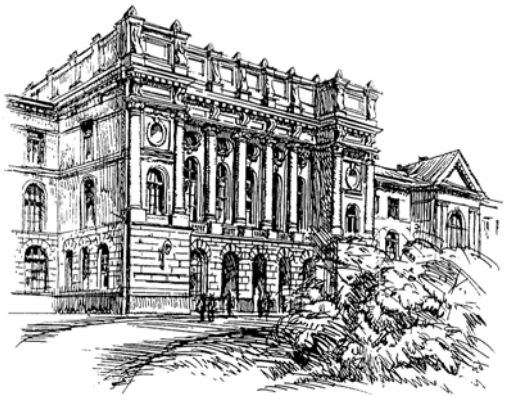
Министерство образования и науки РФ

САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ИЗМЕРИТЕЛЬНЫЕ ТЕХНОЛОГИИ

Сборник научных трудов
Всероссийской научно-практической конференции
с международным участием

16 - 18 июня 2014 года



Санкт-Петербург
Издательство Политехнического университета
2014

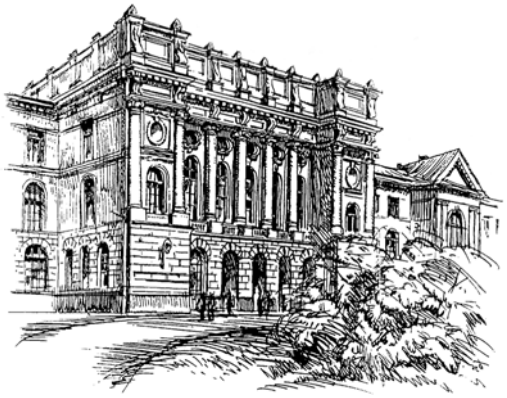
Министерство образования и науки РФ

САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ИЗМЕРИТЕЛЬНЫЕ ТЕХНОЛОГИИ

Сборник научных трудов
Всероссийской научно-практической конференции
с международным участием

16 - 18 июня 2014 года



Санкт-Петербург
Издательство Политехнического университета
2014

Комплексная защита объектов информатизации и измерительные технологии: Сб. науч. тр. Всерос. научн.-практ. конф. с межд. участ. СПб.: Изд-во Политехн. ун-та, 2014.- 149 с.

Вопросы обеспечения безопасности в различных областях жизни общества приобретают все большее значение. Рост числа угроз, тяжесть последствий при их реализации, появление все новых и новых угроз делает задачу решения упомянутых вопросов все более важной. Стремительный рост информатизации общества и, как одно из быстро развивающихся направлений, развитие средств обработки, хранения и передачи информации на объектах информатизации требует решения ряда задач защиты таких объектов, которые базируются, в значительной степени, на информационных и измерительных технологиях.

На конференции представлены три секции.

Секция «Аппаратно-программные средства защиты объектов информатизации» посвящена вопросам повышения эффективности методов и средств защиты объектов информатизации, таких как обнаружение несанкционированных действий, контроль доступа, в том числе вопросам биометрической идентификации, автоматизации различных процессов. А также средствам программной защиты персональных данных, защиты от компьютерных атак и др.

На секции «Математические модели и методы защиты объектов информатизации» рассматриваются доклады по таким актуальным вопросам, как методы и модели теории игр в защите объектов информатизации, использования беспилотных летательных аппаратов для обнаружения угроз, распознавания объектов, теоретического подхода к решению задач создания и оценки систем физической защиты.

Секция «Измерительные технологии» представлена докладами, по вопросам проектирования датчиков физических величин и измерительных систем, что позволяет в конечном итоге обеспечивать безопасность различных объектов и в том числе человека, экологической среды обитания и продуктов питания. Значительная часть докладов секции посвящена изучению физиологии человека и метрологическим аспектам получения достоверной информации.

В конференции участвует широкий круг специалистов из многих университетов и различных организаций Барнаула, Гатчины, Ижевска, Краснодара, Москвы, Новосибирска, Оренбурга, Пензы, Санкт-Петербурга.

Материалы конференции печатаются в авторской редакции.

Ответственный за выпуск – доцент, кандидат технических наук ***А.В. Милицын*.**

СЕКЦИЯ 1
АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Билиженко И.В., Волхонский В.В., Трапш Р.Р.

АНАЛИЗ РАСПРЕДЕЛЕНИЯ УРОВНЯ ИНФРАКРАСНОГО ИЗЛУЧЕНИЯ НАРУШИТЕЛЯ ДЛЯ ЗАДАЧ ОБНАРУЖЕНИЯ КВАЛИФИЦИРОВАННОГО ПРОНИКНОВЕНИЯ

Санкт-Петербург, национальный исследовательский университет информационных технологий, механики и оптики

В соответствии с методикой ГОСТ Р [1] для проверки работоспособности оптико-электронных пассивных инфракрасных извещателей установлено, что извещатель должен обнаруживать движение (выдавать извещение о проникновении) стандартной цели (человека), перемещающеи□ся в пределах зоны обнаружения устройства. При этом в качестве стандартной цели определен конструктивный элемент с размерами 1500x235x300 мм, характеристики излучения которого в ИК диапазоне электромагнитного спектра аналогичны характеристикам излучения человека весом 50-70 кг, ростом 165-180 см, одетого в хлопчатобумажные брюки, куртку или халат и вязаную шапку. Так в работах [2, 3] для оценки вероятности обнаружения использовалась подобная цель (рис. 1).

Более детализированные по температуре (в пяти частях тела) цели определены в стандарте [4]. А в работе [5] приводится один из вариантов подобной стандартной цели (рис. 2.). Наглядно видно, что изображенная цель с большей точностью соответствует человеческому телу.

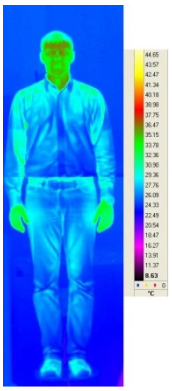


Рис. 1. Реальный нарушитель

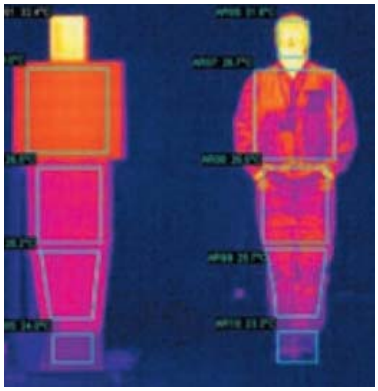


Рис. 2. Стандартная цель

Однако подготовленный нарушитель может использовать методы и средства снижения вероятности своего обнаружения. В частности, использовать теплоизолирующую одежду. Поэтому целесообразно провести исследование теплового портрета нарушителя в различных условиях для проверки степени соответствия стандартных целей модели подготовленного нарушителя. Целесообразность постановки такой задачи объясняется, прежде всего, необходимостью корректной оценки эффективности обнаружения подготовленного нарушителя. Такая задача может решаться на основе результатов, полученных в работе [6] в следующих условиях: температура внутри помещения 23 C^0, модель тепловизора FLIR Titanium 520M (FC7000). В качестве реальной цели использовался человек, одетый в джинсовые штаны и рубашку с длинным рукавом, ростом 180 см и массой тела 75 кг.

На рис. 1 показан исходный тепловой портрет реальной цели. Из рис. 1 видно, что, как и следовало ожидать, наиболее «яркими» с точки зрения интенсивности излучения в рассматриваемом спектральном диапазоне являются открытые участки тела, имеющие температуру в диапазоне 35-36,5^{0}C. Совпадение результатов эксперимента с известными данными, говорит о корректности проведенных исследований. Такая температура обеспечивает достаточно высокий температурный контраст (превышение температуры цели над температурой фона) и, как следствие достаточно надежное обнаружение.

Однако даже обычная одежда, такая, как тонкая куртка, позволяет обеспечить весьма высокий эффект снижения температурного контраста. Это иллюстрируется на рис. 3, на котором показан эффект снижения внешней температуры цели - куртка была надета непосредственно перед экспериментом, т.е. имела температуру близкую к температуре фона. Капюшон, а также возможность надеть перчатки и брюки, могут свести к минимуму температурный контраст по всей поверхности цели.

Однако, очевидно, что будет происходить постепенный прогрев одежды вследствие выделения тепла телом. На рис. 3, а-в приведены результаты, иллюстрирующие этот эффект. Интервал времени от начала измерений составляет 1, 3, 10 минут соответственно. Видно, что уже через 3 минуты имеет место заметный прогрев куртки, температура которой, по крайней мере, в верхней части приближается к исходной температуре. Что естественно приводит к росту температурного контраста, с соответствующим ростом возможности обнаружения.

Очевидно, что использование одежды с более высокими теплоизолирующими свойствами приведет к увеличению интервала времени прогрева.

а) б) в)

Рис. 3. Нарушитель в куртке

Таким образом, становится очевидным, что использование дополнительных теплоизолирующих средств, таких как маска на лицо, перчатки, брюки позволит потенциальному нарушителю сохранять достаточно продолжительное время внешнюю температуру близкую к фоновой. Не говоря уже о возможности использования специализированных средств, например, теплозащитной одежды, используемой пожарными.

Количественную оценку уровня излучения отдельными частями тела во времени иллюстрируют графики на рис. 4. Эти результаты были получены с использованием программы расчета, использующей алгоритм сегментации изображения цели (рис. 1) и расчета уровней излучения от различных частей тела (рис. 5) при фиксированной фоновой температуре.

