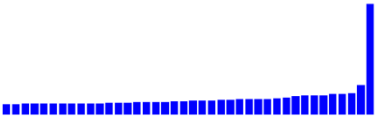


Рис 1. Веса слов в линейные модели машинного обучения на базе TF-IDF

Используя такое поведение модели можно находить в каждом тексте находить ключевые слова, а также их местоположение в текстовом массиве. Точность такого поиска не будет 100% - ной, но достаточной для использования ее при создании грамматика лингвистических правил.

4.Создание грамматика лингвистических правил

Для создания лингвистических правил нам нужны ключевые слова, а также их местоположение в текстовом массиве которые были найдены

ранее.Благодаря местоположению мы можем быстрой найти слова, которые идут до и после ключевого слова, которые мы нашли, используя линейную модель. Проведя частотный и морфологический анализ ключевого слова, а также слов до и после ключевого слова можно сформировать некоторое условное правило, по которому можно найти эти ключевые слова. Причем неотъемлемой частью такого правила должен быть элемент, базирующийся на наличии строго определенного слова или слова из определенной группы слов. Другими словами, правила должны иметь вид[справочникили морфологический признак]+ [Ключевое слово]+ [справочникили морфологический признак]. Причем до и после ключевого слова в правиле не могут находиться только морфологические признаки. Это нужно для того, чтобы гарантировать что мы находим ключевое слово по определенному паттерну включающие в себя слова которые как правило идут до или после ключевых слов. Таким образом формируется правило, которое может находить ключевые слова в узкоспециализированных текстах.

Заключение

В статье был описан способ для автоматического создания грамматика лингвистических правил для извлечения ключевой информации. Данный способ больше подходит для извлечения ключевой информации и узкоспециализированных текстов в виду их особенностей и схожести. Представленный способ не создает универсальные много функциональные правила. Но может автоматически создавать различные простые правила для каждого типа текстов. Что может быть более эффективным если рассматривать, с другой стороны, составление сложных универсальных правил, в которых довольно просто совершить ошибку.

Список литературы:

1. Пуртов Д. Н. Проблема обучения нейронной сети при извлечении ключевой информации / Д. Н. Пуртов, И. Г. Сидоркина // Интеллектуальные системы и информационные технологии – 2019

2. М.А. Павленко Анализ методов решения задачи извлечения информации из текстов [Электронный ресурс] – Режим доступа: http://www.hups.mil.gov.ua/periodic-app/article/11169

3. Гречачин В.А. К вопросу о токенизации текста/ Гречачин В.А. // Международный научно-исследовательский журнал– 2016

4. Рубцова Ю. В. Методы автоматического извлечения терминов в динамически обновляемых коллекциях для построения словаря эмоциональной лексики на основе микроблоговой платформы Twitter/ Рубцова Ю. В.// Доклады

Томского государственного университета систем управления и радиоэлектроники– 2014

УДК 004.052.3:004.725.5

Рогачева Ирина Сергеевна
направление Программная инженерия (бакалавриат), гр. ПС-22

Научный руководитель
Бородин Андрей Викторович
канд. экон. наук, зав. кафедрой информатики и системного программирования
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МОДЕРНИЗАЦИЯ АРХИТЕКТУРЫ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ОТКАЗОУСТОЙЧИВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ, ОСНОВАННЫХ НА КОНЦЕПЦИИ ТРОИРОВАНИЯ С ФУНКЦОНАЛЬНОЙ АДАПТАЦИЕЙ ЭЛЕМЕНТОВ ИЗБЫТОЧНОСТИ

Цель работы – исследование перспектив развития архитектур высокопроизводительных отказоустойчивых вычислительных систем, отличающихся кратностью резервирования сетевой подсистемы и использованием оригинальной отказоустойчивой силовой подсистемы.

Вопросам повышения готовности и доступности вычислительных систем (ВС) в настоящее время уделяется значительное внимание. Это связано с тем, что многие критические процессы человеческой деятельности управляются ВС и масштаб использования ВС в этом качестве год от года стремительно увеличивается. Этот факт определяет **актуальность** данного исследования.

Основным подходом к повышению готовности и доступности ВС является резервирование. При этом, часто, аналогичные по используемой топологии решения возникают в рамках масштабирования ВС для увеличения производительности. В качестве примеров, иллюстрирующих эту ситуацию, были рассмотрены два решения. Это отказоустойчивая система доступа к сети Internet, использующая концепцию «когнитивного интернета» [2], и отказоустойчивая гетерогенная система дистрибуции точного времени в сетях передачи данных [1, 4].

Сравнение топологий обеих систем позволило выявить общие черты используемых технических решений: разделение сетевой подсистемы на

два сегмента. В первом случае неуправляющий и рабочий сегменты, во втором – на сегмент первичных источников времени и сеть общего назначения. В обоих случаях такое разделение было продиктовано соображениями повышения производительности систем. Заметим, что в каждом из рассмотренных примеров критерии производительности разные. Однако, и в том, и в другом случае масштабирование (и резервирование) в функциональных группах обеспечивалось простым наращиванием количества соответствующих хостов, подключенных к обоим сегментам. В такой схеме «узким местом» оказывается сетевая подсистема. Даже в случае наличия механизмов динамической реконфигурации сетевой подсистемы потеря одного сетевого сегмента приведет к деградации характеристик всей системы.

Для решения этой проблемы предложена идея дальнейшего наращивания количества связующих сетевых сегментов, например, до трех. В этом случае мы получаем хорошо зарекомендовавшей себя в критически важных приложениях вариант так называемого троирования [5-8]. Традиционно троирование реализуется в рамках принципа мажорирования [6, 8], когда результатом выполнения функции резервированного узла в каждый момент времени является результат, получившийся хотя бы два раза, и, иногда, в рамках принципов кворума [8], когда решение о том, какой результат выполнения целевой функции верен, принимается на основе какого-либо более сложного суждения, нежели простое большинство. В нашем случае троирование сетевых сегментов не влечет возникновения проблемы выбора результата функционирования того или иного сегмента, требуется лишь принятие решения о конкретном функциональном назначении элемента резервирования в течение некоторого последующего промежутка времени. Таким образом, в нашем случае правомерно говорить о троировании с функциональной адаптацией элементов избыточности.

Типовая архитектура ВС, построенной на базе концепции троирования с функциональной адаптацией элементов избыточности, представлена на рис. 1. Важной особенностью представленного решения, с одной стороны, является дублирование первичных блоков питания, источников бесперебойного питания и вторичных блоков питания коммутаторов и вычислителей. С другой стороны, собственно функциональная избыточность достигается за счет горизонтального масштабирования вычислителей. Эффективность такого решения была обоснована в работе [3] в ходе проведения ряда вычислительных экспериментов по оценке стоимости владения ВС.

В рамках данного исследования предлагается модернизация механизма управления функциональной избыточностью сетевой подсистемой на основе разработанного API, реализующего обмен сообщениями, разбитыми на классы с заданными приоритетами. Важной особенностью данного API является независимость примитивов обмена от адресного плана сети. Работа с адресным планом вынесена в отдельный аспект объектной модели межузлового взаимодействия. Реализация стратегий приоритизации обмена сообщениями и управления стратегиями также вынесена в отдельный аспект проекта. Реализовано, по выбору, управление приоритизацией сообщений в рамках лексикографического порядка критериев обмена сообщениями и в рамках линейной свертки этих критериев.

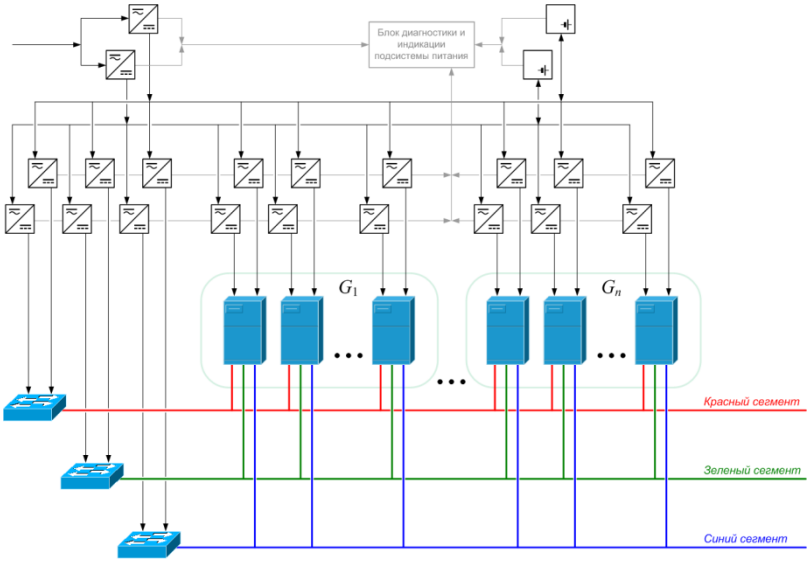


Рис. 1. Типовая топология высокопроизводительной отказоустойчивой ВС

В ходе практических испытаний разработанного программного обеспечения на стендах, собранных на базе лабораторий кафедры Информатики и системного программирования ФГБОУ ВО «ПГТУ» были получены положительные результаты по обеспечению живучести ВС в условиях смоделированных отказов как сегментов сети (до двух), так и хостов в группах (от одного, до $N_G - 1$), где N_G – количество

хостов в функциональной группе *G*. В целом практические эксперименты подтверждают оценки, полученные в работе [3].

Выводы. Главным результатом представленного исследования является вывод о перспективности использования концепции троирования с функциональной адаптацией элементов избыточности при построении высокопроизводительных ВС высокой степени готовности и доступности. Эффективность решения подтверждается при количестве хостов в группе, начиная с четырех, и при количестве групп не менее двух. Этот порог можно считать важнейшим критерием применения предлагаемой архитектуры ВС.

Разработанное программное обеспечение управления функциональной избыточностью сетевой подсистемы обеспечивает идентификацию большинства разновидностей отказов элементов ВС, а также реализует различные стратегии использования избыточной сетевой инфраструктуры. При этом разработанное программное обеспечение не ограничивает количество используемых сетевых сегментов ВС. Описанное программное обеспечение разработано для операционных систем семейства MicrosoftWindows 7+.

Список литературы:

1. Антонов, В. М. Инновационные подходы к развитию техники и технологий. Кн. 1 / В. М. Антонов, А. В. Бородин, Ю. А. Ипатов и др. – Одесса: КУПРИЕНКО СВ, 2015. – 172 с.

2. Бородин, А. В. Методы классификации и снижения размерности при визуализации метрик производительности / А. В. Бородин, А. Н. Азарова // Кибернетика и программирование. – 2015. – № 4. – С. 1-35. – DOI: 10.7256/2306-4196.2015.4.15271.

3. Бородин, А. В. Технико-экономическое обоснование варианта резервирования сетевой компоненты отказоустойчивой масштабируемой вычислительной системы специального назначения / А. В. Бородин // Кибернетика и программирование. – 2015. – № 6. – С. 55-70. – DOI: 10.7256/2306-4196.2015.6.17523.

4. Бородин, А. В. Учебно-испытательный полигон отработки технологий дистрибуции точного времени / А. В. Бородин, А. С. Варламов, Д. В. Кораблев // Кибернетика и программирование. – 2015. – № 3. – С. 11-23. – DOI: 10.7256/2306-4196.2015.3.15438.

5. Лисейкин, В. А. Особенности управления и аварийной защиты изделия при огневых испытаниях стендового блока первой ступени РН «Союз-2-1в» / В. А. Лисейкин, И. А. Тожокин // Вестник Самарского государственного аэрокосмического университета. – 2013. – № 4(42). – С. 181-195.

6. Тюрин, С. Ф. Отказоустойчивый логический элемент LUT ПЛИС FPGA / С. Ф. Тюрин // Вестник Пермского университета. Серия Математика. Механика. Информатика. – 2014. – № 4(27). – С. 97-104.

7. Шишкевич, А. А. Резервирование ЛВС реального времени EtherCAT / А. А. Шишкевич // Известия Тульского государственного университета. Технические науки. – 2014. – №12-2. – С. 244-251.

8. Шишкевич, А. А. Оценка показателей надежности вычислительных устройств с трехкратныммажорированием при отказах и сбоях / А. А. Шишкевич // Известия вузов. Электроника. – 2013. – № 4(102). – С. 84-88.

УДК 681.128.8

Родионова Альбина Константиновна
направление «Информатика и вычислительная техника»
(бакалавриат), гр. ИВТб-42

Научный руководитель
Смирнов Алексей Владимирович,
к. т. н., доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ВЫБОР ТЕХНОЛОГИИ ИЗМЕРЕНИЙ ДЛЯ АВТОНОМНОГО УРОВНЕМЕРА С БЕСПРОВОДНОЙ ПЕРЕДАЧЕЙ ДАННЫХ ПО ТЕХНОЛОГИИ LORAWAN

Цель работы – обоснование выбора технологии при разработке энергоэффективного малогабаритного датчика волнового уровнемера, предназначенного для получения показаний значения уровня жидкости в промышленных условиях работы с последующей передачей данных по беспроводному каналу связи по технологии LoRaWAN.

По информации ведущих нефтедобывающих и нефте-перерабатывающих компаний России, значительная часть емкостей не критически важного производства в настоящее время не охвачено автоматизированными средствами контроля уровня, что обуславливает необходимость содержания штата специалистов для выполнения соответствующих регламентных работ.

В результате анализа существующих требований к уровнемерам, а также тенденций развития рынка в области промышленного «интернета вещей», можно выставить следующие требования к автономному уровнемеру:

1) диапазон определения уровня: от 0,1 до 10 м;

2) точность определения уровня: не хуже +/- 20 мм (при уровне 2-10 м);

3) срок работы датчика уровня жидкости от одного элемента питания: не менее 1 года, при отправке регистрации данных один раз в час;

4) требования к беспроводному каналу связи:

- дальность связи ближнего действия: до 100 м на открытой местности;

- дальность связи дальнего действия: до 15 км на открытой местности;

- использование механизмов гарантированной доставки данных;

- использование частотного диапазона радиосигналов, разрешенного на территории Российской Федерации;

5) возможность настройки интервалов между регистрацией данных от 1 минуты до 24 часов;

6 возможность настройки интервалов между отправкой данных от 1 минуты до 24 часов;

7) возможность задания диапазона уровня жидкости, при превышении которого происходит отправка данных вне установленной временной схемы;

8) максимальные величины токов и напряжений в электрических цепях прибора не должны превышать требований ГОСТ 14255-69.

Ограничения, накладываемые требованиями по точности и диапазону измеряемого уровня, длительности автономной работы на одном элементе питания, а также требования обеспечения взрывозащищенности уровнемера, ограничивающие токи и напряжения, существенно ограничивают варианты выбора метода измерений.

В соответствии с ГОСТ 24802-81 различают 29 видов уровнемеров[1]. Однако, учитывая приведенные выше требования, а также текущий уровень развития технологий с непрерывным частотномодулированным излучением (FMCW – frequency modulated continuous wave) перспективным является выбор данной технологии в качестве основы разработки уровнемера. В данном случае тип уровнемера будет волновой.

Однако, принципиальное отличие практики применения сенсоров FMCW для определения уровня от аналогов заключается в необходимости адаптации процесса измерения к текущим параметрам объекта контроля: текущему уровню, динамике изменения контролируемой поверхности, конструкции емкости. В целях достижения требуемой точности определения уровня жидкости контролируемого объекта необходимо использовать адаптивный алгоритм выбора параметров настройки сенсора FMCW и критериев обработки поступающих данных в зависимости от характеристических признаков объекта контроля.

В качестве примера возможной реализации волнового уровнемера по технологии FMCW можно рассмотреть микросхему IWR1642 производства компании TexasInstruments [2].

Микросхема IWR1642 представляет собой автономное промышленное одночиповое решение радиолокационного датчика FMCW в полосе частот от 76 до 81 ГГц [3]. Рабочий температурный диапазон, точность и диапазон измерений расстояния, а также величина потребления питания данной микросхемы удовлетворяют обозначенным выше требованиям к измерительной части уровнемера.

Таким образом, представляется целесообразным выбор технологии FMCW для построения волнового уровнемера, предназначенного для получения показаний значения уровня жидкости в промышленных условиях работы с последующей передачей данных по беспроводному каналу связи по технологии LoRaWAN.

Список литературы:

1. ГОСТ 24802-81 Приборы для измерения уровня жидкости и сыпучих веществ. Термины и определения. – Введ. 01.07.82. – М.: Госстандарт СССР: Изд-во стандартов, 1991. – 7 с.
2. IWR1642 BOOST Evaluation Board. [Электронныйресурс]. URL: https://www.ti.com/tool/IWR1642BOOST (дата обращения: 25.09.2020).
3. IWR1642 Datasheet (PDF) - Texas Instruments. [Электронный ресурс]. URL: https://www.alldatasheet.com/datasheet-pdf/pdf/1047699/TI1/IWR1642.html (дата обращения: 25.09.2020).