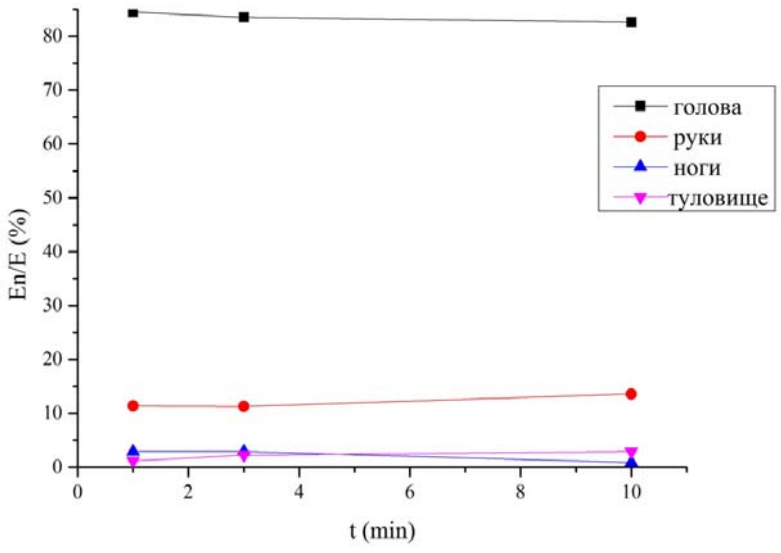


Рис. 4. Относительный уровень излучения от различных частей тела нарушителя

Хорошо видно, что наибольший вклад при исходных условиях (фоновая температура 23^0 C) создает излучение от головы, что подтверждает корректность постановки решаемой задачи.

Представляет интерес возможность оценить характер влияния фоновой температуры на уровень сигнала, формируемого извещателем, от излучения различными частями тела. Соответствующие кривые, позволяющие сделать такую оценку, приведены на рис. 6.

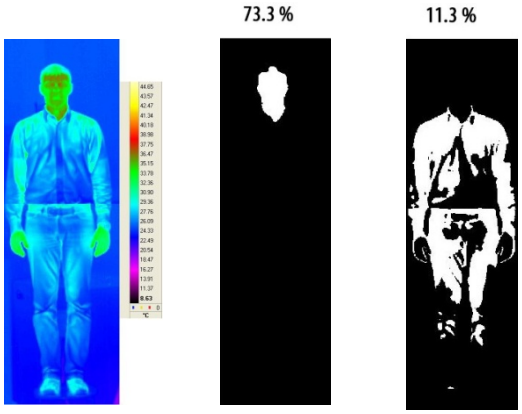


Рис. 5. Сегментированные изображения реальной цели

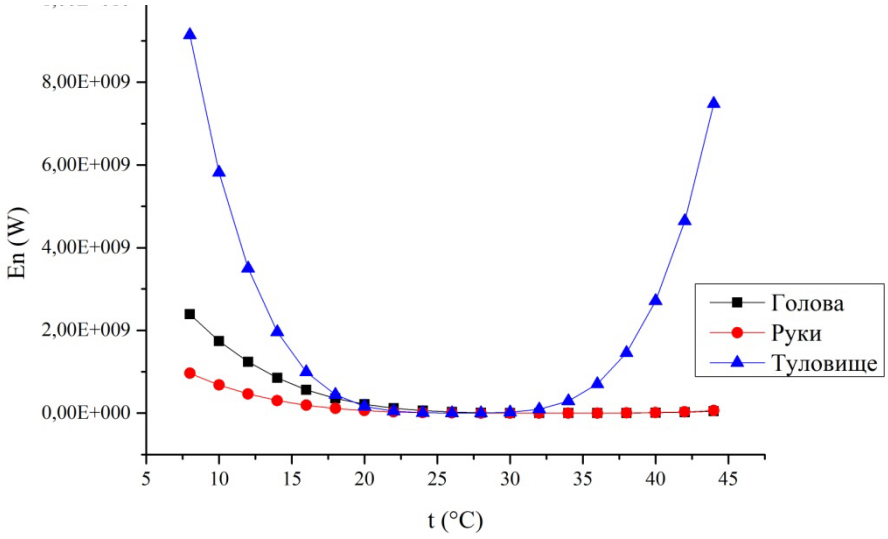


Рис. 6. Характер изменения уровня излучения от фоновой температуры

Т.о. на основании проведенных исследований можно сделать следующие выводы.

Распределение температур по поверхности реального нарушителя существенно отличается от стандартных целей, определяемых в [1, 4].

При использовании теплоизолирующих материалов происходит значительное перераспределение ИК излучения в пределах поверхности

нарушителя. Основными составляющими становятся излучение от лица и рук.

Соотношение уровня излучения от различных частей тела цели существенно меняется при изменении фоновой температуры.

Таким образом, на основании полученных результатов можно говорить о целесообразности введения специальных стандартных целей типа «подготовленный нарушитель» для использования применительно к задачам анализа объектов с повышенными требованиями по обеспечению безопасности, а также при разработке оптико-электронных пассивных инфракрасных извещателей.

Литература

1. ГОСТ Р 50777–95. Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 6. Пассивные оптико-электронные инфракрасные извещатели для закрытых помещений и открытых площадок. – Введ. 27.12.2006. – М.: Госстандарт Российской Федерации. – 25 с.
2. Волхонский В.В., Воробьев П.А., Методика оценки вероятности обнаружения несанкционированного проникновения оптикоэлектронным извещателем // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 1(77). – С. 120-123.
3. Волхонский В.В., Воробьев П.А., Трапш Р.Р. Критерии оценки эффективности функционирования оптикоэлектронных датчиков систем физической защиты // Вестник компьютерных и информационных технологий. – 2014. – № 3. – С.24-29.
4. E N 50131-2-2 Alarm systems – Intrusion systems – Part 2-2: Requirements for passive infrared detectors. Approved 2004-05-04. CENELEC. – 38 p.
5. Полещук Р. Европейские стандарты EN50131 для систем охранной сигнализации // Алгоритм безопасности. – СПб.: – 2010. – №4. – С. 28-31.
6. Воробьев П.А., Трапш Р.Р. Тепловой портрет нарушителя систем физической защиты // Сборник тезисов докладов конгресса молодых ученых, СПб: НИУ ИТМО, Выпуск 2. – 2013.– С. 133-134.

Биричевский А.Р.

ОТРИЦАЕМОЕ ШИФРОВАНИЕ КАК МЕХАНИЗМ ЗАЩИТЫ ПРИЛОЖЕНИЙ ОТ ОТЛАДКИ

Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

Противодействие несанкционированной отладке является важнейшей задачей защиты программного обеспечения. В работе рассмотрена возможность применения отрицаемого шифрования для защиты программных продуктов от отладки.

Отладка приложения представляет собой процесс анализа программного продукта специализированными средствами с целью устранения ошибок. Как и многие другие полезные средства отладка может применяться злоумышленниками для взлома и кражи коммерческих программных продуктов.

Возможность отладки приложений создает производителям коммерческого программного обеспечения ряд значительных проблем, связанных с необходимостью применять специализированные средства защиты приложений.

Под понятием отрицаемого шифрования понимают способ криптографического преобразования, в котором зашифровываются совместно два или более различных сообщений на двух или более различных ключах [1].

В данной работе предлагается использовать для защиты от отладки программных продуктов отрицаемое шифрование.

Средства предназначенные для отладки приложений можно разделить три группы:

дизассемблеры - средства анализа статического кода приложения (без запуска приложения), преобразуют низкоуровневый машинный код программы в понятный для понимания вид (библиотечные функции, блок-схемы);

отладчики - средства активного анализа работы приложения, позволяет злоумышленнику исследовать алгоритм работы приложения, внешнее окружение (занимаемую память, регистры, работу служб операционной системы), позволяет выполнять так называемую "пошаговую" отладку;

эмуляторы - средства имитирующие окружение программы (память, операционную систему и т.д.).

Классические типы средств отладки приложений могут использоваться и совместно. Методы защиты приложений от отладки делят по направлениям анализа против которых они предназначаются.

Против статического анализа (дизассемблирования) могут использоваться различные типы сокрытия машинного кода приложения:

шифрование тела приложения (ключевых блоков) - при запуске приложение расшифровывается и производится запуск основной программы;

запутывание кода (упаковывание) - перемешивание кода, создание большого количества дополнительных ссылок;

алгоритмическая защита - внедрение в код программы (на этапе ее разработки) специализированной логики нацеленной на защиту приложения от анализа; примером может быть маскировка передачи управления (использование косвенной передачи управления).

Для защиты от анализа активного приложения также имеются классически применяемые средства.

Контроль времени. Суть метода заключается в измерении времени выполнения ключевых блоков кода. Так как при отладке (анализе) приложения выполнение команд происходит по команде человека ("пошаговый" режим отладки), время выполнения таких команд значительно больше. Время выполнения команд может быть измерено как запросом системного времени, так и по количеству тактов выполненных процессором.

Контроль контрольных сумм. В данном случае программа подсчитывает контрольные суммы ключевых блоков (например, при старте приложения). Так как при анализе приложения отладчики не редко устанавливают так называемые контрольные точки (точки останова) в коде приложения, контрольные суммы ключевых блоков приложения будут изменены.

Алгоритмическая защита. В случае защиты от активного анализа приложения также имеются много различных специальных приемов программирования.

Контроль внешней среды представляет собой контроль за состоянием множества внешних (относительно приложения) параметров:

количество свободной оперативной памяти;

наличие в оперативной памяти определенных данных;

состояние операционной системы (состояние служб, наличие библиотек).

При работе, приложение проверяет контролируемые параметры и в случае появления аномалий активизирует защитные механизмы приложения.

Методы защиты приложения от статической отладки могут быть дополнительно усилены посредством применения отрицаемого шифрования.

Наиболее часто используемой в приложении структурой является "условие". "Условие" используется как самостоятельно, так и в более сложных структурах, таких как "цикл".

Для защиты от статического анализа (дизассемблирования) целесообразно в ключевых блоках программы вместо структуры "условие" использовать отрицаемое шифрование. Вместо ключа использовать входные данные "условия". На выходе необходимо реализовать ложные ветви кода (например, в зашифрованном сообщении может содержаться адрес следующей блока программы). Такая структура (далее блок шифрования) будет применена и в других методах защиты от отладки, которые будут описаны далее. На вход блока шифрования будет подаваться параметр (ключ). На выходе блока будет получен адрес следующей команды (открытый текст).

Применение отрицаемого шифрования в качестве конструкции типа условие позволит значительно усложнить (особенно при многократном применении) статический анализ приложения (дизассемблирование).

При защите от статического анализа также применяется и шифрование тела или наиболее критичных блоков программы. Для шифрования тела программы или критических блоков приложения возможно применение отрицаемого шифрования. В данном случае в качестве ключа может быть использовать целый ряд внешних параметров (контроль внешней среды) таких как состояние операционной системы. На выходе также как и в предыдущем случае необходимо реализовать ложные ветви кода.