УДК 004.052

Сараева Ольга Андреевна
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм-13

Научный руководитель
Смирнов Алексей Владимирович
кандидаттехн. наук, доцент кафедры Информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет»,г. Йошкар-Ола

РАЗРАБОТКА АВТОНОМНОГО ДАТЧИКА УГЛА НАКЛОНА С РАДИОКАНАЛОМ ДАЛЬНЕГО ДЕЙСТВИЯ

Цель работы – разработка методики определения угла наклона для датчика-сигнализатора с передачей данных как по радиоканалу ближнего, так и дальнего действия.

В настоящее время в нефтедобывающей промышленности существенное распространение получают системы сигнализации, призванные снизить как производственные издержки, так и показатели недополученной прибыли. Широкомасштабное внедрение подобных систем стало возможным в первую очередь благодаря существенному повышению энергоэффективности электронных компонентов, а также развитию технологий энергоэффективной передачи данных, что позволило разрабатывать и производить различные автономные датчики малой стоимости.

К технологиям энергоэффективной беспроводной передачи данных можно отнести:

- BTLE (BluetoothLowEnergy) [1] – технология, обеспечивающая передачу данных на расстояния до 100 метров (радиосвязь ближнего действия);
- LoRaWAN [2] - технология, обеспечивающая передачу данных на расстояния до 15 километров (радиосвязь дальнего действия).

Объединение данных технологий на одной платформе позволяет применять датчики, основанные на ней, как для автономных, локальных систем управления технологическими процессами, так и в распределенных системах мониторинга за технологическими параметрами оборудования.

Определена проблема так называемых «вертолетов» - ситуаций, когда при работе ШСНУ (штанговая скважинная насосная установка) происходит, обрыв шатуна балансира, который, упираясь в основание ШСНУ, опрокидывает ее, что приводит к дорогостоящему ремонту как самой ШСНУ, так зачастую и всей скважины. Время, между обрывом шатуна и началом опрокидывания ШСНУ не менее половины периода качания балансира (от 8 до 30 секунд). Кроме того, в период ремонта нефтедобывающая компания теряет в объеме добычи углеводородов.

Решением обозначенной проблемы является решение, которое удовлетворяет следующим требованиям:

- возможность регистрации обрыва шатуна;
- возможность своевременной передачи информации об обрыве на ближнее расстояние;
- возможность передачи данных об аварии на дальние расстояния;
- беспроводное решение (как следствие – высокая энергоэффективность);
- обеспечение взрывозащищенного исполнения;
- низкая стоимость решения.

Таким образом, решение, удовлетворяющее обозначенным требованиям, является **актуальной задачей**.

На первом этапе работы были выбраны 2 методики определения угла наклона на основе данных акселерометра: 2-х и 3-х осевые.

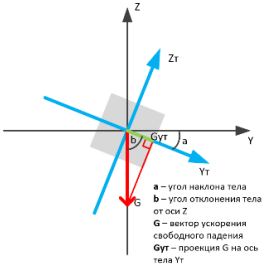


Рис. 1. Схема тела, на котором закреплен трёхосевой акселерометр

Проекции Gyt (зеленый отрезок) и Gzt можно выразить с помощью теоремы о прямоугольном треугольнике:

$$G_{yT} = G * \cos(b)$$

$$G_{zT} = G * \sin(b)$$

Таким образом, можно вычислить угол b отклонения акселерометра от вектора гравитации Z (от вертикальной оси):

$$b = \arccos(\frac{G_{yT}}{G})$$

$$a = 90 - \mathrm{b} = 90 - \arccos(G_{yT})$$

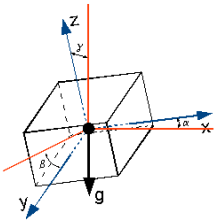


Рис. 2. Трёхосевой случай.

Значения углов могут быть вычислены по следующим формулам:

$$a = \arctan(\frac{A_x}{\sqrt{A_y^2 + A_z^2}})$$

$$\beta = \arctan(\frac{A_y}{\sqrt{A_x^2 + A_z^2}})$$

$$\gamma = \arctan(\frac{A_z}{\sqrt{A_x^2 + A_y^2}})$$

Акселерометр [3] фиксирует проекции силы гравитации[4] на все три оси пространства. Зная значение ускорения свободного падения и его проекции на все 3 оси можно определить угол отклонения акселерометра от вектора гравитации (от вертикальной оси).

Для определения требования разрешающей способности акселерометра была проведена оценка требуемого разрешения при измерении ускорения по каждой оси акселерометра.

В результате оценки работы датчика определены его положения, при которых изменение угла наклона датчика на 1 градус приведет к минимальным изменениям значений проекций гравитационной силы на оси акселерометра.

$g = 9.807 \frac{m}{s^2}$ - ускорение свободного падения

$\alpha := (0..360)$ - угол α

$\alpha =$

0
1
...

Выбор системы координат: с двумя осями

$x(\alpha) := g \cdot \cos(\alpha \cdot °)$ - значение координаты X при изменении угла α

$x(\alpha) =$

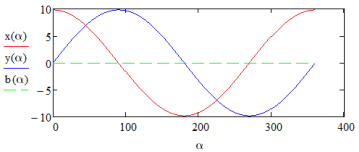
9.807	$\frac{m}{s^2}$
9.805	
9.801	
9.793	
9.783	
9.769	
...	

$y(\alpha) := g \cdot \sin(\alpha \cdot °)$ - значение координаты Y при изменении угла α

$y(\alpha) =$

0	$\frac{m}{s^2}$
0.171	
0.342	
0.513	
0.684	
0.855	
...	

Построение графика значений ускорения от изменения угла



Выбор рассматриваемой части графика: первая четверть, с 0 до 89 градусов

$i := 0..89$

$F\_X_i := x(i) - x(i+1)$

$F\_Y_i := y(i) - y(i+1)$

Для того, чтобы найти насколько изменяются координаты от изменения угла, вычитается из текущего значения координаты следующее

Необходимо найти 2 угла, разница между которыми 1 градус, и изменение значений координат минимально.

$F\_1_i := F\_Y_i + F\_X_i$ - сложение значений координат X и Y

$F\_1 =$

	0	
0	-0.17	$\frac{m}{s^2}$
1	-0.167	
2	...	

- результат сложения

minimum(F) :=
min ← 0
i ← 0
while $F_i < 0$
  min ← F_i if $|min| > F_i$
  i ← i + 1
minimum ← min

- функция нахождения минимального значения

$minimum(F\_1) = -2.112 \times 10^{-3} \frac{m}{s^2}$ - минимум

$indexOF := match\left(minimum\left(F\_1 \cdot \frac{s^2}{m}\right), F\_1 \cdot \frac{s^2}{m}\right) = (44)$ - функция нахождения угла

Определено, что значение проекций ускорения свободного падения на оси акселерометра между углами в 44 и 45 градусов будет минимальным. Требуемая разрешающая способность по ускорению каждой оси акселерометра 2 тысячных метра на секунду в квадрате.

Выводы

В данной статье была описана разработка методики определения угла наклона датчика-сигнализатора и определено требование разрешающей способности акселерометра. Из методики видно, что между углами в 44-45 градусов на оси акселерометра привело к минимальным изменениям значений проекций гравитационной силы при наклоне в 1 градус.

Список литературы:

1. Фальков Е. В., Романов А. Ю. Применение маячков Beacon и технологии Bluetooth Low Energy для построения систем навигации в зданиях // Новые информационные технологии в автоматизированных системах. 2015. №18.
2. Выдрин Дмитрий Федорович, Ситдиков Дмитрий Рафаэлевич Основные параметры беспроводной технологии LoRaWAN // Academy. 2019. №2 (41).
3. Желтухина Л.В. Акселерометр // Достижения вузовской науки. 2016. №20.
4. Василенко Павел Владимирович Гравитационные силы и миграционная подвижность населения региона // Вестник Балтийского федерального университета им. И. Канта. Серия: Естественные и медицинские науки. 2013. №7.

УДК 621.3.084.2

Смирнов Егор Александрович
направление Информатика и вычислительная техника (магистр), гр. ИВТм-11

Научный руководитель
Смирнов Алексей Владимирович
канд. техн. наук, доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА АВТОНОМНОГО ДАТЧИКА ВИБРОСКОРОСТИ НА ОСНОВЕ MEMS АКСЕЛЕРОМЕТРА

Рассматривается возможность применения MEMS акселерометра в качестве сенсора в датчике вибрации с целью снижения стоимости по сравнению с существующими аналогами. Происходит выбор MEMS акселерометра удовлетворяющего выведенным требованиям. Разрабатывается методика испытаний акселерометра, а также прототип и встроенное ПО для проведения испытаний. Осуществляется анализ результатов проведенных испытаний.

Ключевые слова: датчик, виброскорость, виброускорение, вибродиагностика, LoRaWAN.

Введение. Контролируя параметры работы электродвигателя и собирая в течение определенного времени данные о вибрациях и биениях, можно предсказать, когда вероятнее всего произойдет поломка

и даже определить причину ее возникновения. Таким образом, производитель может заранее предусмотреть техническую остановку оборудования для профилактического обслуживания, замены двигателя или других деталей еще до того, как поломка произойдет. Имея данные о вибрации, можно найти причины потенциальной проблемы и устранить их. При этом полученная информация в дальнейшем может быть использована для оценки состояния другого аналогичного оборудования, работающего на заводе.

Для того чтобы определить, что тот или иной механизм требует обслуживания или замены, необходимо контролировать параметры его работы в течение некоторого периода времени. Система мониторинга должна обнаруживать биения и нежелательные вибрации. Эти данные сигнализируют о потенциальных или реальных проблемах.

Цель работы - разработка энергоэффективного малогабаритного датчика виброскорости, предназначенного для получения показаний среднеквадратичного значения виброскорости динамического оборудования в условиях работы во взрывоопасных средах с последующей передачей данных по беспроводному каналу связи по технологии LoRaWAN.

Проведение испытаний. В качестве датчика ускорения был выбран программируемый акселерометр IIS2DH компании STMicroelectronics. Выбор акселерометра происходил с учетом его стоимости, энергопотребления и точности.Одним из главных его достоинств является то, что калибровка данного акселерометра осуществляется производителем. Акселерометр может работать на фиксированных частотах дискретизации. В рамках проекта интересны частоты 400, 1344 и 5376 Гц[3].

Для проведения испытаний необходимо собрать прототип разрабатываемого датчика.Прототип состоит из трех частей:

- Отладочная плата PCA10040
- плата STEVAL-MKI168V1 с акселерометром IIS2DH
- Персональный компьютер с ОС Windows 7

Отладочная плата PCA10040 включает в себя аппаратное обеспечение и исходный код микропрограммного обеспечения. Этот комплект предназначен для разработки и отладки с системой на кристалле nRF52832.

Структурная схема разработанного прототипа для проведения испытаний акселерометра представлена рисунке 1.

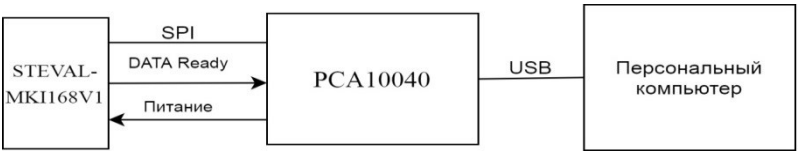


Рис. 1. Структурная схема прототипа.

Перечень параметровакселерометра, которые требуется определить в рамках испытаний (по ГОСТ Р ИСО 16063-1-2009):

- неравномерность амплитудно-частотной характеристики (АЧХ) (п.4.2.1 по ГОСТ);
- нелинейность амплитудной характеристики (п.4.2.2 по ГОСТ);
- относительный коэффициент поперечного преобразования (п.4.3.3 по ГОСТ).

Определение всех требуемых параметров осуществляется посредством специализированного вибростенда, на котором устанавливаются эталонный и испытуемый (калибруемый) преобразователи.

Цель проведения первого испытания – оценка потенциальной возможности использования MEMSакселерометра IIS2DHв качестве сенсора виброускорения в датчике вибрации. Главная задача испытания – это оценка точности определения амплитуды сигнала ускорения на разных частотах. Результат испытания и оценка результата представлены в таблице 1.

Таблица 1. Результат первого испытания

СКЗ виброскорости, мм/с		Разница в процентах
теоретическое	практическое	
7	5.972	14.68571
8	6.837	14.5375
9	7.746	13.93333
10	8.615	13.85
11	9.408	14.47273
12	10.27	14.41667
13	11.156	14.18462
14	11.973	14.47857
15	12.932	13.78667

Главный результат проведенного испытания: при регистрации виброускорения испытуемый акселерометр не вышел за границы точности вибростенда составляющие 15%. Для уточнения неравномерности амплитудно-частотной характеристики и коэффициента преобразования акселерометра следует провести испытания на более точном стенде.

Анализ результатов. Результатом проделанной работы по разработке прототипа и проведению испытаний можно назвать подтверждение возможности использования MEMSакселерометра IIS2DHв качестве сенсора виброускорения в датчике вибрации. В ходе экспериментов удалось зарегистрировать сигналы ускорения на разных амплитудах в диапазоне частот, на которых обычно работает динамическое оборудование. Акселерометр хорошо показал себя на самых разных амплитудах ускорения и частотах колебания вибростола.

Вывод.Итогом работы является проведение испытаний и анализ результатов. Главным итогом испытаний является подтверждение гипотезы о возможности использования МЕМС акселерометра в датчике вибрации.

В дальнейшем планируется выяснить максимальную точность, с которой можно будет производить измерение виброскорости. Для этого предполагается подключить математические методы, а также провести испытания на вибростенде, обеспечивающем точность сигнала виброускорения выше, чем характеристики акселерометра

Список литературы:

1. ГОСТ Р ИСО 10816-1-1997 Контроль состояния машин по результатам измерений вибрации на невращающихся частях. Общие требования. [Электронный ресурс] URL: https://files.stroyinf.ru/Data2/1/4294820/4294820503.pdf (дата обращения: 24.04.2020).

2. ГОСТ Р ИСО 2954-2014 Контроль состояния машин по результатам измерений вибрации на невращающихся частях. Требования к средствам измерений. [Электронный ресурс] URL: https://files.stroyinf.ru/Data2/1/4293765/4293765629.pdf (дата обращения: 24.04.2020).

3. ГОСТ Р ИСО 16063-1-2013 Вибрация. Методы калибровки датчиков вибрации и удара. Часть 1. Основныеположения [Текст]. – М.: Стандартинформ, 2019.

4. Ultra-low-power high-performance 3-axis accelerometer with digital output for industrial applications. Datasheet - productiondata. [Электронный ресурс] URL: https://www.st.com/resource/en/datasheet/iis2dh.pdf (дата обращения: 1.11.2019).

5. Олийник, П. Б. Разработка беспроводного датчика вибрации на основе mems акселерометра [Текст] / П. Б. Олийник. – Харьков: Технологический центр, 2016. – 81 с.

УДК 004.052

Сосорева Анна Игоревна, Васильева Елена Сергеевна
направление Информационная безопасность автоматизированных систем (специалитет), гр. БИ-42

Научный руководитель
Смирнов Владимир Иванович
старший преподаватель кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола.

ФИЗИЧЕСКИЕ ЭФФЕКТЫ, ИСПОЛЬЗУЕМЫЕ В ИЗМЕРИТЕЛЬНЫХ ПРЕОБРАЗОВАТЕЛЯХ АППАРАТУРЫ МАГНИТОМЕТРИЧЕСКОЙ РАЗВЕДКИ*

Цель работы – изучение и анализ физических эффектов, использующихся в измерительных преобразователях аппаратуры магнитометрической разведки.

Структура комплексной системы информационной безопасности охраняемого объекта определяется применением правовых и организационно-кадровых мер, а также средств защиты от технических разведок. Защита от технических средств разведки (ТСР) является неотъемлемой и составной частью научной и производственной деятельности предприятий, учреждений и организаций оборонной промышленности, а также обеспечения боевой деятельности войск и сил флота [1].Проблема комплексной защиты объектов и информации охватывает широкий круг вопросов.

В соответствии с физическими принципами построения ТСР подразделяются на средства оптической, оптикоэлектронной, радиоэлектронной, гидроакустической, акустической, химической, радиационной, сейсмической, магнитометрической и компьютерной

*Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта «Развитие теоретических основ для методов утечки и перехвата речевой информации по техническим каналам с использованием физических эффектов» (проект № 24/2020).

разведок [2]. Таким образом, существует широкий спектр видов, технических средств и возможных методов разведки, применение которых необходимо предвидеть на практике при применении правовых и организационно-кадровых мер, а также средств защиты от технических разведок.

Разведывательная аппаратура предназначена для регистрации физических полей, которые возникают при функционировании объектов разведки и являются источниками информации о них. В связи с этим возникают вопросы теоретического анализа физических эффектов (ФЭ), используемых в аппаратуре технической разведки. Следует отметить, что для анализа ФЭ требуются исследования по каждому виду технических разведок. Наиболее интересной для детального изучения показалась магнитометрическая разведка.

Под магнитометрической разведкой понимается добывание информации путем обнаружения и анализа локальных изменений магнитного поля Земли под воздействием объектов с большой магнитной массой [2]. В качестве меры, с которой сравнивается исследуемое геомагнитное поле используют поля постоянных магнитов или электрического тока. Основной аппаратурой, применяемой в магнитометрической разведке являются магнитометры (приборы, предназначенные для измерения характеристик магнитного поля и магнитных свойств физических объектов).

По физическим эффектам, используемым в измерительных преобразователях прибора, магнитометры можно условно разделить на две большие группы: квантовые и классические (рис. 1). К классическим относят датчики, принцип работы которых можно объяснить с классической точки зрения, а к квантовым – датчики, чей принцип работы основан на чисто квантовых эффектах [3].

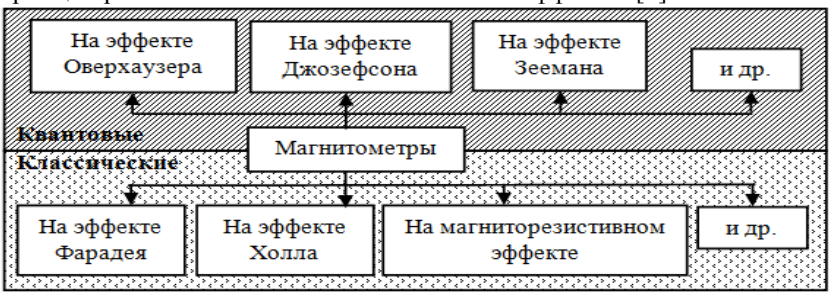


Рис. 1. Схема наиболее распространённых ФЭ, использующихся в измерительных преобразователях аппаратуры магнитометрической разведки

В магнитометрической разведке в основном используются оптико-механические, квантовые (протонный и на основе эффекта Зеемана) и феррозондовые магнитометры [2]. Наиболее распространённые ФЭ, использующиеся в измерительных преобразователях аппаратуры магнитометрической разведки, представлены на рис. 1.

Рассмотрим ФЭ, использующиеся в классических магнитометрах.

Эффект Фарадея заключается во вращении плоскости поляризации линейно поляризованного света, распространяющегося в изотропном веществе вдоль постоянного магнитного поля, в котором находится это вещество [4].

Эффект Холла заключается в следующем. Если металлическую или полупроводниковую пластинку, вдоль которой течёт постоянный электрический ток, поместить в перпендикулярное к ней магнитное поле, то между гранями, параллельными направлениям тока и поля, возникает разность потенциалов [5].

Магниторезистивный эффект (магнетосопротивление) заключается в том, что электрическое сопротивление твёрдого проводника зависит от напряженности магнитного поля, в котором находится проводник.

Рассмотрим ФЭ, использующиеся в квантовых магнитометрах.

Эффект Зеемана заключается в расщеплении уровней энергии атомов, молекул и кристаллов в магнитном поле, приводящем к расщеплению спектральных линий в спектрах этих квантовых систем. ФЭ обусловлен наличием у квантовой системы магнитного момента [5].

Эффект Джозефсона заключается в следующем. При протекании электрического тока через контакт Джозефсона, на контакте возникает падение напряжения. Протекание тока через контакт обусловлено квантовым туннелированием куперовских пар (связанных электронов). В основном состоянии все куперовские пары имеют одну фазу; по контакту Джозефсона течет переменный ток, и контакт излучает электромагнитные волны. При туннелировании куперовские пары приобретают избыток энергии за счет напряжение на контакте. При возвращении пары в исходное состояние излучается фотон [5].

В протонных магнитометрах применяется метод динамической поляризации. В методе динамической поляризации ядер используется эффект Оверхаузера, заключающийся в том, что в некоторых веществах с сильным взаимодействием ядерных спинов сэлектронными можно создать дополнительную поляризацию одной спиновой системы.

Таким образом, были изучены наиболее распространенные ФЭ, используемые в измерительных преобразователях аппаратуры магнитометрической разведки. Помимо рассмотренных существуют и

другие ФЭ, которые могут использоваться в разведывательной аппаратуре. Благодаря широкому спектру ФЭ, на которых построены магнитометры, магниторазведку применяют для решения некоторых инженерно-геологических задач, а также используют в военных и разведывательных целях. Исследования физических эффектов по каждому виду технических разведок будут продолжены.

Список литературы:

1. Меньшаков Ю.К. Основы защиты от технических разведок / Ю.К. Меньшаков. – М.: ИПЦ «Маска», 2017. – 572 с.
2. Меньшаков Ю.К. Теоретические основы технических разведок / Ю.К. Меньшаков. – М.: ИПЦ «Маска», 2017. – 640 с.
3. Игнатьев А.А. Магнитометрия слабых магнитных полей / А.А. Игнатьев, М.Н. Куликов, А.В. Маханьков, А.В. Прозоркевич // Гетеромагнитная микроэлектроника: сб. науч. тр. – Саратов: Изд-во Сарат. ун-та, 2013. – Вып. 15: Гетеромагнитная микро- и наноэлектроника. Методические аспекты физического образования. – С. 11-32.
4. Половинкин А.И. Основы инженерного творчества: учебное пособие / А.И. Половинкин. – 7-е изд., стер. – Санкт-Петербург: Лань, 2019. – 364 с.
5. Соболев А.Н. Физические основы перспективной вычислительной техники и обеспечение информационной безопасности: Учебное пособие / А.Н. Соболев, В.М. Кириллов, А.В. Киселев – М.: Гелиос АРВ, 2012. – 256 с.

УДК 621.391

Спиридонова Т.Э.
группа КТМ-41

Научный руководитель
Шобанов Лев Николаевич,
доцент, руководитель лаборатории САПР
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола.

ПАКЕТ ОБНОВЛЕНИЙ ДЛЯ УСКОРЕННОЙ РАБОТЫ В САПР "ЛОГОС"

В последнее время наблюдается стремительное развитие тяжелых систем автоматизированного проектирования в таких отраслях как авиастроение, автомобилестроение, тяжелое и легкое машиностроение, кораблестроение, архитектуре и т.д. САПР в машиностроении используют для проведения конструкторских, технологических работ; с

помощью систем автоматизированного проектирования на предприятии выполняется разработка конструкторской документации, 2D и 3D моделирование, спецификация и конфигурация, готовые сборки и отдельные объекты. Современные САПР позволяют проводить анализ детали на прочность, напряжение, что благоприятно сказывается на дальнейшем этапе изготовления детали.

В ВУЗах Российской Федерации обучение проектированию и конструированию ведется на САПР зарубежного производства, такие как AutodeskInventor и SolidWorks, но в тоже время существуют отечественные аналоги систем проектирования, такие как КОМПАС и Логос.

Программный пакет "Логос" оснащен мощной средой для 2D и 3D эскизирования и проектирования, что позволит создавать профили и траектории любой сложности. Есть специальное параметрическое ядро. Есть возможность задавать сложные взаимосвязи элементов эскиза как между собой, так и с другими элементами модели, как на уровне параметров, так и на уровне геометрии. Большой выбор вспомогательных инструментов, которые повысят скорость построения и эффективность.

Целью и задачей проекта является работа с уже имеющейся российской системой автоматизированного проектирования, добавления определенных компонентов "ускорителей проектирования" в основной пакет "Логос" для удобного пользования не только на предприятиях ГК "Росатом" и предприятиях закрытого типа, но и для возможности обучения студентов технических вузов для дальнейшего трудоустройства и создание конкурентоспособной САПР не только на российском рынке, но и за рубежом.

Также можно выделить главный пункт проекта: моделирование трехмерных объектов любой сложности, гибкое сочетание твердотельного и поверхностного моделирования, быстрое моделирование компонентов в единую сборку. Создание "ускорителей проектирования", который будет содержать в себе механический калькулятор, генераторы компонентов, что позволит автоматизировать создание изделий и деталей с применением функциональных параметров: скорость, мощность, свойства материала. Набор ускорителей проектирования будет функционировать и работать с использованием математических формул и физических теорий, которые используются для проектирования механических систем.

В проектирование скорость, как критерий выполняемой работы, делит первое место с качеством. И благодаря "ускорителям

проектирования" время, затраченное на конструирование детали, можно уменьшить без потери качества, что поможет облегчить деятельность специалиста, сотрудника с однотипной работой. Создать более удобный визуальный интерфейс моделирования, работы с трехмерными объектами без потери качества.

Дополнительная информация по проекту: при использовании "ускорителей проектирования» пользователь может сэкономить время работы и облегчить нагрузку на программное обеспечение компьютера. Детали, находящиеся в сборках, которые не нужны в данный момент для создания внешних параметров можно с помощью «ускорителей проектирования» скрыть, что облегчит работу операционной системы и самого САПР. Не нужно будет загружать много сборок, деталей. Для инженера-конструктора упрощается работа и повышается скорость и качество, что благоприятно скажется на производительности труда.

Список литературы:

1. Кондаков А.И. САПР технологических процессов, - Москва, Академия, 2007, 269 с.
2. http://logos.vniief.ru/ - официальный сайт САПР "Логос".

УДК 332.1

Степанова Екатерина Олеговна
направление Прикладная Информатика (бакалавриат), гр. ПИ-31

Научный руководитель
Порядина Ольга Викторовна,
канд. экон. наук, доцент кафедры информационных систем в экономике
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ВЛИЯНИЕ ЦИФРОВОЙ ЭКОНОМИКИ НА КАЧЕСТВО ЖИЗНИ НАСЕЛЕНИЯ

Стремительное развитие цифровых технологий и цифровая трансформация экономических отношений уже проявляется во всех сферах жизни людей, несет кардинальные изменения и сильно влияет на качество жизни человека.

Целью исследования является изучение влияния цифровой экономики на жизнь населения. **Задачами** исследования являются: формирование понимания, что такое цифровая экономика, выявление

преимуществ и недостатков цифровизации, описание концепций влияния цифровых технологий в различных сферах общества, исследование отдельных опросов и мнений, связанных с цифровой экономикой.

Центром цифровой экономики является производство цифровых товаров и оказания услуг, связанных с цифровыми технологиями. Появляется и стремительно развивается цифровая инфраструктура, растет качество коммуникационных сетей, например, разработка технологий 4G, 5G и оптоволоконных средств передачи данных, при этом цены становятся ниже, такие как услуги мобильной связи, возможности по использованию мобильных устройств для доступа в интернет становятся шире, что, конечно, позволяет прогнозировать все больший охват и развитие цифровых технологий в мире [2].

Важность развития цифрового сектора для национальных экономик можно отметить в концепциях постиндустриального и информационного общества, которая подтверждается тем, что многие страны в настоящее время реализуют полномасштабные программы, которые нацелены на изменения в производственных процессах, переориентация производства с создания материальных благ на предоставление услуг.

Также появляется автоматизация соответствующих трудовых операций и одновременно возникновение новых профессий и роста спроса на неалгоритмизируемый труд и творчество. Онлайн-программы и основанные на них формы профессионального обучения. Происходит развитие массового онлайн-образования, появление качественных массовых открытых онлайн-курсов. Однако цифровизация учебного процесса привносит затруднения, которые требуют решения вопросов адаптации образовательной системы к цифровой среде, проработки этических аспектов применения цифровых технологий в долгосрочной перспективе.

Цифровые сервисы и современный подход к появлению «умных» пространств кардинально изменяют условия жизни человека на более комфортные. «Умное» пространство представляет собой физическую или цифровую среду, в которой люди и технологические системы открыто взаимодействуют в связанных и скоординированных интеллектуальных экосистемах. Среди примеров такого рода — «умные» города, «умные» дома, цифровые рабочие места и фабрики. В России уже есть крупные цифровые компании, например, первый отечественный онлайн-банк «Тинькофф Банк», не имеющий региональных отделений, цифровые порталы сервисов «Яндекс»

и Mail.ru, интернет-сервис для размещения различного рода объявлений «Avito», социальная сеть «ВКонтакте» и другие.

Основными преимуществами реализации цифровой экономики являются [3]:

1. Оптимизация производства.

2. Рост производительности труда. Качество труда может сильно снижаться под влиянием человеческих факторов, например, состояние здоровья, отсутствие мотивации сотрудников, усталость. Компьютерная техника может без перерывов выполнять свои заданные функции.

3. Доступность управления [3]. Благодаря цифровизации экономики развитие бизнеса стало возможным в различных городах и даже за пределами страны. Кроме того, за счет информационных технологий руководитель без затруднений может поддерживать связь, минимизируя время и деньги.

4. Снижение угроз экономической безопасности и коррупции. Автоматизация значительно уменьшает процедуры при рассмотрении заявок, связанные с бумагами, таким образом, происходит спад коррупции.

5. Свёртывание вопроса национальной принадлежности [3]. Компьютеры не имеют эмоций, чувств и субъективности. На первом месте при работе на производстве остаётся профессионализм персонала, а не национальная принадлежность.

6. Обширные технические возможности. Машины могут вмещать в своей памяти терабайты информации. Это одно из наиболее значимых достоинств, которое характеризуется тем, что информационная безопасность для компании - это самая важная составляющая.

Для того, чтобы выяснить, как воспринимается определение «цифровая экономика» студентами и магистрантами высших учебных заведений, являющихся «поколением NEX» было проведено исследование [1]. Распределение мнений респондентов, оценивающих по десятибалльной шкале важность новых знаний в области цифровой экономики и электронного бизнеса для изменения качества их жизни (1 - совсем неважны; 10 - очень важны), представлено на рисунке 1. Крайне актуальным получения новых знаний в области цифровой экономики и электронного бизнес считают 97% опрошенных респондентов (оценка 8, 9 и 10 баллов), и лишь 3% респондентов отмечают важность получения таких знаний на 7 баллов, при этом среди опрошенных нет оценок ниже 7 баллов [1].

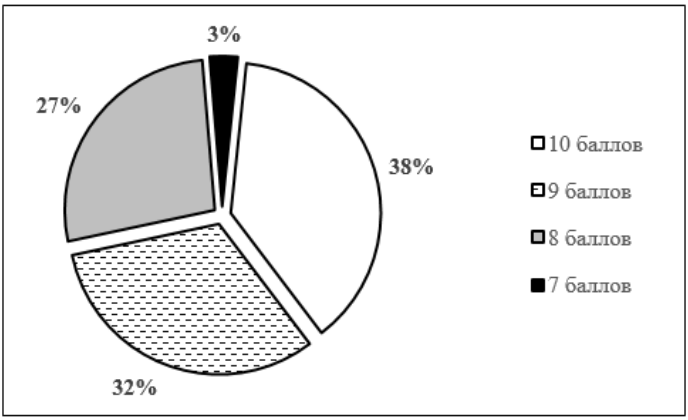


Рис. 1. Распределение мнений респондентов, % от числа опрошенных [1]

Несмотря на то, что ИТ являются ключевым фактором прогресса, необходимо также выявить существенные риски цифровой экономики:

1. Проблемы обеспечение национальной безопасности и уязвимость информационной безопасности. Большая часть информации содержится в интернете, поэтому нужно помнить о возможности потенциальных кибератаках, которые способны разрушить независимость страны и предприятий. Необходимо периодически проводить мониторинг информационной базы на наличие несанкционированных кибератак, а также предъявлять более жесткие требования при наборе кадров на работу с целью защиты информации от утечки.

2. Рост безработицы. Автоматизация производства приводит к снижению рабочих мест, так как один компьютер по своей продуктивности в выполнении работы равен работоспособности нескольких рабочих, в зависимости от характера производства.

3. Спад системного мышления. Системное мышление сменяется компьютеризированным, таким образом мышление становится в поверхностным и скоростным, вместо комплексно-целевого и причинно-следственного.

4. Снижение уровня креативности персонала, способности к созданию нового. Открытый доступ к информации зачастую считается более простым и выгодным путём при поиске идей, чем создание собственной идеи с помощью своего мозга [3].

Итак, в действительности цифровая экономика постепенно внедряется во все области и благодаря этому жизнь граждан изменяется под воздействием внедрения инноваций. Для того чтобы данное

внедрение имело положительный характер следует системно заниматься трансформацией современного общества и распространять технологии.