Для защиты программы от активного анализа средствами отладки, также может применяться отрицаемое шифрование.

Метод защиты от активной отладки "контроль времени" дополнительно усложняется введением в алгоритм метода отрицаемого шифрование.

Первая стратегия применения отрицаемого шифрования для контроля времени - контроль времени выполнения.

На входе блока шифрования: разница во времени (например, может быть передано количество тактов процессора, которое прошло за период времени).

На выходе блока шифрования: адрес следующего блока основной программы (либо ложной ветви алгоритма).

Вторая стратегия применения отрицаемого шифрования для контроля времени - контроль момента времени выполнения.

На входе блока шифрования: настоящее время.

На выходе блока шифрования: адрес следующего блока основной программы (либо ложной ветви алгоритма).

Такая стратегия может также быть применена также в пробных версиях программных продуктов (например для работы программы в течении конкретного месяца).

Стратегий применения отрицаемого шифрования для контроля внешней среды можно разработать достаточно много (стратегия зависит от входных данных - количества оперативной памяти, наличие библиотек и т.д.). Перспективной выглядит следующая стратегия, которая предназначена для контроля адреса flash-памяти микроконтроллера, откуда запущен экземпляр приложения.

На входе блока шифрования: адрес первой команды тестируемого блока (в микроконтроллерах архитектуры ARM - значение счетчика команд).

На выходе блока шифрования: адрес следующего блока основной программы (либо ложной ветви алгоритма).

Используя данный метод, экземпляр программы может определить, что он запущен вне защищенного блока памяти, и активизировать защитные действия.

При внедрении системы защиты от отладки следует принимать что:

программный продукт в любой своей части может быть подвержен анализу;

внешняя среда (оперативная память, внешние библиотеки, средства операционной системы) постоянно находится под наблюдением;

злоумышленник может иметь большие возможности и обладать всеми необходимыми знаниями для анализа приложения.

В каждый момент времени на входе блока шифрования может быть намеренно направлено (злоумышленником в ходе анализа приложения) определенное значение. Использование для таких целей программ отладчиков может рассматриваться как "принуждение" программы к выполнению неких действий. В таком случае применение отрицаемого шифрования поможет более эффективно применять классические методы защиты приложения от отладки.

Список литературы

1. Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В. Способ отрицаемого шифрования // Вопросы защиты информации. 2013. № 2. С. 18-21.

2. Морозова Е.В., Мондикова Я.А., Молдовян Н. А. Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы. № 6. 2013. С. 73-78.

Богданов А.В.

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ЕДИНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ КРУПНЫХ МУЗЕЙНЫХ И ВЫСТАВОЧНЫХ КОМПЛЕКСОВ

Санкт-Петербург, СПбГУ ГПС МЧС России

Процессы управления сложными организационно-техническими системами, к которым по праву можно отнести крупные музейные и выставочные комплексы (КМиВК), характеризуются повсеместным использованием новых высокотехнологичных средств, повышенной потребностью лица принимающего решение (ЛПР) всех уровней и звеньев управления в актуальной, достоверной и оперативной информации [1].

Современный этап информатизации объектов культуры базируется на передовых информационных технологиях и телекоммуникационных сетях, соединяющих в единое целое совокупность разнородных вычислительных средств. Системообразующей основой интеграции процессов управления и средств их автоматизации на разных иерархических уровнях должно стать единое информационное пространство (ЕИП).

Внедрение сложных информационно-управляющих систем в деятельность КМиВК не должно проходить без комплексного решения проблемы обеспечения безопасности вообще, и защиты информации, в частности. В этой связи, задача обеспечения безопасности ЕИП КМиВК является наиболее приоритетной.

Эффективность ЕИП во многом определяется качеством и безопасностью реализуемых информационных технологий. В 2010 году на рынке информационных услуг появилось новое понятие – «облако», олицетворяющая сложную инфраструктуру, скрывающую за собой все детали технической реализации сервиса [2].

Сама по себе технология является отражением всеобщей тенденции глобализации информационных систем, развитие которых сопровождается расширением перечня угроз, появлением дополнительных уязвимостей информационным ресурсов и, как следствие, совершенствованием способов реализации информационных атак.

Можно выделить следующие виды уязвимостей облака [3]:

- неправомерное и нечестное использование облачных технологии;
- небезопасные программные интерфейсы (API);
- внутренние нарушители;
- уязвимости в облачных технологиях;
- потеря или утечка данных;
- кража персональных данных и неправомерный доступ к сервису;
- прочие уязвимости.

В качестве стандартной модели безопасности принято использовать модель, состоящую из трёх обязательных категорий: конфиденциальность, целостность, доступность.

Данная модель предусматривает, что облачная технология это, с одной стороны, - единая система с едиными правилами обработки информации, а с другой – совокупность обособленных систем, каждая из которых имеет свои собственные средства обработки информации. Поэтому, с учетом двойственности характера системы и ее распределённой архитектуры, атака на нее может осуществляться с двух уровней: верхнего и нижнего (возможна и их комбинация). При атаке верхнего уровня используются свойства системы для захвата управления узлом сети и выполнения несанкционированных действий. При атаке нижнего уровня используются свойства протоколов передачи данных для перехвата пакетов и нарушения конфиденциальности или целостности, как отдельных сообщений, так и потока в целом.

Это требует принятия адекватных мер и применения соответствующих средств защиты, которые должны предотвращать как минимум [4]: ложную инициализацию обмена, несанкционированный доступ, необоснованный отказ в доступе, раскрытие содержания передаваемых данных, внесение изменений в передаваемые данные, возможность измерения и анализа характеристик информационной системы, которые повлекут раскрытие сведений.

ЛИТЕРАТУРА:

1. Богданов А.В., Синещук Ю.И., Синещук М.Ю., Примакин А.И., Яковлева Н.А. Основные угрозы и направления обеспечения безопасности единого информационного пространства. «Вестник Санкт-Петербургского университета МВД». – № 2. – 2013. с. 150-154

2. Carl Hewitt, "ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing," IEEE Internet Computing, vol. 12, no. 5, pp. 96-99, Sept.-Oct. 2008

3. Cloud Computing: 7 проблем безопасности [Электронный ресурс]. Сайт Бюро Соломатина. –: http://www.bureausolomatina.ru/

4. Синещук Ю.И., Скряга Ю.А, Потехин В.С. Информационные угрозы и уязвимости технологии облачных вычислений . Информационная безопасность регионов России (ИБРР-2013). VIII межрегиональная конференция, СПБ. 23-25.10.2013. (Материалы конференции стр.63-64.)

Богданов А.В.

МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ КРУПНЫХ МУЗЕЙНЫХ И ВЫСТАВОЧНЫХ КОМПЛЕКСОВ

Санкт-Петербург, СПбГУ ГПС МЧС России

Расширение на современном этапе круга задач крупных музейных и выставочных комплексов (КМиВК), увеличение требований к качеству их решения обусловили переход к новым технологиям управления. При этом состояние проблемы безопасности КМиВК, определяется множеством факторов. Одним из существенных факторов, доминирующих в последнее время, является изменение характера угроз, вызванное повсеместной информатизацией деятельности КМиВК.

Этот аспект музейного комплекса актуализирует проблему разработки (выбора) интегрированной системы безопасности (ИСБ) [1].

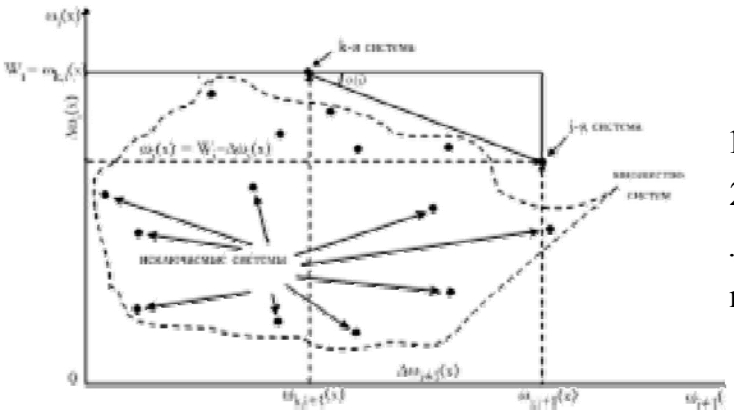
В общем случае, способов организации ИСБ достаточно много: они определяются техническими и функциональными возможностями аппаратно-программных средств, экономическими соображениями. Поскольку такого рода системы характеризуются множеством, зачастую противоречивых показателей, то для обоснования и выбора оптимального по совокупности параметров варианта построения системы целесообразно использовать методы многокритериальной оценки эффективности [2]. К числу таких методов относится метод последовательных уступок (МПУ).

Метод предназначен для сравнительной оценки эффективности исследуемых систем по их показателям эффективности, заданных в количественной форме, а также в соответствии с расстановкой данных показателей по важности и их ограничениям (уступкам).

Прежде всего производится качественный анализ относительной важности показателей эффективности. Показатели располагаются и нумеруются в порядке убывания важности так, что главным является показатель ω_1, менее важным ω_2, затем остальные показатели: $\omega_3, \omega_4, ..., \omega_n$.

Максимизируется первый по важности показатель ω_1 и определяется его наибольшее значение W_1. Затем определяется (назначается) величина допустимого снижения (уступки) показателя ω_1 ($\Delta\omega_1 \geq 0$) и наибольшее значение второго показателя $\omega_2 \rightarrow W_2$ при условии, что значение первого показателя должно быть не меньше, чем $W_1 - \Delta\omega_1$. Снова определяется (назначается) величина уступки, но уже по второму показателю – $\Delta\omega_2 \geq 0$, которая используется при нахождении условного максимума W_3 третьего показателя ω_3 и т.д. Наконец, максимизируется последний по важности показатель ω_n при условии, что (n-1) предыдущих должны быть не менее соответствующих величин $W_i - \Delta\omega_i$. (Рисунок 1)

Полученная в результате совокупность показателей эффективности соответствует оптимальной системе или варианту ее построения.



1) $W_1 = \sup\omega_1(x)$;

2) $W_2 = \sup\omega_2(x), \text{при} \omega_1(x) \geq W_1 - \Delta\omega_1$;

. . . . . .

n) $W_n = \sup\omega_n(x), \text{при} \omega_{n-1}(x) \geq W_{n-1} - \Delta\omega_{n-1}$

(*где sup – верхняя граница;* $x \in X$ *; – множество значений технических характеристик)*

Рис. 1. Графическая и математическая интерпретация МПУ

В результате (n-1) шагов определяется совокупность ТТХ технических средств, обеспечивающих рациональные значения показателей эффективности функционирования системы.

Проблема защиты информации представляет особую важность для современных КМиВК, которые отличаются высоким уровнем компьютеризации процессов управления на всех уровнях иерархии.

Концентрация больших объемов обобщенной и систематизированной информации КМиВК в автоматизированных системах ее обработки приводит к увеличению вероятности утечки конфиденциальных сведений, а значит и к необходимости принятия мер по обоснованию эффективной системы безопасности.

ЛИТЕРАТУРА

1. Краснов А.В., Богданов А.В. Информационная система обеспечения безопасности крупных музейных комплексов. М.: Пожаровзрывобезопасность, №1, 2007.
2. Синещук Ю.И. и др. Автоматизация управления силами флота. СПб. ВМИРЭ, 2008.

Волхонский В.В.

ОСОБЕННОСТИ И ПРОБЛЕМЫ ЭТАПОВ ПОСТРОЕНИЯ И ПРИМЕНЕНИЯ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ

Санкт-Петербург, национальный исследовательский университет информационных технологий, механики и оптики

Различные этапы создания и применения систем физической защиты (СФЗ), могут в значительной мере влиять на результативную эффективность СФЗ. При этом различные проблемы могут возникать на разных этапах создания систем – анализа объекта, оценки угроз и способов их реализации, оценки возможного ущерба, отбора существенных угроз, подготовки ТЗ, проектирования, выбора оборудования, монтажа, пусконаладки, приемки и эксплуатации. Остановимся на некоторых проблемах, возникающих на этих этапах.

На всех этапах могут возникать *проблемы терминологии*. Несоответствие используемых терминов может приводить к разночтению в понимании одних и тех же понятий заказчиком и разработчиком, а также другими участниками. Так термины «физическая защита» или «системы физической защиты» используются в настоящее время в четырех смысловых значениях: защита от физических лиц; защита физическими лицами; использование физических препятствий для нарушителя; обеспечение физической целостности объектов. Последнее смысловое значение - обеспечение физической целостности объекта, представляется наиболее правильным и общим. Поэтому, можно говорить, что система физической защиты –

это совокупность методов и средств обеспечение физической целостности объекта обеспечения безопасности.

Зачастую понятие «обеспечение безопасности» подменяют только обнаружением угроз, забывая об основных функциях СФЗ, которая должна обеспечивать предотвращение, обнаружение и ликвидацию угроз до нанесения существенного ущерба, а также контроль текущей ситуации, снижение потерь при внештатной ситуации и постфактум анализ произошедшего. Тем не менее, регулярно звучат такие фразы, как «установлена система видеонаблюдения, город стал безопасным» и т.п. Но разве система телевизионного наблюдения может ликвидировать угрозу? А без своевременной (до нанесения существенных потерь) ликвидации угрозы обеспечение безопасности невозможно.

Известна важность четкой *постановки задачи* для ее корректного решения. Однако, во многих случаях, СФЗ создаются с формально написанным техническим заданием (ТЗ), а то и без такового. В совокупности, с отсутствием в ТЗ эффективных методик и критериев оценки СФЗ, это приводит в нештатных ситуациях к неполном выполнению системой поставленных задач, либо даже к их не выполнению.

Часто в ТЗ оговариваются параметры только элементов СФЗ, например, разрешающая способность телекамер. При этом может иметь место подмена понятий, например, вместо разрешающей способности продавцы, а иногда производители указывают количество пикселей или приводят другие некорректные технические характеристики. К примеру, для телекамеры указывается минимальная освещенность без указания условий измерения.

Приходится регулярно сталкиваться с ошибками реализации СФЗ, приводящими к заметному ухудшению реальных параметров систем. Т.е. с ошибками проектировщиков и установщиков систем. Например, с неправильным выбором места установки и ориентации телекамер. И, как следствие, снижением информативности формируемых видеоизображений.

Можно выделить две неразрывные составляющие СФЗ - *средства* обеспечения безопасности *и методы* их использования. Но на практике часто имеет место разрыв между функциональными возможностями технических средств СФЗ и методами их использования. Можно создать хорошую систему ФЗ, но отсутствие корректно разработанных методов её использования зачастую сводит на нет заложенные в неё и реализованные возможности системы физической защиты.

На всех этапах следует вести учет угроз самой СФЗ, а также угроз, создаваемых системой физической защиты. В противном случае, как

показывает практика, СФЗ может наносить существенный ущерб объекту защиты, либо не выполнять своих функций.

Необходима разработка эффективных *критериев оценки* систем физической защиты и методик их применения как для систем в целом, так и для отдельных подсистем и их элементов. И не просто критериев оценки, такие, к примеру, есть и используются производителями, а первую очередь, критериев ориентированных на *конечного пользователя* системы. А для этого оценка СФЗ должна даваться по конечному результату, на выходе СФЗ, как некоего «черного ящика». Поскольку пользователя интересует конечный результат, а в этом его интересы и интересы разработчиков, производителей и поставщиков могут расходиться.

Гусев В.С.

БЕЗОПАСНОСТЬ БАНКОВСКОЙ СИСТЕМЫ – СУЩЕСТВЕННАЯ ЧАСТЬ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

На рубеже XX и XX1 веков в России сложилась очень непростая политическая, экономическая, социальная и экологическая ситуация, обусловленная сменой форм собственности и переходом к новой общественной формации. Изменение экономики под воздействием рыночных механизмов выделило обеспечение экономической безопасности страны в самостоятельную функцию государства – с позиций как интересов личности, так и сложной совокупности национальных интересов.

Проблемы обеспечения экономической безопасности не менее сложны, чем процессы, происходящие в обществе. Они связаны с реформами в политической, экономической, социальной и духовной областях. Чтобы сформировать правовое государство, перестроить политическую систему общества, установить демократию, необходимо было переосмыслить концепцию и национальной и экономической (как определенной формы ее выражения) безопасности. Не случайно уже в 1996 году Президентом России в стратегии экономической безопасности Российской Федерации (основные положения) впервые были определены

наиболее вероятные угрозы в этой сфере. Было выделено четыре блока угроз:

- увеличение имущественной дифференциации населения и повышение уровня бедности;
- деформированность российской экономики;
- возрастание неравномерности социально-экономического развития регионов;
- криминализация общества и хозяйственной деятельности.[1]

Нужно подчеркнуть, что признание угроз экономической безопасности в таком виде в 1996 году на президентском уровне, уже было поступком, на фоне всеобщей эйфории постперестроечных и демократических преобразований в стране. Дальнейшее развитие эта тема получила и в последующих концептуальных документах, таких как «Концепция национальной безопасности Российской Федерации» от 17 декабря 1997 г и особенно в редакции Указа Президента РФ от 10 января 2000 г № 24., и, наконец, в ныне действующей «Стратегии национальной безопасности Российской Федерации до 2020 года». [2]

О глубине разработки проблемы за последние 15 лет свидетельствуют сами определения основных угроз экономической безопасности России приведенные в Стратегии, их формулировка, не сглаживающая всей остроты и сложности возникающих, в том числе и в перспективе, задач: « Главными стратегическими рисками и угрозами национальной безопасности в экономической сфере на долгосрочную перспективу являются сохранение экспортно-сырьевой модели развития национальной экономики, снижение конкурентоспособности и высокая зависимость ее важнейших сфер от внешнеэкономической конъюнктуры, потеря контроля над национальными ресурсами, ухудшение состояния сырьевой базы промышленности и энергетики, неравномерное развитие регионов и прогрессирующая трудонедостаточность, низкая устойчивость и защищенность финансовой системы, сохранение условий для коррупции и криминализации хозяйственно-финансовых отношений, а также незаконной миграции.» [3]

Стратегия вводит понятия энергетической и продовольственной безопасности, подчеркивает недостаточную эффективность государственного регулирования экономики, наличие дефицита топливно-энергетических, водных и биологических ресурсов. Особо отмечено существование дискриминационных мер и усиление недобросовестной конкуренции в отношении России, влияние кризисных явлений в мировой финансово-банковской системе.

Приводя направления борьбы с современными вызовами в экономической сфере, Стратегия, декларируя необходимость комплексного решения возникающих проблем в экономике,

одновременно дает пути разрешения, локализации отмеченных угроз: «обеспечение национальной безопасности за счет экономического роста достигается путем развития национальной инновационной системы, повышения производительности труда, освоения новых ресурсных источников, модернизации приоритетных секторов национальной экономики, совершенствования банковской системы, финансового сектора услуг и межбюджетных отношений в Российской Федерации». [3]

Для противодействия угрозам экономической безопасности силы обеспечения национальной безопасности во взаимодействии с институтами гражданского общества должны быть нацелены, говорится в Стратегии, в том числе на укрепление финансовых рынков и повышение ликвидности банковской системы.

Образно говоря, если представить экономику как некий человеческий организм, то финансовую систему можно интерпретировать как кровеносную систему, а финансы – это кровь, движущая сердце и все остальные органы. Понятно, что любой сбой в этой системе, чреват серьезными нарушениями здоровья всего организма. Не случайно, поэтому, в стратегическом документе уделяется столь большое внимание финансово-банковской составляющей жизни нашего государства.

Банки эволюционировали вместе со всей страной: от технологических исполнителей воли государства в рамках командно-административной системы времен развитого социализма, до серьезных участников, движителей рыночной экономики, без которых становится невозможно развитие целых отраслей, в том числе инновационных.

Роль банков в современных рыночных условиях хозяйствования определяется тем, что доминирующим ресурсом в рыночной экономике являются деньги. Этот ресурс в безналичной форме «производится» банками в соответствии с требованиями объективных экономических законов. Особенность ресурса «деньги» заключается в том, что он легко превращается в другие ресурсы при условии правильной организации эмиссии и обращения денег в наличной и безналичной формах в соответствии с потребностями экономики.