Список литературы:

1. Борисов, С. А. Феномен цифровой экономики информационного общества и его значение для повышения качества жизни населения / С. А. Семенов, С. Г. Захарова // Экономика и общество. – 2018. – №3 (6). – Режим доступа: https://scipress.ru/economy/articles/fenomen-tsifrovoj-ekonomiki-i-informatsionnogo-obshhestva-i-ego-znachenie-dlya-povysheniya-kachestva-zhizni-naseleniya.html. – 15.05.2020.
2. Семячков, К. А. Цифровая экономика и ее роль в управлении современными социально-экономическими отношениями / К. А. Семячков // Современные технологии управления. – 2017. № 8. – Режим доступа: https://cyberleninka.ru/article/n/tsifrovaya-ekonomika-i-ee-rol-v-upravlenii-sovremennymi-ekonomicheskimi-otnosheniyami. – 15.10.2020.
3. Трофимова, Т. В. Развитие цифровой экономики в России: преимущества и недостатки / Т. В. Трофимова, О. А. Шулешова // Научно-практический электронный журнал Аллея Науки. – Н. Новгород, 2018. - № 9(25). – Режим доступа: https://cyberleninka.ru/article/n/tsifrovaya-ekonomika-dostoinstva-i-nedostatki-perspektivy-razvitiya-i-praktika-primeneniya. – 15.10.2020.

УДК 004.052

Степанов Алексей Геннадьевич
направление Информационные технологии в управлении бизнес-архитектурой (магистратура), гр. ПИм-21

Научный руководитель
Еклашева Ольга Витальевна
канд.экон.наук,доценткафедры ИСЭ
ФГБОУ ВО «Поволжский государственный технологический университет», г.Йошкар-Ола

ИСПОЛЬЗОВАНИЕ МАШИННОГО ОБУЧЕНИЯВ ВИДЕОИГРОВОЙ ИНДУСТРИИ

Не так давно началось активное развитие машинного обучения. Программное на его основе имеет огромный потенциал, поэтому важно изучать данное направление. Одной из возможных сфер применения является создание видеоигр.Их разработка - один из наиболее распространённых элементов индустрии развлечений. Его размах можно сравнить, с производством фильмов. Исходя из данной актуальности эту отрасль следует постоянно модернизировать, чтобы

создавать более качественные продукты. Рассмотрению использованиямашинного обучения для этой цели и будет посвящена данная работа.

Крупные коммерческие игровые продукты делаютсябольшимколичеством профессионалов. В этой индустрии, как и во многих других появляется практика использования нейросетей. Машинное обучениесчитается этапом развития искусственного интеллекта [2]. Основная идея машинного обучения заключается в том, чтобы компьютер не просто использовал написанный алгоритм, а сам обучился решению поставленной задачи [1].

Одними из компаний использующих данную технологию является Valve. Онивнедрили технологию искусственного интеллекта в античит, определяющий нечестных игроков,совей игры еще в начале 2018 года.Нейросетьанализирующаядействияигроковв режиме реального времени называетсяVACnet.Её Обучение происходит на базе проекта «Патруль», помогающим в их нахождении, копируя спорные моменты, отправленные на рассмотрение модераторам. Игроки обозначают подтверждённые случаи жульничества, после чего нейронная система запоминает их и самостоятельно делает выводы в случае обнаружения схожих ситуаций.

Другим примером использования нейронных сетей для упрощения разработки может послужить авиасимуляторMicrosoftFlightSimulator 2020 года. В нём воссоздан весь земной шар, но вручную разработчики создавали модели только наиболее известных объектов. Весь остальной мир был заполнен домами и деревьями при помощи алгоритмов автоматической генерации.Анализируя спутниковые снимки, нейронные сети разбивают их на фрагменты, а затем вычленяют и классифицируют здания, дороги и растительность.Его внешние особенности — например, цвет фасада или дизайн окон — задаются с учетом географического расположения постройки. В общей сложности нейросети распознали и создали виртуальные копии примерно для 1.5 миллиарда зданий.Это позволило разработчикам FlightSimulator сэкономить множество времени и денег и сосредоточиться на самой важной части — на симуляции полёта.

Ещё одной компанией, сумевшей сократить время на разработку при помощи машинного обучения, является CD Projekt RED.Она использовала технологию JALI, которая помогает делать лицевую анимацию неигровым персонажам максимально эффективно и быстро.JALI - это программное обеспечение с использованием машинного обучения для автоматического создания лицевой анимации.

Она упрощает процесс создания правдоподобной анимации лица для множества второстепенных персонажей, не прибегая к технологии захвата движения, для чего потребовалось бы колоссальное количество времени, актеров и денег. JALI способна оптимизировать мимику персонажа в зависимости от языка, на котором он будет разговаривать. Другими словами, мимика одного и того же персонажа будет выглядеть по-разному в русской и, допустим, японской локализациях. На данный момент поддерживается около 11 языков

Эти примеры подтверждают, что использование машинное обучение может облегчит многие сферы человеческой жизни. Поэтому компаниям, желающим преуспеть в своей области стоит обратить внимание на данную технологию. Она имеет множество применений в многостороннем деле разработки видеоигр.Одним из важных преимуществ является значительно сокращение времени на создание и расходов, что очень важно в современной экономике. К её плюсам можно отнести также возможность решать задачи трудноисполнимые при помощи обычного программного обеспечения.

Список литературы:

1. С.А.Шумский. Машинный интеллект. Очерки по теории машинного обучения и искусственного интеллекта. -М., РИОР, 2019. - 339 с.
2. Т.Рашид. Создаём нейронную сеть. Математические идеи, лежащие в основе нейронных сетей, и поэтапное создание собственной нейронной сети на языке Python. // Вильямс, 2018. – 274 с.

УДК 371.693.4

Томуров Павел Дмитриевич,
направление Информатика и вычислительная техника (магистратура), профиль Программное обеспечение мобильных систем, гр. ИВТм-12
Ульянкин Никита Алексеевич,
направление Информатика и вычислительная техника (бакалавриат), гр. ИВТ-41

Научный руководитель
Танрывердиев Илья Оруджевич,
канд. техн. наук, доцент, кафедра проектирования и производства ЭВС
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ВИРТУАЛЬНАЯ ОБУЧАЮЩАЯ СРЕДА ДЛЯ СПОРТИВНОЙ ПОДГОТОВКИ ЧЕЛОВЕКА

Цель работы – исключение проблемы травматизма детей на этапе освоения спортивных базовых элементов, повышение эффективности

тренировок и сокращение сроков обучения детей спортивным базовым элементам.

Виртуальная обучающая среда – это часть системы для обучения детей спортивным базовым элементам с применением VR-систем[1]. Эта система представляет собой аппаратно-программный комплекс, который в VR- среде имитирует тренировки, с особенностями, которые делают их максимально приближёнными к реальным. Есть множество спортивных симуляторов, но в них отсутствует элемент обучения. В симуляторах с элементом обучения отсутствует спортивный тренировочный процесс. Они разработаны для области медицины, транспорта и военной промышленности.

Идея работы заключается в совокупности элемента обучения и формирования устойчивых когнитивных структур в пределах одной системы.

Аналоги.

1. Классификация двигательных ошибок для обеспечения обратной связи в режиме реального времени для спортивных тренировок в виртуальной реальности - тематическое исследование в приседаниях и толчках Тай-Чи.

Известен способ «Классификация двигательных ошибок для обеспечения обратной связи в режиме реального времени для спортивных тренировок в виртуальной реальности - тематическое исследование в приседаниях и толчках Тай-Чи» (Classification of motor errors to provide real-time feedback for sports coaching in virtual reality — A case study in squats and Tai Chi pushes) [2].

В данном способе реализуется среда обучения, в которой реализуется новый, интерпретируемый и работающий в режиме реального времени конвейер для классификации ошибок пользователя. Данный конвейер может автоматически генерировать расширенную обратную связь в реальном времени на основе движения обучаемого. Реализована словесная и визуальная обратная связь.

Таким образом, данный аппаратно-программный комплекс содержит элемент обучения, конвейер классификации ошибок, подсказывает пользователю, как сделать упражнение правильно. Помимо этого, в приложении есть слуховая и визуальная обратные связи.Однако в данной среде отсутствуют условия, которые делают виртуальные тренировки максимально приближенными к реальным, что в свою очередь скажется на правильном формировании устойчивых когнитивных структур.

2. Аппаратно-программный комплекс «Тренажёр ранней вертикализации пациентов после инсульта «Ревайвер» «(ReviVR)».

Известен способ «Аппаратно-программный комплекс «Тренажёр ранней вертикализации пациентов после инсульта «Ревайвер» «(ReviVR)»[3].

Аппаратно-программный комплекс «Ревайвер» – тренажер для медицинской реабилитации пациентов с нарушениями движений в нижних конечностях. Представляет собой аппаратно-программный комплекс, основанный на комбинировании технологии виртуальной реальности и биологической обратной связи в виде тактильной обратной связи.АПК предназначен для выполнения реабилитационных курсов, позволяющих совместить визуальное восприятие пациента, возникающее при просмотре процесса ходьбы от первого лица в сцене виртуальной реальности, и тактильные ощущения от давления пневмокамер на стопы пациента.

Таким образом, данный аппаратно-программный комплекс восстанавливает когнитивные структуры, развивает их. Помимо этого, в приложении есть система постановки задач для испытуемого, тактильная и визуальная обратные связи. Однако отсутствует элемент обучения.

Программное обеспечение виртуальной обучающей среды.

Разработка программного обеспечения системы планируется на движке Unity 3D. Приложение состоит из графического интерфейса и виртуальной обучающей среды. Оно реализовано посредством объединения сцен.

Есть два варианта работы с приложением: работа в главном меню и тренировка.

В главном меню доступны следующие опции:

1. Запуск комплекса упражнений - это тренировка.
2. Настройка различных параметров программы (локализация, яркость, громкость).
3. Просмотр информации о приложении.
4. Обучение работе с приложением.

Чтобы начать взаимодействие непосредственно с виртуальной обучающей средой, нужно надеть систему захвата движений и очки виртуальной реальности, подключить это всё к компьютеру и начать тренировку.

Тренировочный комплекс состоит из трёх упражнений:

1. Упражнение «Начальное положение».
2. Упражнение «Передача паса».
3. Упражнение «Приём паса».

Благодаря проверке выполнения упражнений, системе оценки правильности выполнения и зрительным стимулам, на виртуальных

тренировочных сеансах создаются условия, максимально близкие к реальным тренировкам.

Архитектура.

Архитектура программного обеспечения виртуальной обучающей среды представлена на рис. 1:

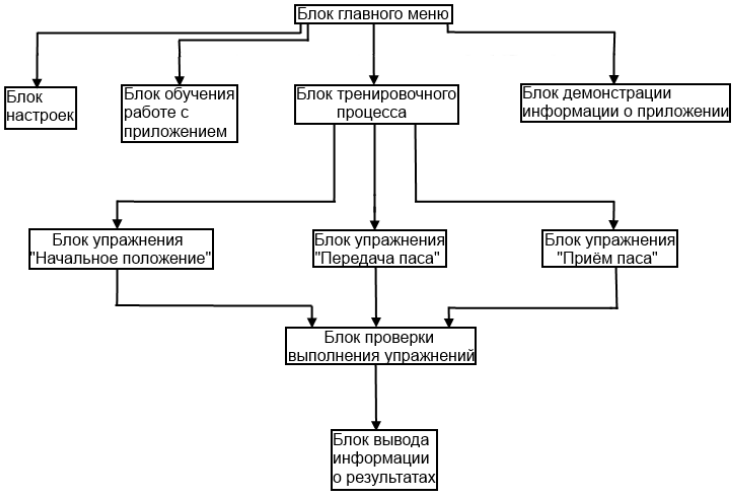


Рис.1 Архитектура программного обеспечения

Список литературы:

1. Танрывердиев И. О., Томуров П.Д., Ульянкин Н.А. Способ для обучения детей спортивным базовым элементам с применением VR-систем // Инженерные кадры – будущее инновационной экономики России. – 2019. – С. 134–136.

2. F. Hülsmann, J. P. Göpfert, B. Hammer, S. Kopp, M. Botsch Classification of motor errors to provide real-time feedback for sports coaching in virtual reality — A case study in squats and Tai Chi pushes // Computers & Graphics,(2018), с. 47-59 URL: https://www.sciencedirect.com/science/article/abs/pii/S0097849318301304#fig0003

3. Руководство по эксплуатации. Аппаратно-программный комплекс тренажер для реабилитации пациентов в раннем периоде после инсульта «Ревайвер» [Электронный ресурс] URL: https://smuit.ru/files/REVIVR-documentation.pdf

УДК 621.865.8

Торбеев Дмитрий Алексеевич
направление Информатика и вычислительная техника(магистратура),
гр.ИВТм-11

Научный руководитель **Васяева Елена Семеновна,**
канд.тех. наук, доцент, кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственных технологический университет», г. Йошкар-Ола

К ВОПРОСУ РАЗРАБОТКИ СИСТЕМЫ УПРАВЛЕНИЯ РОБОТОМ МАНИПУЛЯТОРОМ

Цель работы – Разработать управляющую программу, позволяющую управлять приводами робота–манипулятора с обеспечением поддержания заданного положения манипулятора.

В состав робота–манипулятора входит механическая часть (включающая звенья манипулятора), система управления приводами механической части.

Исполнительный механизм манипулятора, представляет собой открытую кинематическую цепь, звенья которой последовательно соединены между собой сочленениями различного типа (вращательные либо поступательные). Комбинация и взаимное расположение звеньев и сочленений определяет число степеней подвижности, а также область действия захвата робота. Зачастую предполагается, что первые три сочленения в исполнительном механизме манипулятора обеспечивают транспортные степени подвижности (обеспечивая перемещение рабочего органа в требуемое положение), а остальные сочленения – реализуют ориентирующие степени подвижности (ориентируя рабочий орган согласно заданию)[1].

На крайнем звене манипулятора будетрасполагается рабочий орган – устройство, выполняющее захватывающую функцию. Такое устройство как схватнапоминает кисть человеческой руки: захват объекта осуществляется с помощью механических «пальцев». По способу удержания объекта необходимо захватное устройство удерживающего типа, на объект будет оказано силовое воздействие за счёт различных физических эффектов.

Система управления данным роботом должна обеспечивать поставленную задачу – возможность игры в шашки, а именно: иметь программу для считывания сигналов распознавания местоположения и

типа шашек с шахматной доски;иметь по меньшей мере одну игровуюпрограмму, предназначенную для проведения соответствующей игры в шашки с учетом распознанных местоположений и типов фигур; программу управления манипулятором для перемещения игровых фигур с возможностью их взятия по сигналам от игровой программы.

В настоящее время известны различные манипуляторы, снабженные захватами для захватывания и перемещения различных предметов, наиболее подходящие модели описаны в следующих патентах:

Патент №3715140 (опубл. 24.11.1988) - погрузочное устройство, содержащее два пальца в виде параллельных стержней на концах двух элементов, сходящихся и расходящихся по направляющим. Такая конструкция имеет весьма ограниченное применение, поскольку ею неудобно захватывать предметы с криволинейной поверхностью. Кроме того, этому устройству необходимо значительное пространство для обеспечения возможности раздвигания стержней.

Патент №4398720 (опубл. 16.08.1983) - игра, которая проводится на доске с магнитами под каждым квадратом и с помощью снабженных магнитами фигур. Манипулятор имеет два перемещаемых в горизонтальной плоскости плеча, причем перемещения плеч производятся с помощью тросиков, которые тянутся соответствующими сервоприводами. Захват представляет собой три расположенных по кругу пальца, загнутых на обоих концах внутрь этого круга.Этот аналог имеет следующие недостатки. Использование магнитов в доске и фигурах может привести к тому, что фигура встанет не в центре клетки или притянется к соседней клетке или фигуре. При этом манипулятору необходимо каждый раз преодолеватьпритяжение магнитов для отделения фигуры от доски, что требует увеличения мощности соответствующего привода, а, следовательно, и его веса.[7].

Выводы

Для управления разрабатываемым устройством необходимо применение вычислительного устройства. Таким устройством может служить микроконтроллер для выполнения следующих функций: принятие сигналов обратных связей по току и скорости двигателей, вычисление регуляторы двигателей, управление двигателями, выдача управляющих сигналов на драйверы двигателей. Самые распространенные на рынке микроконтроллеры, имеющие положительные отзывы и соответствующий предполагаемым требованиям – AVR, STM32, TI.