Именно банки организуют финансовые потоки, обеспечивая концентрацию распыленных между многими собственниками сумм денег и их направление не только на текущее производство, но и на его модернизацию с целью выпуска новых видов продукции и оказания различных услуг Правительству и населению. Банки, таким образом, служат фундаментом и важнейшей частью финансовой инфраструктуры рыночной экономики и призваны обеспечивать условия нормальной жизнедеятельности государства и граждан страны. [4]

Вот почему обеспечение безопасности банковского сектора экономики имеет принципиальное важнейшее значение в общей системе комплексной экономической безопасности нашего государства.

В современных условиях обеспечение банковской безопасности происходит на нескольких уровнях:

Первый уровень - государственный

Второй уровень – региональный

Третий уровень – собственно банки.

Задачей первого и второго уровня является создание надлежащих условий, прежде всего правовых (юридических) для функционирования банков. Разработка и принятие нормативных документов (законов, указов Президента, документов Правительства и Центробанка) регламентирующих деятельность субъектов финансовой сферы, в том числе их ответственность за возможные отклонения от нормативных требований. Ярким примером такого регулирования (по материалам СМИ) могут служить предложения Президента России Владимира Путина, который поручил правительству и Центробанку до 1 июня 2014 г. внести в законодательство изменения, касающиеся введения уголовной ответственности должностных лиц банков за фальсификацию отчетности.. Отмечается, что менеджмент банков будет нести уголовную ответственность независимо от наличия ущерба, причиненного в результате такой фальсификации.

Банк России и кабинет министров должны внести законодательные изменения по определению механизмов противодействия распространению заведомо ложных сведений о финансовом состоянии кредитных и иных публичных финансовых организаций из анонимных источников.

Кроме того, Путин В.В. поручил к 1 июня 2014г. внести поправки по дифференциации ставок взносов банков в фонд страхования вкладов. ЦБ совместно с правительством также должны до начала лета 2014 г. проработать вопросы об усовершенствовании процедур финансового оздоровления и ликвидации кредитных организаций.

Уместно напомнить, что еще в декабре прошлого года В.В. Путин, выступая с посланием к Федеральному собранию, заявлял о необходимости введения уголовного наказания для руководителей финансовых организаций, предоставляющих недостоверные сведения о возглавляемых ими структурах соответствующим органам. "Нужно предложить принципиальную и твердую линию по избавлению нашей кредитно-финансовой системы от разного рода "отмывочных" контор, или, как еще говорят, "прачечных". При этом интересы добросовестных клиентов и вкладчиков проблемных банков должны быть надежно защищены", - подчеркивал глава государства.

Актуальность подобных высказываний Президента очень хорошо иллюстрируется последними событиями на финансовом рынке связанными с лишением лицензии на право проведения банковской деятельности целой группы финансовых учреждений России – все они были связаны с грубейшими нарушениями действующих норм и законов, а зачастую и с прямыми преступлениями со стороны акционеров-собственников банков и их персонала.

Так, например, отрицательный капитал «Инвестбанка» (Москва), лишившегося лицензии 13 декабря 2013 года оценивается ЦБ в рекордную сумму 45 млрд.руб. Как он образовался? ЦБ поясняет : «Ссуды отдельных заемщиков неоднократно реструктуризовались с изменением существенных условий первоначальных договоров в сторону, более благоприятную для заемщиков: продлевались сроки погашения основного долга и уплаты процентов, в чем усматривается отсутствие у заемщика средств для погашения своих обязательств перед банком. В результате кредитный портфель, который формировался с 2009 года в размере 31,5 млрд. руб. полностью обесценился.» Вложения в сомнительные ценные бумаги в объеме 8,2 млрд.руб. Предварительная проверка банка ЦБ показала, что стоимость активов не превышала 32,5 млрд.руб. при величине обязательств перед кредиторами 62,6 млрд.руб.

В лишенном лицензии «Банке проектного финансирования» (БПФ – Новосибирск) вообще не оказалось сведений о некоторых вкладчиках. Люди обращаются в Агентство по страхованию вкладов, но, имея на руках документы подтверждающие наличие вклада, не могут получить страховку, так как в документах бухгалтерского учета банка они не значатся.

Чем как безнаказанностью можно объяснить, что ряд руководителей банков проводили, мягко говоря, рискованную политику в своем бизнесе. Так, бывший руководитель и его подельники из банка «Кредиттраст» , используя реквизиты более 70 фиктивных компаний, изготовили десятки подложных договоров купли продажи векселей, соглашений о выпуске векселей и соглашений о цессии, а также договоров об отчуждении прав требования возврата кредита, в результате чего из оборота банка было необоснованно выведено денежных средств в размере около 1,2 млрд. рублей, что привело к банкротству.

Руководство «Моего банка» вывело перед продажей банка 90% активов, образовав «дыру» в балансе в 10 млрд. руб.

Осенью 2012 года в ходе подготовки к IPO инвесторы оценили глобальные депозитарные расписки «Промсвязьбанка» в 10-12 $, а весь банк в 1.5-1.8 млрд.$. Согласись банк на такое предложение он торговался бы ниже капитала (с коэффициентом 0,7-0,9 к капиталу).

Объем собственных средств на тот момент составлял 58 млрд. руб. К счастью из-за такой низкой оценки инвесторами публичное размещение акционерами было отложено.

Из приведенных примеров совершенно очевидно, что рискованное ведение бизнеса, осуществлялось банками вполне осознанно и, в не малой степени, поощрялось практикой, когда лица, ответственные за принятие сомнительных решений не боялись тех катастрофических последствий, которые наступали, ибо страдали, как правило, ни в чем не повинные клиенты и вкладчики, а истинные виновные успевали уйти от ответственности, да еще при этом сохранив значительные суммы, предусмотрительно выведенные за границу.

Рассматривая имеющуюся практику обеспечения безопасности на третьем уровне – собственно в банковской сфере, необходимо сразу же подчеркнуть некоторые ее особенности, отнюдь не способствующие оздоровлению этой области хозяйствования в смысле защиты ее от криминала и коррупции.

Первое – банки весьма консервативны в смысле раскрытия внутренних проблем, оказывающих влияние на их деятельность. Стремление «не выносить сор из избы», за которым стоит опасение подпортить имидж банковской деятельности, превалирует, как правило, над здравым смыслом. Причем это касается как мелких правонарушений внутри банка: например хищения материальных ценностей, межличностных конфликтов, так и тех случаев, когда речь идет о серьезных «проколах» в кредитовании, крупных невозвратах, искажении финансовой отчетности и пр. Внутренняя кухня, внутрикорпоративная солидарность – это табу, как для СМИ, так и для любых посторонних лиц (даже если это налоговая инспекция или полиция).

Второе – большинство преступлений, совершаемых в банковской сфере или в ее ближайшем окружении, как правило, не обходятся без участия самих банковских служащих. Идет ли речь о кражах денег или ценностей, хранящихся в банковских ячейках, или о махинациях с ценными бумагами, или «липовании» при оформлении кредитов – почти всегда преступники используют в качестве источников информации сотрудников банков. При этом переход от просто информаторов к соучастникам в преступлении происходит почти всегда и очень быстро.

Третье – практически все банки, хотя, естественно никто в этом не признается, «избалованы» властью денег, так как большинство возникающих у них проблем они решают с помощью элементарных взяток. При этом размеры подкупа чиновников или правоохранителей иногда достигают фантастических сумм.

Четвертое – мотивы, под воздействием которых совершаются преступления в банковской сфере, до удивления просты: да, это те же

деньги. Его величество «откат», за предоставление банковских услуг, размеры которого зависят от множества условий (регион, где проходит сделка, сумма самой сделки, характер взаимоотношений между участниками и пр.), а величина может достигать многих миллионов, отнюдь не способствует желанию банкиров способствовать расследованию преступной деятельности в их среде.

И наконец, пятое – особое положение сотрудников банков, призванных обеспечивать безопасность. Любой профессионал, прошедший школу работы в полиции или другой правоохранительной службе, довольно легко выявляет все выше названные особенности банковской деятельности и должен сделать для себя непростой выбор: что из перечисленного он принимает, становится ли он соучастником процессов или сторонним наблюдателем.

Автор понимает, что его суждения не встретят одобрения у банковского сообщества, но они основываются на почти 10 летнем опыте работы в этой среде. Единственное, что можно добавить, что эти позиции -оценка криминальной составляющей и, естественно, не касаются всех банкиров, подавляющее число которых весьма добросовестно ведут свой бизнес.

Если говорить о направлениях обеспечения банковской безопасности на уровне самих банков, то они за более чем 20-летнюю историю развития банковского сектора в новой России достаточно неплохо проработаны и исходят как раз из комплексности подхода, принципов разумной достаточности, своевременности, динамичности. Другое дело, что несмотря на очевидную востребованность и крайнюю необходимость иметь в банковском секторе постоянно действующую систему мероприятий по обеспечению безопасности этого бизнеса, в силу некомпетентности ряда руководителей кредитных организаций, неумелого использования ими основных принципов и практических подходов к решению проблемы комплексной банковской безопасности, мероприятия в этой сфере в большинстве своем не носят системного характера и направлены на ликвидацию только отдельных угроз, что не обеспечивает надежной защиты банков.

На практике часто приходится сталкиваться со случаями, когда руководитель (владелец) банка или иное лицо принимающее решение, игнорируют мнение профессионалов безопасности, опираются на собственные, чаще всего дилетантские, представления, почерпнутые из СМИ или художественной литературы. К сожалению, обязательного обучения руководителя банка вопросам безопасности, как это делается, например, с директорами предприятий, допускаемым к работам со сведениями, составляющими государственную тайну, когда они в обязательном порядке проходят государственную аттестацию,

законодательством РФ не предусмотрено. А необходимость этого назрела.

Нужно подчеркнуть, что обеспечение банковской безопасности не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности кредитной организации, непрерывном управлении ею, контроле, выявлении ее узких и слабых мест и потенциально возможных угроз банковской структуре.

Банковская безопасность может быть обеспечена лишь при комплексном использовании всего арсенала средств защиты во всех структурных элементах банковской системы. Наибольший эффект достигается тогда, когда все используемые средства методы и мероприятия объединяются в единый целостный механизм – систему безопасности кредитной организации.

Никакое подразделение безопасности не может обеспечить требуемый уровень безопасности без помощи и надлежащей подготовки персонала кредитной организации и соблюдения им всех установленных правил, направленных на обеспечение безопасности.

На практике комплексная система безопасности должна создаваться на основе концепции безопасности кредитной организации – научно обоснованной системе взглядов на определение основных направлений, условий и порядка практического решения задач защиты банковской структуры от противоправных действий и недобросовестной конкуренции. [5]

Практические работники, исходя из опыта работы банков Северо-Запада РФ, как правило, направляют свои усилия на следующие направления деятельности подразделений безопасности банков:

1.Разработка структуры подразделения безопасности исходя их характера деятельности банковского учреждения.

2. Информационно-аналитическая работа подразделений безопасности.

3. Организация обеспечения безопасности банковского персонала.

4. Организация работы с персоналом кредитной организации.

5. Организация защиты конфиденциальной банковской информации.

6. Организация борьбы с мошенничеством в банковской сфере.

7. Организация противодействия легализации преступно полученных капиталов.

8. Организация обеспечения безопасности платежных систем, информационных банковских систем.

9. Организация защиты конфиденциальной банковской информации от утечки по техническим каналам.

10. Защита банковской информации при использовании Интернета.

11. Ограждение от недобросовестной конкуренции в банковской сфере.

12. Организация работы банка и подразделения безопасности в кризисной ситуации.

13. Организация работ по технической укрепленности кредитной организации.

14. Организация пропускного и внутриобъектового режима.

15.Организация обеспечения безопасности перевозки денежных средств и материальных ценностей.

16. Организация работы по возврату проблемных кредитов.

17. Организация взаимодействия с правоохранительными органами. [5]

Каждое из перечисленных направлений заслуживает отдельной развернутой статьи. Но в качестве примера того, как могут работать названные выше меры в решении наиболее часто встречающейся и наиболее сложной с точки зрения локализации этой угрозы проблемы рассмотрим ситуацию невозврата крупного кредита.

Для рассмотрения взята ситуация имевшая место в одном из коммерческих банков Санкт-Петербурга в 2008 году, в преддверии наступавшего банковского кризиса. Клиент, небольшая частная фирма, занимавшаяся производством оборудования для нефтегазоразведочной отрасли, уже имел положительную кредитную историю в этом банке, но размеры кредитов были невелики от 5-10 млн. рублей и брались они на небольшие сроки. В конце 2008 года поступила заявка на кредит размером в 300 млн. рублей для исполнения крупного заказа ОАО «Газпром». В качестве обеспечения предлагалось здание офиса фирмы в центре Санкт-Петербурга, часть произведенного оборудования и поручительства собственников фирмы. Рассмотрев, представленные заемщиком документы, кредитный комитет принял положительное решение и кредит был выдан.

Проблемы начались через три месяца, когда прекратилась уплата процентов по кредиту. Это послужило толчком для более глубокого изучения клиента, которое вскрыло целый ряд грубейших нарушений, как со стороны клиента, так и со стороны многих служб банка, включая и службу безопасности. Итогом же стало уголовное дело по статье «мошенничество» и как закономерный итог – владельцы фирмы получили 5 лет лишения свободы. Что же выяснилось? Сначала было установлено, что представленные клиентом в банк документы о якобы заключенном контракте с «Газпромом» - подделка. Использовались

устаревшие уже выведенные из оборота бланки «Газпрома», подписи и печати – фальшивые, лица, якобы подписавшие контракт – мифические. Эту проблему можно было решить еще в самом начале оформления кредита, если бы сотрудники банка (безопасность, клиентский блок или кредитчики) сделали бы один телефонный звонок и убедились в подлинности контракта.

Далее вскрылись проблемы с залоговым обеспечением: вместо здания, якобы принадлежавшего собственникам фирмы-заемщика, в наличии оказалось лишь три жилых квартиры. Все остальные документы на здание были сфальсифицированы: представлены фальшивые выписки из решений администрации городского района Петербурга. Бланки протокола были подлинные, но за указанным на них номером администрация, оказывается, рассматривала совсем другие вопросы, не имевшие к закладываемому зданию отношения. Произведенное фирмой оборудование – буровые установки – раздавались в залог сразу нескольким банковским организациям, при этом идентифицирующие «шильдики» на установках просто менялись в зависимости от того, кто приезжал их осматривать. При оформлении поручительства собственников также не обошлось без подлога, один из поручителей умудрился представить паспорт, в котором не стояло штампа о браке, и в силу этого не бралось согласие супруги, якобы отсутствовавшей, но которая, когда дело дошло до судебных разбирательств, оказалась весьма активной соучастницей кредитования.

Полученные компрометирующие данные использовались банком для рассмотрения материалов в арбитражном суде, который вынес решение в пользу кредитной организации, передав залог в ее распоряжение, и далее в обращении в органы МВД для возбуждения уголовного дела по ст. 159 ч 4 УК РФ. Проведенное следствие, которому служба безопасности банка оказывала всемерное содействие, установило, что кроме мошенничества с кредитом в рассматриваемом нами банке, эти же заемщики умудрились набрать в Санкт-Петербурге кредитов еще в шести других банках на сумму почти 1 млрд. руб., при этом везде использовались подлог документов, фальсификация и обман.

Возникает законный вопрос, почему во всех, вовлеченных в процесс псевдокредитования банках, «прошляпили» столь очевидные компрматериалы. Последующий анализ ситуации показал:

1. Явные огрехи во взаимодействии между подразделениями безопасности банков, несвоевременный обмен информацией между ними, ввод информации в единый банк компроматов Бюро кредитных историй Северо-Запада с запозданием, из-за боязни, уже упоминавшегося «выноса сора из избы».

2. Пренебрежение со стороны руководства банков к первичной информации о возможной несостоятельности клиентов, полученной подразделениями безопасности.

3. Стремление сотрудников клиентских и кредитных подразделений выдать кредит любой ценой в расчете на солидный «откат» и в связи с этим игнорирование тщательной проверки финансового состояния заемщика. Отсутствие постоянного мониторинга экономической деятельности клиента до и особенно после выдачи кредита.

4. Завышенная оценка залогового имущества и «закрытие глаз» на явные нестыковки в его оформлении.

5. И, наконец, отсутствие комплексности в организации процесса кредитования, когда все звенья банка, участники этого процесса, работают по единому замыслу в тесном взаимодействии на принципах открытости и взаимного доверия и в рамках строго соблюдения нормативной базы.

Приведенный пример со всей очевидностью показывает, что банковская безопасность – понятие сложное, требующее комплексного, системного подхода к решению ее правовых, организационных, кадровых, технических и иных проблем.

Литература:

1. Гусев В.С. и др. Экономика и организация безопасности хозяйствующих субъектов. Учебник – СПб.: ИД «Очарованный странник», 2001. – 256 с.

2. Концепция национальной безопасности Российской Федерации. В редакции Указа Президента РФ от 10.01.2000 г. № 24

3. Стратегия национальной безопасности Российской Федерации до 2020 года. Указ Президента РФ от 12.05.2009 г. № 537

4. Бажанов С.В. Интеграция российского и международного финансовых рынков. СПб.: Издательство «КультИнформПресс». 2005. – с.480,ил.

5. Н.А.Савинская, Н.М.Калугин Банковская безопасность: комплексная система обеспечения безопасности кредитной организации; Учеб.пособие.-СПб.:СПбГИЭУ,2001.- 302 с.

Гущин Н.А., Сальников В.Ю.

ВОЗВРАТНО-ОРИЕНТИРОВАННОЕ ПРОГРАММИРОВАНИЕ В 64-Х БИТНЫХ АРХИТЕКТУРАХ

Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

В работе исследуется один из видов компьютерных атак, популярных на x86-совместимых машинах и схожих с ними, связанных с переполнением буфера, когда адрес возврата функции на стеке подменяется адресом иной функции в программе - применительно к 64-х битным архитектурам. Данный тип атак носит название: «Атака возврата в библиотеку (англ. Return-to-libc attack)»[1] и позволяет нападающему выполнить какую-либо существующую функцию без необходимости внедрять вредоносный код в программу.

Для оценки возможностей использования ВОП-эксплойтов были изучены особенности 64-х битной архитектуры, и ее отличия от 32-х битной x86 архитектуры.

В частности, одним из критических изменений является измененный машинный интерфейс для приложений Application Binary Interface (ABI) x64 — это 4 регистра соглашения о вызовах с возможностью последующего возвращения этих регистров в стек. Передача аргументов через регистры в принципе меняет ситуацию[2]. Однако, и при использовании модифицированных методов передачи аргументов при вызове функций существуют способы атаки, использующие схожую с классической методику. Например, borrowed code chunks [3].

В качестве базовых были рассмотрены существующие способы защиты от атак возврата в библиотеку, среди них: наиболее эффективная на данный момент техника рандомизации адресного пространства (ASLR), предназначенная для рандомизации положения исполняемых сегментов при запуске процесса. Однако, как в Linux, так и в Windows, некоторые части адресного пространства не меняются из-за приложений с фиксированным адресом загрузки или разделяемых библиотек, несовместимых с ASLR. Более того, в некоторых эксплоитах базовый адрес DLL можно вычислить динамически - через утечку указателя или перебором.

Другие, дополняющие ASLR, защиты от атак, повторно использующих код, включают расширения компилятора, рандомизацию кода, проверку целостности потока управления и динамические решения, работающие при выполнении. Но на практике большинство из этих подходов почти никогда не применяются для защиты COTS-программ (Commercial-Off-

The-Shelf Software – коммерческое программное обеспечение), наиболее часто являющихся мишенью ВОП-атак, либо из-за нехватки исходного кода или отладочной информации, либо из-за издержек выполнения.