Список литературы:

1. А. Г. Схиртладзе, В. И. Выходец, Н. И. Никифоров Классификация и структура промышленных роботов [Электронный ресурс]. – Режим доступа: http://www.metal-working.ru/.
2. Промышленный робот [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki.
3. Анализ современного состояния применения роботов в промышленности [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki
4. А. Г. Схиртладзе, В. И. Выходец, Н. И. Никифоров Классификация и структура промышленных роботов [Электронный ресурс]. – Режим доступа: http://www.metal-working.ru/.
5. T. K. Ten. KateF. LiefhebberA. H. G. Versluis J. A. van. Woerden Collaborative Control of the Manus Manipulator [Электронныйресурс]. – Режимдоступа: https://link.springer.com/.
6. B.J.F. Driessen, ing J.A. van Woerden Enhancing the usability of the MANUS manipulator by using visual servoing [Электронныйресурс]. – Режимдоступа: http://citeseerx.ist.psu.edu/.
7. Патент РФ №2008105538/22, 2008.02.18Захват манипулятора, манипулятор и робот для настольных игр// Патент России № 75319. 2008. Бюл. № 2. Костенюк К.В., Магомедов Д.З.

УДК 004.942

Угрюмов Станислав Сергеевич
направление Информационные системы и технологии (бакалавриат),
гр. 5838
ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения»,
г. Санкт-Петербург

Научный руководитель **Угрюмов Сергей Алексеевич**,
д-р техн. наук, профессор кафедры технологических процессов и машин лесного комплекса
ФГБОУ ВО «Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова»,
г. Санкт-Петербург

АВТОМАТИЗАЦИЯРАСЧЕТА ПРОИЗВОДИТЕЛЬНОСТИМНОГООПЕРАЦИОННЫХ ЛЕСНЫХ МАШИН

Введение. В современном лесозаготовительном производствеприменяются различные технологии и оборудование, на

выбор которыхоказывают влияниепараметры древостоев, природно-почвенные условия работы, требуемые объемы заготавливаемой и перерабатываемой древесины, уровень оснащенности техникой и организации труда [1]. Основными задачами современного развития лесного комплекса является совершенствование технического уровня производства, рациональное и комплексное использование древесины с максимальным использованием и переработкой образующихся древесных отходов, повышение производительности работы основного оборудования. В настоящее время в технологических процессах лесозаготовки как за рубежом, так и в нашей стране активно применяются многооперационные лесные машины (харвестеры и форвардеры), которыеосуществляют заготовку и транспортировку древесину с высокой производительностью при снижении производственных затрат в расчете на единицу выпускаемой продукции.

В практических задачах подбора оборудования и оптимизации технологических процессов лесозаготовки и транспортирования древесины важно знать производительность применяемого оборудования, или оборудования, планируемого к применению, а также технологические параметры, которыми можно управлять для корректировки производительности, как правило, в сторону ее увеличения.

Расчет производительности лесозаготовительного и транспортного оборудованияв большинстве случаев трудоемок и значителен по времени. Кроме этого, зачастую при оценке производительности трудно отыскать тот или иной технический параметр, требующийся для расчета.

Целью работы является упрощение расчета производительности многооперационных лесных машин и транспортного оборудованияпутем автоматизации расчетов и автоматизированного выбораэффективных марок лесных машин на основе расчетной производительности.

Результаты работы.В данной работе для упрощения расчетов производительности лесных машин была использована программа VisualStudio 2019, работающая на операционной системеWindows. Результатом работы программы является автоматизация процесса расчета производительности по известным в технической литературе зависимостям с рекомендацией оптимальной маркии фирмы-производителя лесозаготовительныхили транспортных машин.

При разработке кода программыбыли заведены формулы расчета производительности харвестеров и форвардеров.

Для иллюстрации работы программыприведены результаты автоматизации расчета производительности форвардера. По среднестатистическим данным на сплошных рубках при работе форвардерапосле харвестерасредняя часовая производительность составляет 17,0 м^3/ч [2].

При автоматизации расчета производительности форвардера использовали основные расчетные формулы [3,4]:

$$П_{см} = \frac{(T - t_{п.з} - t_{от})\varphi V_п}{t_ц}; \quad (1)$$

где T – время смены, мин;

$t_{п.з}$ – время на подготовительно-заключительные операции, мин;

$t_{от}$– время отдыха, мин;

φ – коэффициент учитывающий заполнение пачки, φ =0,8…0,9;

$V_п$ – объем транспортируемой пачки, м^3;

$t_ц$ – время цикла работы форвардера, мин.

$$t_ц = t_х + t_н + t_{гр} + t_п, \quad (2)$$

где $t_х$ – время движения от разгрузочного пункта к пачке, мин;

$t_н$ – время на набор пачки, мин;

$t_{гр}$ – время на движение в загрузочном состояние, мин;

$t_п$– время на перегрузку пачки с форфардера в автомобиль, мин.

При составлении кода программы были учтены исходные данные для расчета размерных характеристик деревьев, хлыстов и сортиментов, заведены формулы расчета продолжительности цикла работы форвардера и его производительности за различные временные промежутки (час, смена, сутки). В базу данных заведена библиотека форвардеров основных фирм-производителей с указанием базовых технических данных.

Для примера на рис. 1 приведен фрагмент кода разработанной программы.

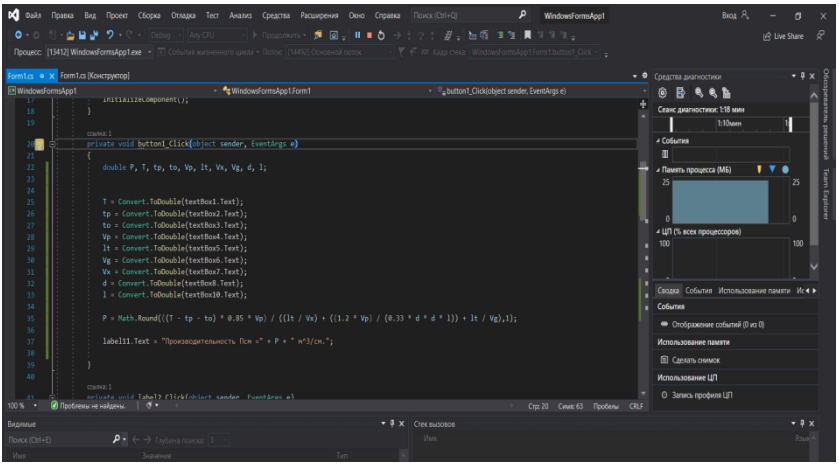


Рис.1. Фрагмент кода разработанной программы

По итогу расчета выдается окно, в котором отображается информация по использованным при расчетеисходным данным (временные затраты внутри цикла работы, объем транспортируемой пачки, расстояние транспортировки и др.), а также результат расчета производительности форвардера для принятых условий эксплуатации.Пример визуализации итога расчетов представлен на рис. 2.

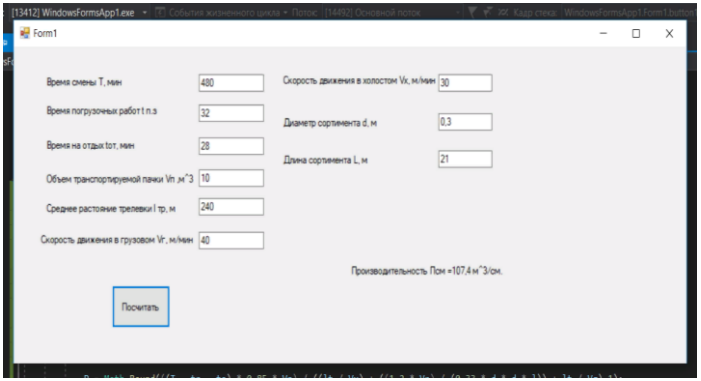


Рис. 2. Фрагмент визуализации итога расчета производительности форвардера

Выводы. Разработаннаяпрограмма для автоматизации расчета производительности лесозаготовительных и транспортных машин позволяет существенно упростить процесс расчета производительности

и подбора марки лесозаготовительного и транспортного оборудования с экономией времени. Программа автоматизированного расчета производительностихарвестеров и форвардеров позволяет оптимизировать расчет и выбор комплекта оборудования для выполнения лесозаготовок и транспортирования древесины в зависимости от размерно-качественных параметров древостоя и выбранной технологии заготовки древесины.

Список литературы:

1. Технология и оборудование лесопромышленных производств. Технология и машины лесосечных работ / под ред. В.И. Патякина. – СПб: СПбГЛТУ, 2010. - 330 с.
2. Шелепов В.В. Сортиментная заготовка древесины / В.В. Шелепов. − Кострома: КГУ, 2010. − 53 с.
3. Волдаев М.Н. Проектирование лесозаготовительных и деревоперерабатывающих производств лесного комплекса / М.Н. Волдаев. – Йошкар-Ола: ПГТУ, 2017. – 92 с.
4. Ширнин Ю.А. Технологические расчеты лесопромышленных производств / Ю. А. Ширнин [и др.]. – Йошкар-Ола: ПГТУ, 2017. – 192 с.

УДК 004.056.57

Фомин Евгений Вячеславович
направление Информационная безопасность (аспирантура)

Научный руководитель **Сидоркина Ирина Геннадьевна**
д-р техн. наук, профессор кафедры информационной безопасности
ФГБОУ ВО "Поволжский государственный технологический университет", г. Йошкар-Олы

АНАЛИЗ КЛАССИФИКАЦИИ ДЕСТРУКТИВНЫХ ПРОГРАММ

Персональные компьютеры стали незаменимыми автоматизированными карманными помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Но из-за массового использования вычислительных средств в разных аспектах жизни, обострило проблему защиты информации и к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе системы, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Компьютерный вирус — один из наиболее распространенных и едва ли не самых серьёзных деструктивных программ, которые

представляют значимую угрозу информации в современных информационных системах[1].

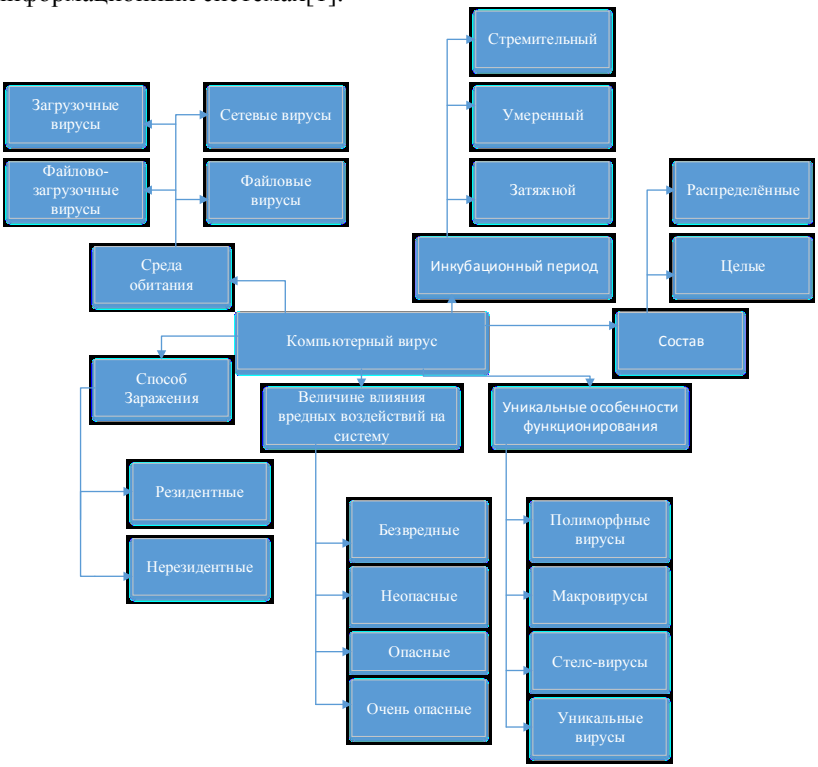


Рис. 1. Графическая модель классификации компьютерных вирусов.

Классифицировать компьютерные вирусов в зависимости от среды обитания можно на:

- **Сетевые вирусы** используют для своего распространения сетевые протоколы передачи информации или электронные почты

- **Файловые вирусы** заражают главным образом в исполняемые модули расширениями .exe, .com .bin, .ovl и т.д. Но могут внедряться и в другие типы файлов. Код зараженной программы обычно изменяется таким образом, чтобы вирус получил управление первым, до начала работы программы-носителя. При передаче управления вирусу он находит новую программу и выполняет вставку своей копии в нее.

- **Загрузочные вирусы** внедряются в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик жесткого диска, либо

меняют указатель на активный boot-сектор. Они заражают жесткие и гибкие диски. В отличие от файлового вируса он состоит из двух раздельных секций: головы и хвоста. Положение головы вируса всегда одинаково — она расположена в Boot секторе.

Классифицировать компьютерные вирусов по способу заражения можно на:

- Резидентные вирусы способны заполнять своими копиями всю оперативную память, перехватывать события и инициировать процедуры заражения обнаруженных объектов[2].

- Нерезидентные вирусы не оставляют своих резидентных частей в оперативной памяти компьютера и не способны дальнейше размножаться. Активны только в момент запуска зараженной программы.

Классифицировать компьютерные вирусы по деструктивным возможностямможно на:

- Безвредные вирусы. Вирусы не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

- Неопасные вирусы. Вирусы, влияние которых ограничивается уменьшением свободной памяти на логическом диске;

- Опасные вирусы. Вирусы которые могут привести к серьезным последствиям в работе компьютера при реализации функционирования вируса;

- Очень опасные вирусы. Вирусы в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже повредить аппаратные средства компьютера.

Классифицировать компьютерные вирусы по особенностям алгоритма работы можно на:

- Полиморфные вирусы. Достаточно труднообнаружимые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика[2].

- Макровирусы. Заражают файлы документов, содержащие в своем составе программный код макрорасширений. Большинство макровирусов можно считать резидентными, поскольку они присутствуют в области системных макросов в течение всего времени

работы редактора. Они, так же как резидентные, загрузочные и файловые вирусы, перехватывают системные события и используют их для своего размножения. К подобным событиям относятся различные системные вызовы, возникающие при работе с документами Word и таблицами Excel;

- Stels-вирусы. Алгоритмы работы данной категории вирусов позволяет полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо "подставляют" вместо себя незараженные участки информации[3]

- Уникальные вирусы. Часто используются для точечного получения НСД в системе. В алгоритмах функционирования такого вируса заложена основная задача как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса и т.д.

Классифицировать компьютерные вирусы по своему составу можно на:

- **Целые.** Вредоносное ПО представляет собой целый единый блок.

- **Распределённые.** Вредоносное программное обеспечение разделено на блоки, представляющие собой инструкции для воссоединения в единую целостную вредоносную систему[1].

Классифицировать компьютерные вирусы по инкубационному периоду можно на:

- Затяжной. Период, характеризующийся долговременным проявлением вируса в системе. Такое вредоносное ПО, начинает свое вредное воздействие на зараженную систему спустя некоторое время или при определённых условиях. Именно вирусы с затяжным инкубационным периодом сложнее всего обнаружить в системе. Известным примером таких вирусов являются трояны.

- Умеренный. Период, характеризующийся проявлением вируса в среднем темпе. Вредоносное ПО внедрившись в систему начинает собирать, анализировать, размножаться, передавать злоумышленнику данные обрабатываемые в компьютере. Известными примерами таких вирусов являются черви.

- Стремительный. Период, характеризующийся быстрым проявлением вируса в системе и приводящий систему в неэксплуатируемое состояние. Известным примером такого вируса является вирус Triada.

Заключение

Теперь имея чёткое представление о различных типах вредоносных программ следует сделать вывод, что даже несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.. Рекомендуется всегда устанавливать такой антивирус, который имеет высокий уровень обнаружения и сможет не только обеспечить защиту от всех известных угроз, но и возможность блокировать неизвестные угрозы. Не следует устанавливать пиратское программное обеспечение с встроенной лицензией или кейлогерами. Действуйте аккуратно при посещении торрентов, сайтов с азартными играми и т.п. Всегда следите за обновлениями операционной системы и установленного ПО, убедитесь, что брандмауэр включен. При установке бесплатного программного обеспечения следите за тем, что предлагается установить помимо основной программы, не спешите нажимать кнопку «Далее» во время установки. Снимайте все галочки напротив предлагаемых дополнительных установок, не относящихся к данной программе.

Список литературы:

1. Коэн Ф."Компьютерные вирусы — теория и эксперименты." 2004 г.
2. Классификация вредоносных программ. URL Доступа: https://www.kaspersky.ru/blog/klassifikaciya-vredonosnyx-programm/2200/
3. "Что такое компьютерные вирусы, и как они работают?" Том 5, М.: Диалог-МИФИ, 1996, 256 стр.

УДК 67.017

Ханина Юлия Александровна
направление Материаловедение и технологии
материалов(бакалавриат),гр.МТМ-41

Научный руководитель **Алибеков Сергей Якубович,**
канд. техн. наук,профессор кафедры машиностроения и материаловедения
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА УСТРОЙСТВА ДЛЯ НАНЕСЕНИЯ ЗАЩИТНО-ДЕКОРАТИВНЫХ ПОКРЫТИЙ ЦИНКОСОДЕРЖАЩИМИ ЭЛЕКТРОЛИТАМИ

Установка, позволяющая равномерно нанести цинкосодержащее покрытие на внутренние поверхности длинномерных полых изделий с использованием новых электролитов, содержащих цинк с различными

полимерными материалами, позволяющих повысить прочность сцепления цинкового покрытия и качество покрытия.

Цель выполнения проекта: разработка способа нанесения покрытий на внутренние поверхности длинномерных полых изделий (труб, профилей) с целью увеличения срока службы, повышение качества покрытий, снижение себестоимости и повышение экологической безопасности, повышение срока службы труб, трубопроводов, емкостей, деталей машин, инженерных сооружений, используемых в нефтегазовой, теплоэнергетической, машиностроительной отраслях промышленности, уменьшение себестоимости нанесения покрытий

Цинковые покрытия являются самыми распространенными защитно-декоративными покрытиями для предохранения от коррозии, как черных, так и, цветных металлов и сплавов. Цинковые покрытия по отношению к многим металлам и сплавам являются анодом, поэтому пока есть хотя бы 10% покрытие от общей площади, цинк защищает основу. Цинковые покрытия являются самыми дешевыми, поэтому являются экономически более выгодными и долгосрочными. Разработка новых способов нанесения на внутренние поверхности длинномерных полых изделий (труб, профилей) является актуальной задачей. В настоящее время, полые изделия покрывают цинком способом окунания в расплавы или электролиты. [1] Также существует множество способов нанесения на внутренние поверхности полых изделий цинковых покрытий:

1. Окунание
2. Распыление пульверизатором (на наружные поверхности), при котором расход электролита резко возрастает
3. Кистью или ершиком
4. Валиком
5. Горячее цинкование

При способе окунания длинномерных полых изделий в цинкосодержащие расплавы или электролиты, осуществляется путем окунания этих изделий. При таком способе нанесения покрытия, равномерность покрытия не гарантируется, на нижних поверхностях скапливается больше цинка и толщина покрытий выше. Расход расплавов цинка в этом случае резко возрастает.

Перед нанесением покрытия таким способом, с поверхности расплава необходимо удалять шлаки, поверхности изделий должны быть тщательно подготовлены и детали необходимо двигать в процессе покрытия с целью равномерного распределения покрытия на внутренние поверхности. Температура расплава должна быть

постоянной, чтобы цинк находился в жидком состоянии. Процесс покрытия является малопроизводительным и длительным.[2]

Предлагаемый способ лишен вышеуказанных недостатков, покрытия получаются равномерными, расход цинкосодержащих электролитов уменьшается, а производительность повышается, а также повышается экологичность процесса нанесения. Способ технически легко осуществим и экономически выгоден. Проведем сравнение стоимости. [Таблица 1]

Таблица 1

Способы	Средняя стоимость
Цинковое покрытие на подвесах	12 руб. за 1 $дм^2$
Спреевое покрытие	100 мл – 297,75 руб.
Окунание (до 3 тонн)	35 700 руб.

Предлагаемый способ на порядок дешевле аналогов примерно 3500р.

Устройство состоит из диффузора, распылителя с трубкой, из полимерного материала (поливинилхлорид).

Диффузор подается на начало трубы, в бункер засыпается цинкосодержащий электролит и подаётся воздух через трубку под давлением. Труба или полое изделие вращается, с целью равномерного нанесения цинкосодержащего покрытия. Диффузор равномерно распределяет цинкосодержащий электролит по внутренней поверхности покрываемого изделия, равномерно. Диффузор постепенно двигается внутри трубы от начала до конца, при этом, не происходит разбрызгивания цинкосодержащего электролита в окружающую среду, расход электролита уменьшается за счет снижения разбрызгивания в замкнутом пространстве. Для предотвращения провисания трубы с диффузором, на трубе предусматриваются кольца из полимерного материала (поливинилхлорид, полипропилен). Кольца имеют различные диаметры и формы, в зависимости от покрываемого изделия. За счет вращения самой трубы и равномерного разбрызгивания электролита под давлением, адгезия цинкосодержащего электролита, адгезия резко увеличивается.

Список литературы:

1. Шлугер М.А.,Ток Л.Д. Гальванические покрытия в машиностроении. Справочник. Под ред. М.А. Шлугера, Л.Д.Тока. – М.: Машиностроение, 1985: Том 2, – 248 с.

2. Пурин Б.А, Цера В.А., Озола Э.А., Витиня И.А, Комплексные электролиты в гальванотехнике. – Рига: Лиесма, 1978. – 267 с.

УДК 004.032.26

Черняев Александр Алексеевич
направление Информатика и Вычислительная техника (магистратура), гр. ИВТм-13

Научный руководитель **Савинов Александр Николаевич**,
к.т.н., доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА МЕТОДА И АЛГОРИТМА ПРОГНОЗИРОВАНИЯ ЭФФЕКТИВНОСТИ ТЕКСТОВОЙ РЕКЛАМЫ НА ОСНОВЕ ТЕОРЕМЫ БАЙЕСА

Цель работы –разработка метода и алгоритма прогнозирования эффективности текстовой рекламы на основе теоремы Байеса.

Тема актуальна в связи вшироким распространением рекламы во всех информационных каналах. Реклама стала неотъемлемой маркетинговой частью нашей жизни, и необходимо, чтобы она соответствовала интересам и запросам пользователей. В связи с этим актуальным становится решение задачи построения методов и алгоритмов оценки эффективности рекламы. По формуле Байеса можно прогнозировать эффективность разрабатываемой текстовой рекламы, которая возможно будет интересна пользователю по его поисковым запросам браузера (взяв в расчёт как ранее известную информацию, так и данные новых наблюдений).

Сегодня в сети Интернет размещаются колоссальные объемы информации. Определенная ее часть предоставляется в открытом доступе любому пользователю сети Интернет. На основании необходимости быстрого поиска релевантной информации выросла отдельная отрасль в сфере информационных технологий, а именно сфера предоставления поисковых услуг в сети Интернет для пользователей. Один из лидеров данной отрасли в мировом масштабе – компания Google обрабатывает порядка 41 млрд. 345 млн. пользовательских запросов в месяц. Разумеется, наиболее часто повторяющиеся поисковые запросы можно группировать и анализировать. А в случае удачного прогнозирования изменения величины конкретного поискового запроса можно определять будущие потребности пользователей сети Интернет.

Как правило, разработкой информационных систем прогнозирования занимаются коммерческие компании, результаты которых чаще всего

закрыты от публичного доступа. Однако исходные статистические данные находятся в открытом доступе и относительно просто могут быть получены посредством программных интерфейсов.

Объектом исследования являются поисковые запросы пользователей.

Предметом исследования являются разработка метода и алгоритма прогнозирования эффективности текстовой рекламы на основе теоремы Байеса.

Прогнозирование можно определить, как некую возможность предвидеть состояние исследуемого явления, произвести анализ состояния и будущего изменения свойств и характеристик исследуемого явления. Исходя из того, что любое решение, или прогноз – это проекция явления в будущее, а будущее – содержит элемент неопределенности, то важно при выборе методов и моделей прогнозирования адекватно оценивать в какой степени та или иная модель или метод соответствует реальной ситуации, и какого качества можно получить результат. Другими словами – с допустимой погрешностью или нет.

Для нашего исследования был выбран метод прогнозирования на основе теоремы Байеса. Теорему Байеса называют мощным методом создания нового знания, но её можно использовать и для рекламы.

Исследователи искусственного интеллекта, включая разработчиков робомобилей в Google, применяют ПО Байеса, чтобы помогать машинам распознавать закономерности и принимать решения. Байесовские программы, согласно Шэрон БёрщМакгрейн [SharonBertschMcGrayne], автору популярной истории теоремы Байеса, «сортируют емейл и спам, оценивают медицинские риски и государственную безопасность, расшифровывают ДНК, прочее». На сайте Edge.org физик Джон Мэтер беспокоится, что байесовые машины могут стать настолько умными, что вытеснят людей.

Теорема Байеса гласит, что вероятность наступления «события» при условии проведения «наблюдения» равна произведению вероятности наступления события и вероятности проведения наблюдения при условии наступления события, деленному на безусловную вероятность проведения наблюдения (см. рис. 1).

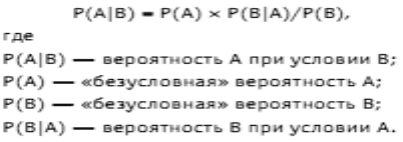


Рис. 1. Теорема Байеса

Самый простой пример — подбрасывание монетки. Если бы мы знали силу, с которой мы ее подбрасываем, ускорение, сопротивление воздуха, скорость ветра и всё-всё-всё, что может как-то повлиять на ее полет, мы бы могли сказать со 100-процентной вероятностью, куда она упадет. Но поскольку мы этого не знаем, мы подбрасываем ее миллион раз и говорим, что примерно половина из этого миллиона раз выпадет орел, а вторую половину раз — решка.

Предположим, решается вопрос о выпуске новойрекламы. Согласно данным за прошедшие периоды, новаярекламазаинтересовывала новых пользователей только в 30% случаев. Математик записал бы это утверждение следующим образом: P(FYP 1) = 30%, то есть вероятность заинтересовыванияновых пользователейпри выпуске рекламы составляет 30%. Нередко при выпуске рекламы в массы, происходит тестовый показ рекламы.Для всех случаев, когда новая реклама далахороший результат уже в первое время реализации, пробные рекламы были удачными только на 80%. Математик записал бы это следующим образом: P(S|FYP) = 80%, то есть «условная» вероятность успеха тестирования рекламы (S, successful — успешный) при условии, что рекламапоказала хороший результат уже при первых показах (черта «|» означает «при условии»), равна 80%.

Перепишем уравнение теоремы Байеса, подставив в него следующие обозначения интересующих нас функций:

•P(FYP|S) — вероятность привлечения новых пользователей при первых просмотрах рекламы при условии удачного тестирования рекламы, иными словами, вероятность наступления события FYP при условии S;

•P(FYP) — «безусловная» вероятность привлечения новых пользователей при первых показах;

•P(S) — «безусловная» вероятность удачного тестирования рекламы;

•P(S|FYP) — вероятность удачного тестирования рекламы при условии привлечения пользователей при первых показах.

Таким образом, в результате анализа в рамкахданной задачи, можно сказать что с помощью теоремы Байеса можно показывать рекламу, которая

с большей вероятностью заинтересует пользователя и которой он воспользуется. При разработке методики, основанной на использовании классического метода Байеса, сформулирован вывод, что для составления грамотной стратегии необходимо выполнить следующие этапы:

1) анализировать не менее чем 15 факторов, влияющих на эффективность рекламной информации;

2) формировать эффективные рекламные стратегии на основе компьютерного варьирования значений факторов с учетом соблюдения требований к критериям эффективности.

Список литературы:

1. https://habr.com/ru/post/404633/
2. http://www.bseu.by:8080/bitstream/edoc/80615/1/Prognozirovanie_v_reklame.pdf
3. https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0_%D0%91%D0%B0%D0%B9%D0%B5%D1%81%D0%B0#%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%B0%D1%8F_%D1%84%D0%BE%D1%80%D0%BC%D0%B0
4. https://www.marketing.spb.ru/lib-around/stat/bayesian.htm
5. http://elib.altstu.ru/journals/Files/pv2006_03_1/pdf/197borod.pdf
6. https://tass.ru/sci/6815287

УДК 004.932.2

Чеснокова Дарья Евгеньевна
направление Программная инженерия, гр. ПС-14

Научный руководитель **Чесноков Сергей Евгеньевич,**
к.т.н., доцент кафедры информатики
ФГБОУ ВО «Поволжский государственный технологический университет», г.Йошкар-Ола

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ОЦЕНКИ КАЧЕСТВА ИЗОБРАЖЕНИЙСИСТЕМЫ ВИДЕОАНАЛИТИКИ[1]

Цель работы – разработка программного модуля оценки качества изображений системы видеоаналитики проекта eVision

[1] Работа была выполнена при поддержке ООО «Лаборатория цифровой трансформации» (www.digtlab.ru).

(www.evision.tech) для исключения из обработки изображений с неприемлемым уровнем яркости/контрастности или искажений в виде размытия/смещения изображений относительно камеры.

Система видеоаналитики проекта eVision(рис.1.1) основана на технологии компьютерного зрения и позволяет получать видеопоток данных с нескольких подключенных камер видеонаблюдения. Этот видеопоток принимается и обрабатывается в режиме реального времени. Использование алгоритмов машинного обучения позволяет решать задачи идентификации лиц для систем управления доступом по биометрическим данным.

Структурная схема системы представлена на рис.1.1.

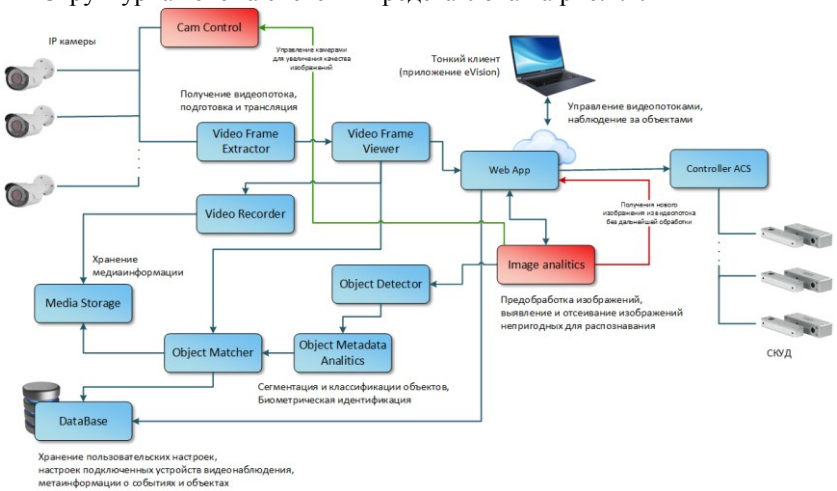


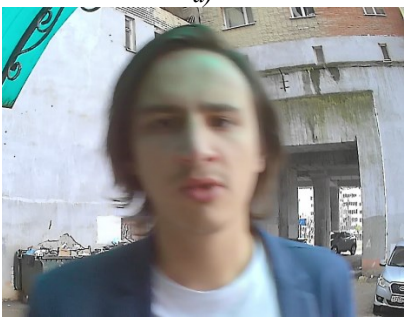
Рис.1. Сетевая система видеоаналитики eVision

Работа системы в режиме реального времени накладывает определенные ограничения на качество передаваемых на обработку изображений (нарезанных кадров видеопотока). Изображения должны быть приемлемого качества для выполнения операции идентификации человека по лицу [3].

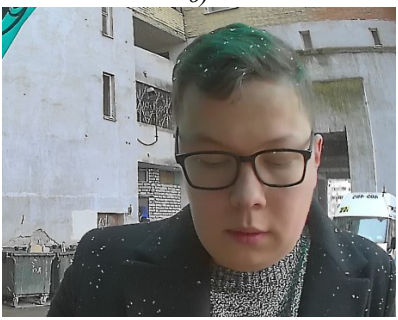
Данные в виде кадров видеопотока, получаемых с камер видеонаблюдения,являются неоднородными. На рис. 1.2 представлены изображения с одной из камер видеонаблюдения с искажениями и без них.

а)

б)



с)



д)

Рис.2. Изображения с камеры видеонаблюдения: *а* – изображение ночной сьемки с дефектом движения объекта (идентификация не производится); *б* – изображение ночной сьемки приемлемого качества; *с* – изображение дневной сьемки с искажением движения объекта (идентификация не производится); д - изображение дневной сьемки приемлемого качества.

В системе видеоаналитики используется частота поступления кадров не менее 25 кадров в секунду, поэтому обработка кадров, которые явно несут заметные искажения, не оправдана с точки зрения использования вычислительных ресурсов.

Модуль анализа изображений (рис.1.1) работает по заложенному алгоритму, и ему сложно дать общую оценку качества изображений. Для анализа изображений используются частные оценкиконтрастности и резкости изображений. Причем все оценки должны производиться в отсутствии эталонных изображений.

Оценка резкости изображения выполняется по алгоритму на основе анализа амплитудной составляющей спектра полученного изображения. В работе [4] дано описание этого алгоритма и исследованы границы выбора порогового значения в качестве параметра алгоритма.

Так как в модуле анализа изображений используется преобразование изображения к полутоновому (с точки зрения увеличения производительности системы), то подходящималгоритмом оценки контрастности является алгоритм вычисления яркостной контрастности изображения[1, 2]. Она определяется как дисперсия яркости пикселей изображения:

$$\sigma^2 = \frac{1}{N}\sum_{p=1}^{N}(Y_p - Y)^2, \quad (1)$$

где Y – среднее значение яркостной контрастности всего изображения, Y_p – значение яркостной контрастности в точке p, N–общее число точек изображения.