ЛИТЕРАТУРА:

1. Wikipedia: Return-to-libc attack [электронный ресурс]. URL: http://en.wikipedia.org/wiki/Return-to-libc_attack (дата обращения: 04.05.2014)
2. MSDN: Overview of x64 Calling Conventions [электронный ресурс]. URL: http://msdn.microsoft.com/ru-ru/library/ms235286.aspx (дата обращения: 04.05.2014)
3. x86-64 buffer overflow exploits and the borrowed code chunks exploitation technique [электронный ресурс]. URL: http://users.suse.com/~krahmer/no-nx.pdf (дата обращения: 04.05.2014)

Липатова К.В., Бердник М.В.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ЗА СЧЁТ ОПТИМАЛЬНОГО ПОДБОРА ПРОГРАММНЫХ СРЕДСТВ

Краснодар, Кубанский государственный технологический университет

Аннотация:

Статья посвящена вопросам повышения уровня информационной безопасности с помощью программных средств защиты. Особое внимание уделяется классификации программных обеспечения, а также вопросам реализации научных принципов информационной системы, которые должны обеспечиваться путём внедрения данных программ.

Summary:

Article is devoted to questions of increase of level of information security by means of protection software. The special attention is paid to software classification, and also questions of realization of the scientific principles of information system which have to be provided by introduction of these programs.

Тенденция развития современных технологий характеризуется постоянным повышением значения информации. Случаи хищения интеллектуальной собственности, промышленного шпионажа, получение

несанкционированного доступа к персональным данным и стратегически важным информационным ресурсам случаются все чаще и носят все более серьезный и угрожающий характер. Поэтому выбор средств и методов защиты информации от преднамеренного или случайного вмешательства в процесс ее функционирования, будь то кража информации, внесение изменений или разрушение ресурса системы, - это первое, о чем необходимо позаботиться.

Спектр *средств и методов защиты информации* обычно делят на две основные группы: организационные и технические.

Под *организационными* подразумеваются законодательные, административные и физические, а под *техническими* – аппаратные, программные и криптографические средства и методы защиты информации, направленные на обеспечение защиты объектов, людей и информации. [3]

Более подробно рассмотрим программные средства защиты информации. Программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.

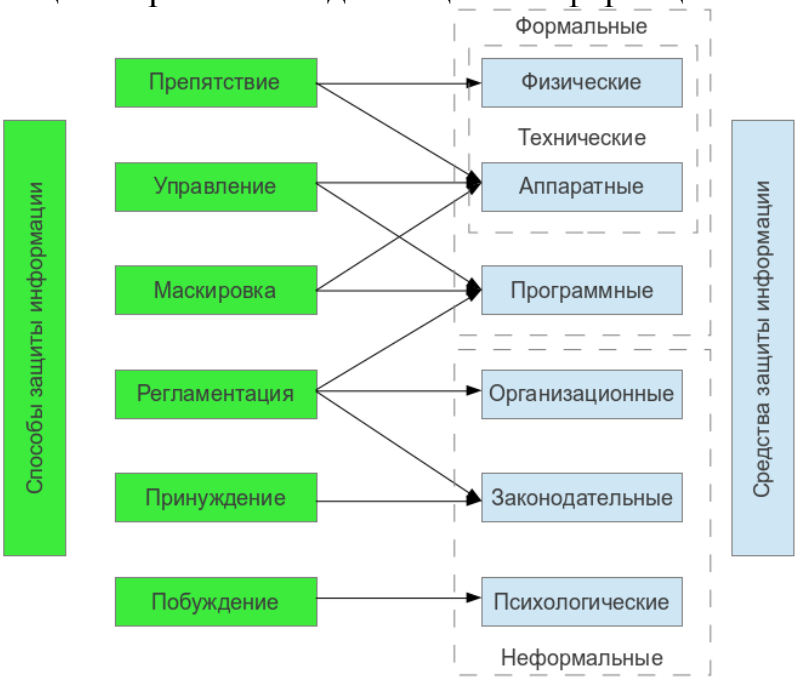


Рис.1 - Классификация методов и средств защиты информации

Как видно из рис.1, обеспечить защиту программных средств можно используя 3 способа защиты:

1. Управление - оказание управляющих воздействий на элементы защищаемой системы.
2. Маскировка - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника.

3. Регламентация - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов. [1]

Среди программных средств защиты можно выделить следующие:

1. средства архивации данных – программные средства, основной функцией которых является слияние нескольких файлов и каталогов в единый файл — архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов;
2. антивирусные программы – программы, разработанные для защиты информации от вирусов;
3. криптографические средства - специальные средства шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования;
4. средства идентификации и аутентификации пользователей – программные средства, предназначенные для распознавания пользователя по присущему или присвоенному ему идентификационному признаку, а также включающие в себя процесс проверки принадлежности пользователю предъявленного им идентификационного признака;
5. средства управления доступом - программные средства, обеспечивающие реализацию контроля и управления доступом;
6. средства протоколирования и аудита – средства сбора и накопления информации о событиях, происходящих в информационной системе предприятия, а также анализа накопленной информации, проводимого оперативно, почти в реальном времени, или периодически.

Надежная система защиты информации возможна только тогда, когда она будет построена на совокупности научных принципов. Поэтому выбирать программные средства нужно таким образом, чтобы данные принципы соблюдались:

1. объективность, научность - программы должны выбираться на основе глубокого анализа действительности, достоверной и научно обработанной информации, статистических данных.
2. законность и правовая обеспеченность - выбранные средства должны быть не запрещены для использования нормативными документами, а также являться лицензионными и сертифицированными; работа с данными программами должна быть регламентирована нормативно-правовой базой действующего законодательства.

3. комплексность, системность - необходимо, чтобы программные средства интегрировались с другими средствами, методами и способами обеспечения защиты информации, образовывая тем самым систему защиты информации.
4. экономическая эффективность – совокупные затраты от внедрения программных средств не должны превышать стоимость информации, на защиту которой направлены средства.
5. баланс интересов личности, общества и государства – установление программного обеспечения не должно нарушать Конституционные права и свободы граждан; при составлении комплексной системы защиты информации необходимо учитывать интересы общества и государства.
6. интеграция с международными системами безопасности. Программные средства должны быть совместимы с другими средствами защиты информации и интегрироваться с уже имеющимися международными системами безопасности. [2]

Таким образом, правильно выбранный программный комплекс позволит защитить критически важные данные и информационные активы, потеря которых может нанести непоправимый финансовый и репутационный урон.

Список использованной литературы:

1. Гришина Н.В. Организация комплексной системы защиты информации / Н.В. Гришина – М.: Гелиос АРВ, 2007. – 256 с.
2. Проект «Концепция стратегии кибербезопасности Российской Федерации»
3. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / П.Б. Хорев – М.: Издательский центр «Академия», 2005. – 256 с.

Малышкин С.Л.

ОЦЕНКА ВЕРОЯТНОСТИ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННОГО ПРОНИКНОВЕНИЯ ИНТЕГРИРОВАННОЙ СИСТЕМОЙ БЕЗОПАСНОСТИ

Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В настоящее время все большее распространение получают интегрированные системы безопасности (ИСБ), подсистемы которых

объединены каналами связи и имеют общие средства сбора и обработки информации и управления. Вследствие интеграции подсистем на том или ином уровне, можно говорить об увеличении вероятности обнаружения (ВО) угроз по сравнению с ВО в случае использования отдельных подсистем. В общем случае вероятность обнаружения угрозы ИСБ в целом зависит от вероятностей обнаружения этой угрозы отдельными подсистемами. А вероятность обнаружения угрозы подсистемой, в свою очередь, зависит от параметров средств обнаружения (СО). Поэтому для анализа эффективности ИСБ в целом необходимо знать вклад отдельных СО в обеспечение безопасности. Цель данной работы – дать оценку ВО угрозы несанкционированного проникновения интегрированной системой безопасности.

Рассмотрим произвольных объект, оборудованный ИСБ, состоящей из N подсистем. Совокупность подсистем обозначим $\mathbf{S} = [S_1, S_2, \dots, S_N]$. Пусть имеется J возможных угроз данному объекту. Это могут быть, к примеру, различные типы нарушителей, например, неквалифицированный, квалифицированный, профессионал. Сюда же можно включить различные варианты подготовленности, оснащенности, информированности нарушителя, а также их возможные комбинации.

Объект может быть разделен на I зон обеспечения безопасности. В зависимости от возможных угроз, в каждой зоне обнаружения (ЗО) располагаются те или иные средства обнаружения угроз, средства инженерной защиты, а также силы реагирования. Множество зон объекта обозначим $\mathbf{Z} = [Z_1, Z_2, \dots, Z_I]$. Множества $\mathbf{Z}$ и $\mathbf{S}$ образуют соответствие $q = (\mathbf{Z}, \mathbf{S}, \mathbf{Q})$, $\mathbf{Q} \subseteq \mathbf{Z} \times \mathbf{S}$. Т.е. та или иная зона может быть оборудована одной или несколькими подсистемами ИСБ или ни одной из них. Соответствие включает в себя все возможные пары элементов множеств $\mathbf{Z}$ и $\mathbf{S}$: $\mathbf{Q} = (\{Z_1, S_1\}, \{Z_1, S_3\}, \dots \{Z_i, S_n\}, \dots, \{Z_I, S_N\})$.

Рассмотрим случай с одной ЗО, оборудованной СО нескольких подсистем, способными обнаруживать j-ю угрозу. Вероятности обнаружения обозначим $P_{1j}^{O} - P_{Nj}^{O}$, где N – количество подсистем.

Рассчитаем суммарную ВО j-й угрозы с учетом всех подсистем, способных ее обнаружить. Так как различные подсистемы обычно используют для обнаружения угрозы разные физические принципы, будем исходить из предположения, что вероятность обнаружения угрозы какой-либо подсистемой P_{nj}^{O} не зависит от вероятности обнаружения той же угрозы другими подсистемами. Т.е. в данном случае можно говорить о независимости обнаружения нарушителя любой из подсистем. Т.о., рассматриваются три независимых события. В этом случае вероятность обнаружения хотя бы одной подсистемой j-й угрозы P_j^O будет равна

$$P_j^O = 1 - \prod_{n=1}^{N}(1 - P_{nj}^O). \quad (1)$$

Типичный пример многорубежной охраны представляет собой I последовательно расположенных неперекрывающихся ЗО. Нарушитель, передвигаясь по объекту по определенному маршруту, пересекает эти ЗО. ВО n-й подсистемой j-й угрозы в i-й зоне обозначим P_{inj}^{O}.