Оценка контрастности (1) нормируется путем вычисления отношения среднеквадратического отклонения к максимально возможному значению яркости:

$$C = \frac{2\sigma}{Y_{max}}. \quad (2)$$

Диапазон изменения значения C– [0;1]. Значение 0 соответствует однотонному изображению, значение 1 – максимально контрастному.

Выводы

В работе представлены алгоритмы оценки контрастности и резкости изображений, используемые в системе видеоаналитики для «отсеивания» изображений с существенными искажениями в модуле предобработки. На практике выявлено, что контрастность изображения не может являться единственным точным показателем качества изображения, так как размытые изображения менее информативны, но могут иметь большую степень контрастности, чем четные изображения, но с меньшим числом значений максимальной и минимальной яркости.

Предлагается использование комплексного критерия оценки качества по двум безэталонным оценкам резкости и контрастности изображений.

В качестве дальнейшего направления исследований планируется выполнить оценку времени выполненияалгоритма получения комплексной оценки качества изображений для системы видеоаналитики и провести его оптимизацию.

Список литературы:

1. Фисенко В.Т. Компьютерная обработка и распознавание изображений: учебное пособие / В.Т. Фисенко, Т.Ю. Фисенко - СПб: СПбГУ ИТМО, 2008. – 192 с.

2. Небаба С.Г. Тестирование технологии подготовки изображений лиц к распознаванию личности в видеопотоке в режиме реального времени // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки», 2017. №3-4. С. 73-77.
3. Kanjar D. Image Sharpness Measure for Blurred Images in Frequency Domain // International Conference on Design and Manufacturing. Procedia Engineering, 2013. P. 149-158.
4. Development of an effective algorithm for a standard-free evaluation of the sharpness of images of a video stream of a video analytics system // ЧесноковаДарьяЕвгеньевна, Чесноков Сергей Евгеньевич Slovak International Scientific Journal, №6, С.8-12, 2020 г.

УДК 004

Шайкин Андрей Владимирович
Направление « Информатика и вычислительная техника» (магистратура), гр. ИВТМ-01-20

Научный руководитель **Галанина Наталия Андреевна,**
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения информационных систем
ФГБОУ ВО "Чувашский государственный университет им. И.Н. Ульянова", г. Чебоксары

РАЗРАБОТКА МИКРОСЕРВИСА ДЛЯ ВИЗУАЛИЗАЦИИ ФОРМАЛИЗОВАННЫХ ДОКУМЕНТОВ

Актуальность. В настоящее время любая бухгалтерская операция должна оформляться первичным учетным документом. К первичным учетным документам относятся товарные накладные, акты выполненных работ и т. д. Система законодательных актов разрешает их составлять в электронном виде. Единым форматом для формализованных документов является XML [1]. Данный формат трудночитаем для человека.

Цель работы: разработка микросервиса для визуализации формализованных документов, поддерживающих актуальные приказы (Приказ 820, Приказ 552, Приказ 189, Приказ 55).

Для решения поставленной задачи был выбран высокоуровневый язык программирования Python (рис.1), интегрированная среда разработки PyCharm (рис.2) и DjangoFramework (рис.3).

Рис. 1. Логотип языка программирования Python

Рис. 2. Логотип PyCharm IDE

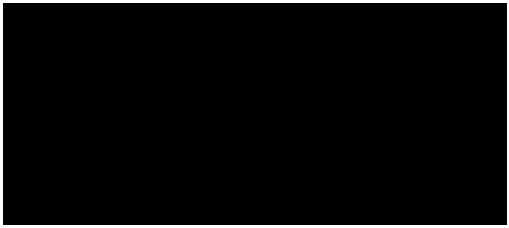


Рис. 3. Логотип DjangoFramework

Формализованный документ представляет собой XML-файл со строгой структурой, закрепленной законом [3-10]. Часть формализованного документа представлена на рис.4. Для обработки xml-структуры была использована библиотека lxml [4].

Рис. 4. Участок формализованного документа

Т.к. один и тот же формализованный документ может поддерживать несколько стандартов, то для унификации выходных данных было решено реализовать универсальный класс КоннекторДляФормализованныхДокументов (рис. 5) [2].

```
# noinspection NonAsciiCharacters
class КоннекторДляФормализованныйДокумент(
    Методы, ДополнительныеСвойства, Приказы,
    Исполнитель, Заказчик,
    ГрузПолучатель, ГрузОтправитель,
):
    def __init__(self, data: dict, document_type: str) -> None:
        self.ИсходныеДанные = data
        self.ТипДокумента = document_type
    @cached_property
    def Файл(self):
        return self.ИсходныеДанные["Файл"]
    @cached_property
    def Документ(self):
        return self.Файл["Документ"]
    @cached_property
    def Актуальный(self):
        return any({
            self.Приказ820,
            self.Приказ552,
            self.Приказ551,
            self.Приказ189,
        })
```

Рис. 5. Базовый класс КоннекторДляФормализованныхДокументов

Микросервис должен быть Restful, одной из главных особенностей которого является отсутствие состояний, т.е. точка доступа должна быть самодостаточна. Разработанные точки доступа приложения представлены на рис.6. Каждая точка доступа решает только свою задачу:

- token – точка доступа, отвечающая за получение и обновления JWT-токенов пользователей;
- rest – точка доступа для интеграции микросервиса с другими сервисами.

Точка доступа rest может быть разделена на разные версии, которые могут отличаться друг от друга. Разработанныймикросервис имеет одну версию точки доступа `rest`:

- info – точка доступа для получения информации о документе;
- stamp – точка доступа для внедрения графической отметки об электронной подписи в документ;
- conversion – точка доступа для преобразования документа и получения на выходе потока данных.

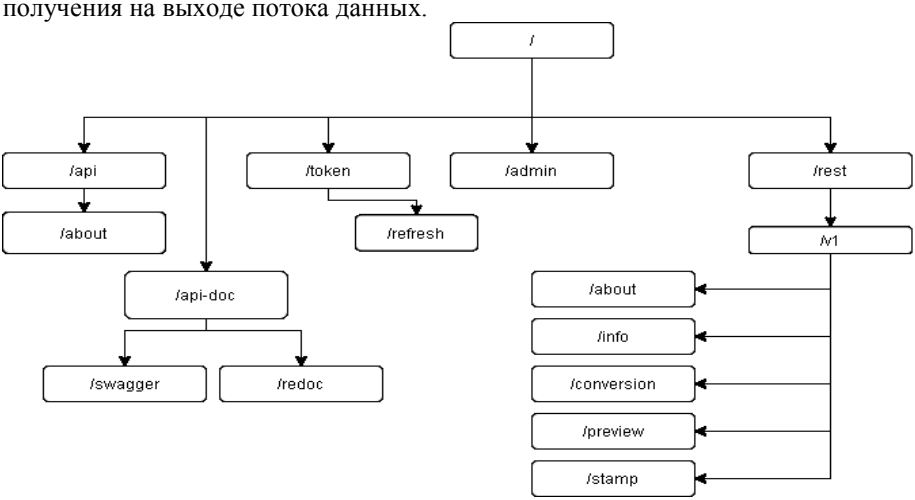


Рис. 6. Точки доступа микросервиса

Выводы. Разработанный микросервисRESTful позволяет визуализировать формализованный документ, поддерживающий актуальные приказы, в соответствии с которым он был построен. Графическое представление формализованного документа является

более читабельным и легко воспринимаемым для человеческого зрения, чем текстовый аналог (рис.7-8).

Приложение №1
к постановлению Правительства Российской Федерации
от 26.12.2011 №1137
(в ред. Постановления Правительства РФ от 19.08.2017 № 981)
(печатная форма может содержать дополнительные реквизиты)

Счет-фактура № 820 СЧФ от 01.02.2003 (1)

Продавец	Seller Organization	(2)
Адрес	Свердловская область	(2а)
ИНН/КПП продавца	ИНН/КПП 1234567894/667301001	(2б)
Грузоотправитель и его адрес	РЕАЛИЗОВАТЬ.	(3)
Грузополучатель и его адрес	РЕАЛИЗОВАТЬ.	(4)
К платежно-расчетным документам	№ СЧФ/123/456 от 01.02.2003	(5)
Покупатель	BuyerOrganization	(6)
Адрес	112,some-foreign-address	(6а)
ИНН/КПП покупателя	ИНН/КПП 1234567894/667301001	(6б)
Валюта: наименование, код	Российский рубль, 643	(7)
Идентификатор государственного контракта, договора (соглашения) (при наличии)		(8)
Доп.сведения	ДатаГен: 20.05.2019 14.32.21, ЗаказчикАдрес: 112,some-foreign-address, ИсполнительИНН: 1234567894, ЗаказчикИНН: 1234567894, ИсполнительКПП: 667301001, Заказчик: BuyerOrganization, ИсполнительАдрес: Свердловская область, ЗаказчикКПП: 667301001, Исполнитель: Seller Organization	

Наименование товара (описание выполненных работ, оказанных услуг), имущественного права	Код вида товара	Единица измерения		Количество (объем)	Цена (тариф) за единицу измерения	Стоимость товаров (работ, услуг), имущественных прав без налога - всего	В том числе сумма акциза	Налоговая ставка	Сумма налога	Стоимость товаров (работ, услуг), имущественных прав с налогом - всего	Страна происхождения товара		Регистрационный номер таможенной декларации
		Код	Условное обозначение (национальное)								Цифровой код	Краткое наименование	
1	1а	2	2а	3	4	5	6	7	8	9	10	10а	11
Стол	-	715	пар	15	20000	300000.00	1592.00	20%	0.00	-	980	-	-
Всего к оплате						-	-			345.00			

Рис. 7. Результат обработки микросервиса формализованного документа

Руководитель организации или иное уполномоченное лицо _____ (подпись) _____ (ф.и.о)

Главный бухгалтер или иное уполномоченное лицо _____ (подпись) _____ (ф.и.о)

Индивидуальный предприниматель или иное уполномоченное лицо _____ (подпись) _____ (ф.и.о) _____ (реквизиты свидетельства о государственной регистрации индивидуального предпринимателя)

АЛЬФА
Цифровой документооборот

Подписано ЭП
TEST-KSB
CAdES-X Long Type 1
Серийный номер 011f00ea004cab8db245936b18b1a193c9
Дата подписания 24.01.2020
Дата истечения сертификата 24.04.2020

Рис. 8. Внедренная в документ графическая отметка электронной подписи

Список литературы:

1. Иванова Н.Н. Математическая логика и теория алгоритмов / Н.Н. Иванова, Н.А. Галанина / Чебоксары: Изд-во Чуваш.ун-та, 2020.-188 с.

2. Шайкин А.В. Выбор онлайн-мессенджера для разработчика чат-бота / А.В. Шайкин, Н.А. Галанина // Человек и общество перед вызовами глобальных трансформаций. Двадцать третьи Вавиловские чтения: материалы международной междисциплинарной научной конференции: в 2ч. / под общ.ред. проф. В. П. Шалаева. – Йошкар-Ола: Поволжский государственный технологический университет, 2020 – Ч. 2 С. 147 – 153.

3. Галанина Н.А. Реализация блоков шифрации и дешифрации сигналов в непозиционных устройствах ЦОС / Н.А. Галанина, Н.Н. Иванова, А.А. Иванов / Вестник Чувашского университета, 2007.- № 2.- С. 209-216.

4. Введение в библиотеку Pythonlxml [Электронный ресурс]. Режим доступа: https://webdevblog.ru/vvedenie-v-biblioteku-python-lxml/
5. Товарная накладная [Электронный ресурс]. Режим доступа: https://www.diadoc.ru/docs/forms/first-documents/nakladnaya
6. Акт приемки-сдачи работ (услуг) [Электронный ресурс]. Режим доступа: https://www.diadoc.ru/docs/forms/first-documents/Act
7. Счет-фактура [Электронный ресурс]. Режим доступа: https://www.diadoc.ru/docs/forms/chet-f
8. Корректировочный счет-фактур [Электронный ресурс]. Режим доступа: https://www.diadoc.ru/docs/forms/ksf
9. Универсальный передаточный документ [Электронный ресурс]. Режим доступа: https://www.diadoc.ru/docs/forms/upd
10. Универсальный корректировочный документ [Электронный ресурс]: Режим доступа: https://www.diadoc.ru/docs/forms/ukd

УДК 004.896

Якушев Павел Юрьевич
направление Информатика и вычислительная техника(магистратура), гр.ИВТм-11

Научный руководитель **Васяева Наталья Семеновна,**
канд.тех. наук, кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственных технологический университет», г. Йошкар-Ола

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ СИСТЕМЫ ПРОВЕДЕНИЯ И ОРГАНИЗАЦИИ ФЕСТИВАЛЕЙ КОМПЛЕКСА«ГТО»

Цель работы – повышение эффективности за счет более удобного и комфортного процесса внесения результатов соревнований в систему.Основные задачи, которые будет решать мобильное приложение:

1. Более удобный процесс внесения результатов соревнований в системуГТО.
2. Возможность online просмотра своих результатов участниками соревнований и их тренерами.
3. Возможность быстрого расчета количества очков (в стобалльной системеГТО) при введении результата соревнования, для сдачи на медаль какой-либо ценности с помощью online калькулятора.
4. Работа с микросервисом распознавания лиц для регистрации участников.

Фестиваль ГТО представляет собой комплекс различных спортивных состязаний по разным видам спорта. В этих соревнованиях принимают участие от сотни до тысячи и более спортсменов разных возрастных категорий и полов. После прохождения каждого из испытаний, результаты участников вносятся впротокола, которые передаются секретарям. Они в свою очередь вручную конвертируют результаты спортсменов в стобальную шкалу при помощи таблицы оценки выполнения испытаний в рамках фестивалей “ГТО”, которая отнимает колоссальное количество времени из-за различия баллов за результат в зависимости от возраста и пола спортсмена. После конвертации всех результатов необходимо подсчитать количество баллов каждого участника и определить смог ли спортсмен выполнить нормативы и на какой именно значок ГТО.

Из-за однообразной и монотонной работы, у организаторов при данных операциях высок риск проставления ошибочных результатов участнику из-за невнимательности. Для устранения данных проблем существует WEB версия системы организации и проведения фестивалей комплекса “ГТО”. Но у данного решения есть один неучтенный недостаток - некоторые пользователи системы, не могут физически иметь при себе компьютер или даже ноутбук. Например, участник или тренер, да и секретарям в некоторых случаях легче вносить результаты с мобильного устройства.

Далее, на рисунках,представлены все варианты использования системы:

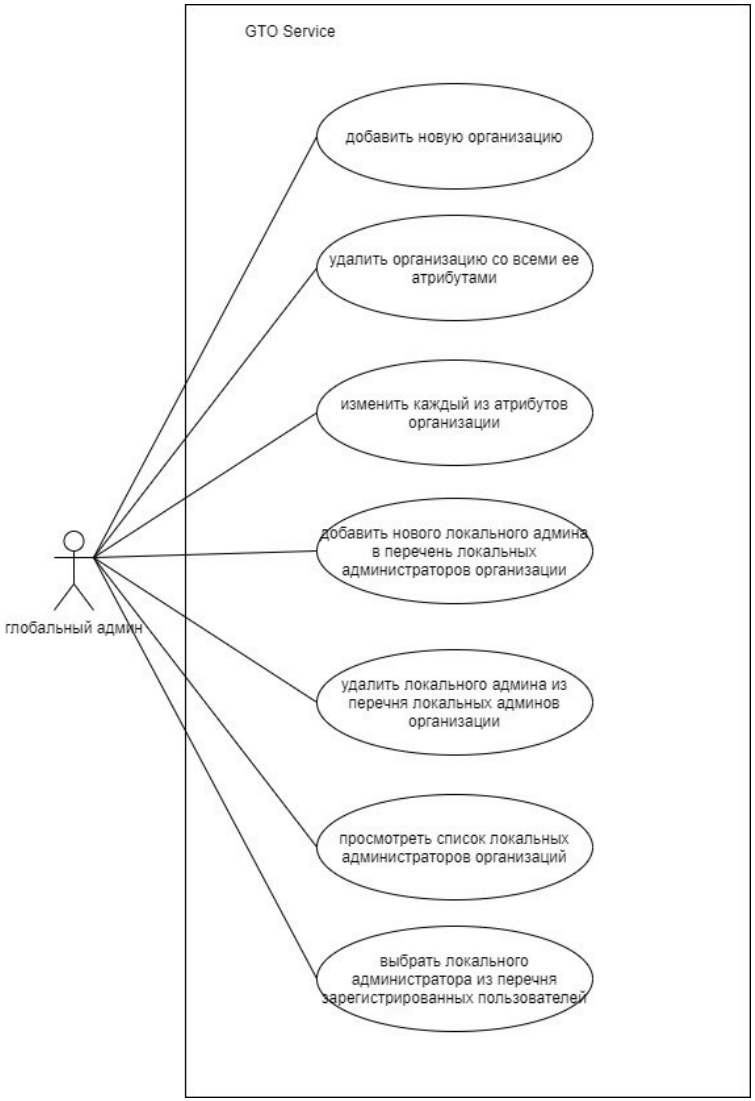


Рис 1. Диаграмма использования мобильного приложения системы проведения и организации фестивалей комплекса ГТО (Глобальный администратор)

Рис 2. Диаграмма использования мобильного приложения системы проведения и организации фестивалей комплекса ГТО (Локальный администратор)

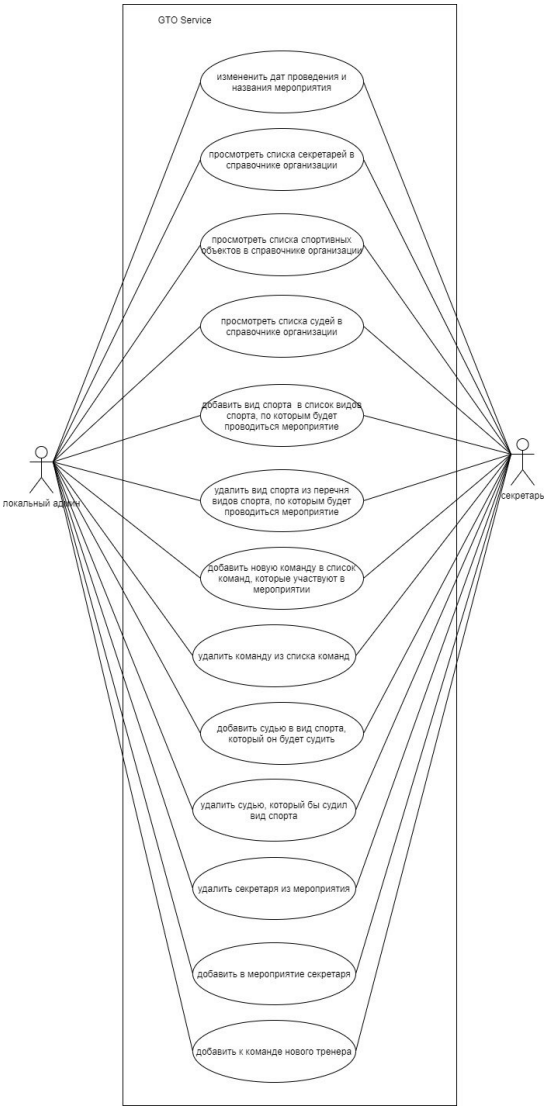


Рис 3. Диаграмма использования мобильного приложения системы проведения и организации фестивалей комплекса ГТО (Локальный администратор, Секретарь – общие кейсы)

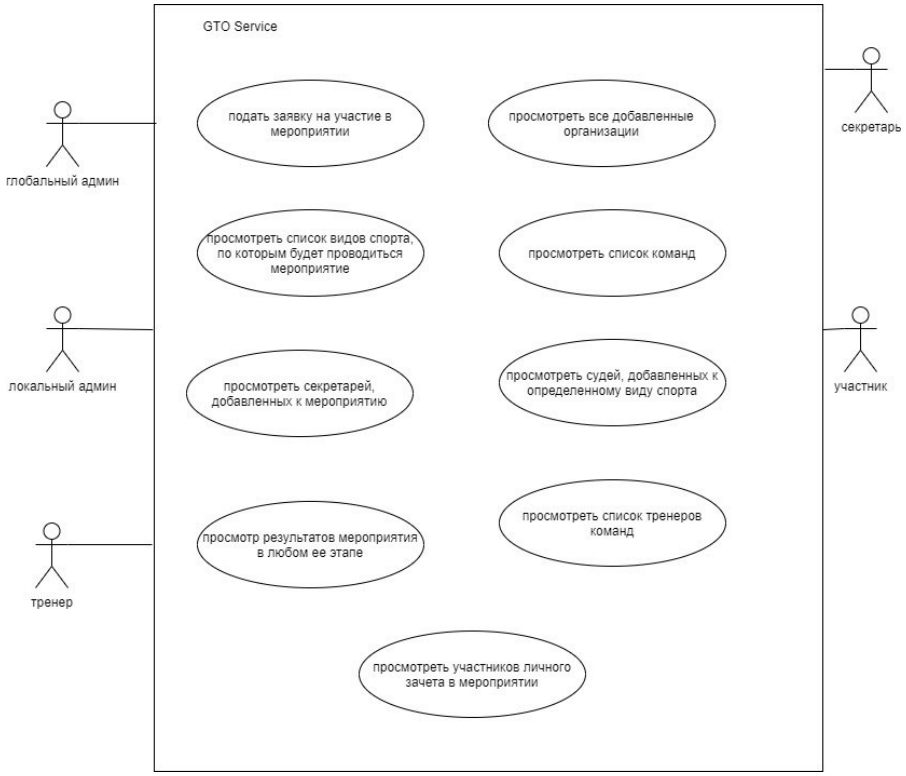


Рис 4. Диаграмма использования мобильного приложения системы проведения и организации фестивалей комплекса ГТО (общие кейсы всех ролей)

Выводы

Использование именно мобильного приложения в проведении и организации фестивалей «ГТО» вполне оправданно. Во-первых, вся система в общем не имеет аналогов на рынке программ и является единственной в цифровом сегменте по предоставляемому функционалу. Во-вторых, регистрация участников на основе распознавания лиц производится исключительно в мобильном приложении. В-третьих, некоторые пользователи системы, не могут физически иметь при себе компьютер или даже ноутбук, а смартфон всегда у всех под рукой.

Список литературы:
1. Роберт Мартин. Чистая архитектура. Искусство разработки программного обеспечения.: Пер. с англ. – СПб.: Питер, 2018. – 352 с
2. Роберт Мартин. Чистый код: создание, анализ и рефакторинг. Библиотека программиста.: Пер. с англ. – СПб.: Питер, 2010. – 464 с
3. Описание всей процедуры проведения соревнований ГТО, а также общие положения [Электронный ресурс]. - Режим доступа: https://www.gto.ru/

УДК004.932.4

Яндыганов Иван Анатольевич
направление Информатика и вычислительная техника (магистратура), гр. ИВТм-13

Научный руководитель
Ипатов Юрий Аркадьевич,
канд. техн. наук, доцент кафедры информатики
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА АЛГОРИТМА ИНТЕЛЛЕКТУАЛЬНОГО СЖАТИЯ ТРАФИКА В ВИДЕОКОНФЕРЕНЦИЯХ

Цель работы – разработка и реализация алгоритма интеллектуального сжатия трафика в видеоконференциях с целью эффективного использования пропускной способности сети за счет уменьшения потока передаваемых данных.

В текущей эпидемиологической ситуации видеоконференции прочно закрепились в нашей жизни – они используются для проведения дистанционных занятий в школах и университетах, при организации удаленной работы на предприятиях, для проведения различных собраний и совещаний без непосредственного контакта в формате offline. Но такой способ организации встреч повышает нагрузку на серверах провайдера, повышает расход Интернет-трафика и, следовательно, растут денежные расходы за пользование Интернетом у обычных пользователей.

Для экономии трафика существуют различные алгоритмы сжатия видеоизображений. Используются (использовались) такие алгоритмы, как: RunLengthEncoding, векторная квантизация, разница кадров, компенсация движения. Одними из популярных являются дискретное косинусное преобразование(DCT) и дискретное wavelet-преобразование (DWT).DCT применяется к блокам изображения 8x8, вычисляются 64

коэффициента, которые затем квантизуются, обеспечивая сжатие. При использовании DWT сигнал проходит через пару фильтров: высоко- и низкочастотный (на выходе будут две последовательности: h[n] и g[n]). Тогда выходные последовательности сигналов будут иметь избыточную информацию и достаточно взять либочетные, либо нечетные выборки.

В данной работе предполагается разработать и реализовать алгоритм интеллектуального сжатия трафика. Во время видеоконференций фон, находящийся за спиной говорящего не несёт полезной информации, а, следовательно, можно отказаться от его передачи. Тогда необходимо на видеоизображении определить силуэт человека, а оставшуюся часть изображения (фон) «вырезать» и не передавать (в качестве фона можно использовать какое-то статичное изображение).

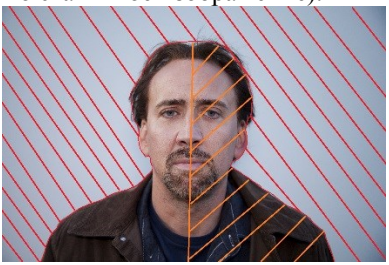


Рис.1. Иллюстрация обработки изображения для сжатия.

Для ещё более сильного сжатия трафика предполагается, что человек (в анфас) почти симметричен, и допускается использовать лишь половину силуэта человека для передачи. Для восстановления изображения можно воспользоваться либо простым отзеркаливанием, либо использовать средства искусственного интеллекта. Однако в любом случае сжатое таким образом видеоизображение будет повержено воздействию аномалий. Но при использовании для необходимых нам целей предполагается, что аномалии не будут вносить существенных искажений в полезную информацию.

Выводы

После реализации алгоритм можно будет применять для видеоконференций, когда имеет место быть ограниченность Интернет-трафика или низкая скорость загрузки/выгрузки данных по сети Интернет. Качество получаемого изображения будет заметно ниже, чем при стандартных видеоконференциях, однако при должной разработке и отладке алгоритма количество аномалий можно свести к минимуму.

Применение этого алгоритма позволить экономить Интернет-трафик, понизить денежные расходы на Интернет, снизить нагрузку на сервера провайдера.

Список литературы:

1. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ-МИФИ, 2002. – 384 с.

2. Сергеенко В. С., Баринов В. В. Сжатие данных, речи, звука и изображений в телекоммуникационных системах. – М.:РадиоСофт, 2009. – 360 с.

СОДЕРЖАНИЕ

Предисловие……3

Абрамов Д.Ю.
Современные системы информационной безопасности 4

Аипов Р.Г.
Создание шифрованного канала передачи данных между подведомственными организациями..... 8

Андреева А.И.
Техническая защита информации от утечек по акустическим каналам 12

Андреев Д.А.
Комплексная система защиты в среде unity 15

Апакаева Я.А.
Комплексная защита информационной безопасности на примере ооо «арб медиа».....18

Ахметзянова Л.Р.
Анализ способов классификации системы обнаружения вторжений в защите информации.....21

Бородин А.В.
О технологии противодействия реверс-инжинирингу в среде туманных вычислений.....23

Васильева Е.С, Сосорева А.И.
Разработка онтологии по физическим эффектам в программе protege ...27*

Ватютов Р.А.
Бортовая радиолокационная система посадки вертолета 31

Гаврилов М.В.
Проектирование системы электронного учета успеваемости студентов 34

Ганин И.С.
Система распознавания речевых команд на основе нейросетевой модели авторегрессии 36

Глебова Е.Н.
Статические методы анализа кода на предмет уязвимости 39

Гоголев И.М.
Siem система финансовой организации для сбора и автоматического анализа событий в корпоративной среде 42

Грачев Д.В., Грачева К.В.
Анализ способов обнаружения дроновпри их вторжении 46

Григорьев Д.Г.
Разработка корпоративного web-сервиса обслуживания служебных записок 50

Данилов Р.А.
Разработка системы обработки изображений на raspberrypi 53

Денисов С.А.
Автоматизированное рабочее место цифровой подстанции.....55

Дмитриева К.Ю.
Технико-экономический анализ вариантов централизованного и индивидуального поквартирного теплоснабжения для города йошкар-ола 58

Жаркова М.В.
Современные тенденции развития технологий разрушающих программных воздействий.....62

Жаркова М.В.
Основная характеристика защиты криптовалюты в современном мире ..66

Иванов Г.В.
Разработка мобильного приложения на основе искусственной нейронной сети 70

Иванов А.В., Иванов Р.А.
Особенности визуализации в codesys 2.3 72

Карташев Р.А., Сидуков Д.А.
Разработка алгоритма объезда препятсвий 76

Кладовикова Е.А.
Модернизация информационной системы налоговых органов российской федерации. 79

Кокшев П.А.
Исследование и разработка нейросетевых алгоритмов обнаружения вторжений для сетевого анализатора данных цифровой подстанции . 83

Кошкин Е.Н., Корнилов А.С.
Разработка двухагентной автоматизированной транспортной системы устранения препятствий на линии 86

Кузовов Н.Д.
Разработка программы для классификации вызванных потенциалов в системе нейрокомпьютерного интерфейса 89

Кулаков В.А.
Визуализация топологии компьютерной сети для мониторинга безопасности 91

Лебедев М.А.
Социальная реклама –инструмент в современных условия инженерной деятельности 94

Лежнина А.С.
Исследование подходов к оценке угроз и рисков информационной безопасности 99

Лоскутова С.С.
Разработка алгоритма чувствительности и программного обеспечения для решения обратных задач прочности летательных аппаратов 107

Мишин С.А.
Pid регулятор в узле рулевого управления 110

Морохина Д.Д.
Разработка системы распознавания шашек камерой opentvh7.....113

Морохина Д.Д., Дегаев М.Н.
Исследование методик описания и классификации уязвимостей информационной безопасности 118

Москвичев М.Е.
Распознавание лиц участников для регистрации и авторизации в информационной системе организации и проведения соревнований комплекса «гто» 125

Мошкин Н.А.
Сравнительный анализ способов оптимизации алгоритмов машинного обучения.....128

Осокина Е.В.
Математическая модель акустического тракта эхолота 132

Павлова Д.Д.
Безопасность электронных платежных систем.....135

Перевозчикова Н.М.
Использование zulu гис в ооо «газпром газораспределение Йошкар-ола»..139

Порфирьев А.И.
Вопросы применения банка данных угроз для определения уровня защищенности 142

Пуртов Д.Н.
Способ создания грамматика лингвистических правил для извлечения ключевой информации 145

Рогачева И.С.
Модернизация архитектуры высокопроизводительных отказоустойчивых вычислительных систем, основанных на концепции троирования с функциональной адаптацией элементов избыточности.....148

Родионова А.К.
Выбор технологии измерений для автономного уровнемера с беспроводной передачей данных по технологии lorawan.....152

Сараева О.А.
Разработка автономного датчика угла наклона с радиоканалом дальнего действия 154

Смирнов Е.А.
Разработка автономного датчика виброскорости на основе mems акселерометра 158

Сосорева А.И., Васильева Е.С.
Физические эффекты, используемые в измерительных преобразователях аппаратуры магнитометрической разведки 162*

Спиридонова Т.Э.
Пакет обновлений для ускоренной работы в сапр "логос".....165

Степанова Е.О.
Влияние цифровой экономики на качество жизни населения 167

Степанов А.Г.
Использование машинного обученияв видеоигровой индустрии 171

Томуров П.Д., Ульянкин Н.А.
Виртуальная обучающая среда для спортивной подготовки человека173

Торбеев Д.А.
К вопросу разработки системы управления роботом манипулятором....177

Угрюмов С.С.
Автоматизациярасчета производительностимногооперационных лесных машин.....179

Фомин Е.В.
Анализ классификации деструктивных программ 183

Ханина Ю.А.
Разработка устройства для нанесения защитно-декоративных покрытий цинкосодержащими электролитами 187

Черняев А.А.
Разработка метода и алгоритма прогнозирования эффективности текстовой рекламы на основе теоремы байеса.....190

Чеснокова Д.Е.
Разработка программного модуля оценки качества изображенийсистемы видеоаналитики 193

Шайкин А.В.
Разработка микросервиса для визуализации формализованных документов.....197

Якушев П.Ю.
Мобильное приложение системы проведения и организации фестивалей комплекса«гто» 202

Яндыганов И.А.
Разработка алгоритма интеллектуального сжатия трафика в видеоконференциях.....208

Научное издание

ИНЖЕНЕРНЫЕ КАДРЫ – БУДУЩЕЕ ИННОВАЦИОННОЙ ЭКОНОМИКИ РОССИИ

Материалы VI Всероссийской
студенческой конференции

Йошкар-Ола, 10-13 ноября 2020 г.

Часть 4

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ОСНОВА СТРАТЕГИЧЕСКОГО ПРОРЫВА В СОВРЕМЕННОЙ ПРОМЫШЛЕННОСТИ

Излагается в авторской редакции
Техническая подготовка материалов: *А.Н. Савинов*

Подписано в печать 15.12.2020. Формат 60×84 $^{1}/_{16}$.
Бумага офсетная. Печать офсетная.
Усл. печ. л. 12.61. Тираж 100 экз. Заказ № 5518.

Поволжский государственный технологический университет
424000 Йошкар-Ола, пл. Ленина, 3

Отпечатано в типографии ООО «Вертола»
424030 Республика Марий Эл, г. Йошкар-Ола, ул. Мира,21