Для представления маршрута НП воспользуемся методом, применимым для различных типов подсистем, предложенным в [1, 2]. Как говорилось выше, объект может быть разделен на I зон, множество которых обозначили как $\mathbf{Z} = [Z_1, Z_2, \dots, Z_I]$. Множество препятствий обозначим $\mathbf{B} = [B_1, B_2, \dots, B_K]$. Нарушитель, передвигаясь по маршруту, может перемещаться из одной зоны в другую, а также преодолевать препятствия. При этом элемент маршрута нарушителя – переход – может быть реализован как переход от начала i-й зоны до начала k-й зоны; как переход от начала i-й зоны до начала k-го препятствия; как преодоление k-го препятствия с переходом в i-ю зону.

Т.о., возможны три вида соответствий для описания данных возможностей реализации переходов: соответствие между элементами множества зон $\mathbf{C_1} \subseteq \mathbf{Z} \times \mathbf{Z}$, между множеством зон и множеством препятствий $\mathbf{C_2} \subseteq \mathbf{Z} \times \mathbf{B}$ и между множеством препятствий и множеством зон $\mathbf{C_3} \subseteq \mathbf{B} \times \mathbf{Z}$. Объединим $\mathbf{C_1}$, $\mathbf{C_2}$ и $\mathbf{C_3}$ в супермножество $\mathbf{C} \supseteq \mathbf{C_1}, \mathbf{C_2}, \mathbf{C_3}$, которое содержит все возможные варианты переходов: $\mathbf{C} = [\{Z_1, Z_2\}, \{Z_2, Z_1\}, \{Z_2, B_1\}, \dots \{Z_i, B_k\}, \dots \{Z_I, B_K\}] = [c_1, c_2, \dots, c_l, \dots, c_L]$.

Элементы множества $\mathbf{C}$ могут принимать значения различных параметров переходов, например, продолжительности преодоления перехода или вероятности обнаружения перехода. Параметры переходов запишем в отдельные множества $\mathbf{C_T} = \left[T_{j1}, T_{j2}, \dots, T_{jl}, \dots, T_{jL}\right]$ и $\mathbf{C_P} = \left[P_{n1}^0, P_{n2}^0, \dots, P_{nl}^0, \dots, P_{nL}^0\right]$, соответственно для продолжительностей переходов и вероятностей обнаружения. Здесь P_{nl}^0 – вероятность обнаружения l-го перехода n-й подсистемой, а T_{jl} – продолжительность преодоления l-го перехода j-м типом нарушителя.

Маршрут нарушителя R_m включает в себя подмножество $\mathbf{C_m} \subseteq \boldsymbol{C}$ множества возможных переходов $\boldsymbol{C}$. Общая продолжительность маршрута T_{R_m} является суммой продолжительностей всех переходов c_m данного маршрута: $T_{R_m} = \sum_{R_m} T_m$. Согласно принципу своевременного обнаружения, эффективность СБ определяется по суммарной вероятности обнаружения нарушителя в момент (критическая точка обнаружения – КТО), когда у сил реагирования еще достаточно времени для его перехвата [3]. В нашем случае время до КТО можно найти, вычтя задержку прибытия сил реагирования $T_з$ из общей продолжительности

маршрута нарушителя: $T_{KTO} = T_{R_m} - T_з$. Обнаружение после КТО не имеет смысла, т.к. силы реагирования уже не успеют перехватить нарушителя.

С учетом вышесказанного перепишем выражение (1):

$$P_{jm}^{CO} = 1 - \prod_{l=1}^{KTO} \prod_{n=1}^{N} \left(1 - P_{lnj}^{O}\right), \qquad (2)$$

где P_{jm}^{CO} – вероятность своевременного обнаружения j-го нарушителя на m-м маршруте. Полученная формула позволяет рассчитать суммарную вероятности своевременного обнаружения нарушителя на маршруте проникновения интегрированной системой безопасности.

ЛИТЕРАТУРА

1. Волхонский В.В., Гатчин Ю.А. Подход к задаче анализа эффективности системы безопасности на основе вероятностных оценок временных параметров процесса проникновения на защищаемый объект // Вестник компьютерных и информационных технологий. М., Издательский дом «Спектр». – 2012. – №2. – с. 35-39.

2. Волхонский В.В. Некоторые вопросы разработки методологии построения систем контроля доступа и выбора технологии идентификации // Информационно-управляющие системы. – СПб.: – 2012. – № 4. – с. 78-83.

3. Гарсиа М. Л. Проектирование и оценка систем физической защиты / М.Л. Гарсиа ; пер. с англ. под ред. Р.Г. Магауенова. – М.: Изд-во Мир, 2003. – 386 с.

Малышкин С.Л.

АППРОКСИМАЦИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТИ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАНЫХ ДЕЙСТВИЙ ПАССИВНЫМИ ИНФРАКРАСНЫМИ ИЗВЕЩАТЕЛЯМИ

Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

На современном этапе развития общества всё большее значение приобретает защита информации, включающая в себя и физическую защиту объектов информатизации. Последняя предполагает использование различных ресурсов для создания препятствий доступу к

объекту защиты – носителям информации и другим информационным ресурсам. Эффективность такой защиты в значительной степени зависит от надежности обнаружения несанкционированных действий (НСД) на ранних стадиях проникновения на объект. Поэтому при анализе эффективности такой системы очень важной является правильная оценка вероятности обнаружения нарушителя в той или иной зоне обнаружения. Т.к. проведение испытаний часто является трудоемким и затратным процессом, а экспертные оценки не всегда бывают точны, представляет интерес применение вероятностного подхода к анализу надежности обнаружения НСД.

В работе [1] предложено оценивать вероятность обнаружения НСД с учетом плотности распределения продолжительности обнаружения и расстояния обнаружения. В [2, 3] проведено исследование влияния параметров движения нарушителя (скорости и направления) на вероятность обнаружения цели пассивным инфракрасным (ПИК) извещателем. При этом предлагается метод оценки вероятности обнаружения с помощью полученных опытным путем гистограмм плотности распределения расстояния обнаружения цели (нарушителя). Однако недостаток полученных дискретных распределений состоит в отсутствии аналитических выражений для закона распределения, что ограничивает возможности их применения в задачах анализа и синтеза систем физической защиты. Поэтому представляется целесообразным осуществить аппроксимацию экспериментальных данных, полученных в [2, 3] и получить аналитические выражения для законов распределения расстояния обнаружения нарушителя.

Исходные данные для аппроксимации представляют собой выборки расстояния обнаружения цели [2, 3]. В качестве цели использовался человек, одетый в джинсовые штаны и рубашку с длинным рукавом, ростом 180 см и массой тела 75 кг. Измерения проводились при следующих параметрах движения: скоростей движения 0,3, 1,5 и 3,0 м/с; направлений движения тангенциального (поперек направления на ПИК извещатель) и радиального (вдоль диаграммы направленности).

В ходе работы была выполнена проверка гипотезы о соответствии опытных данных различным известным распределениям, в частности, следующим: Гаусса, Рэлея, логнормальному, гамма-распределению, Максвелла, Вейбулла. Оценка точности аппроксимации производилась по критерию согласия Пирсона χ^2 при уровне значимости 0,05. На рис. 1 приведены примеры гистограмм плотности распределения расстояния обнаружения цели и соответствующие аппроксимирующие кривые.

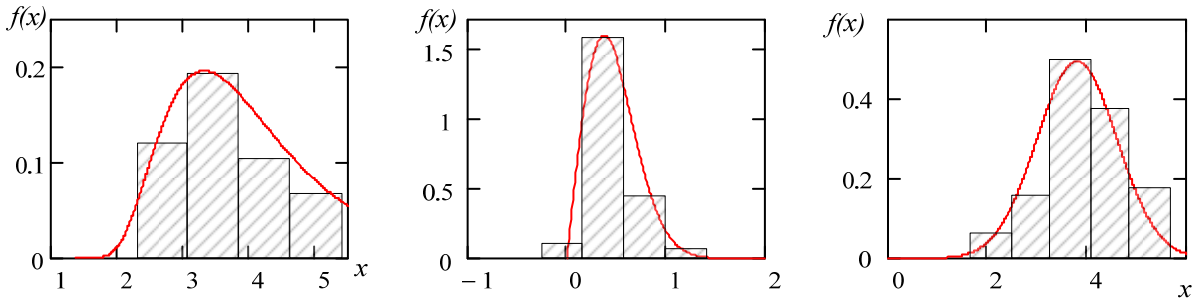


Рис. 1. Аппроксимация гистограмм плотности распределения расстояния обнаружения

В результате были отобраны наиболее точно соответствующие опытным данным распределения – Гаусса $f(x)=\frac{1}{\sigma\sqrt{2\pi}}\exp\left\{-\frac{(x-m)^2}{2\sigma^2}\right\}$, Рэлея $f(x)=\frac{x}{c^2}\exp\left\{-\frac{x^2}{2c^2}\right\}, x\geq 0, c>0$, логнормальное $f(x)=\begin{cases}\frac{1}{xc\sqrt{2\pi}}\exp\left\{\frac{-(\ln x-\mu)^2}{2c^2}\right\}, & x>0\\ 0, & x\leq 0\end{cases}$, гамма $f_k(x)=\begin{cases}\frac{\lambda^k x^{k-1}e^{-\lambda x}}{\Gamma(k)}, & x>0\\ 0, & x\leq 0\end{cases}$. А также построены графики зависимости значений параметра χ^2 от параметров движения нарушителя. Значения χ^2 для разных случаев скорости и направления движения цели приведены в табл. 1.

Таблица 1. Значения χ^2 для различных параметров движения цели

Направление	Скорость	Распределение Гаусса	Распределение Рэлея	Логнормальное распределение	Гамма-распределение
Тангенциальное	v=0.3 м/с	13,54	10,96	8,1	27,19
	v=1.5 м/с	110	111,12	110,5	143,54
	v=3.0 м/с	67,61	76,54	60,87	73,47
Радиальное	v=0.3 м/с	0,61	0,28	72,18	0,3
	v=1.5 м/с	1,07	1,93	14,01	2,76
	v=3.0 м/с	14,15	10,5	5,53	6,79

На основании полученных данных можно судить о применимости для аппроксимации закона распределения расстояния обнаружения цели ПИК извещателем одного из аналитических выражений, упомянутых выше, в различных условиях несанкционированного проникновения.

ЛИТЕРАТУРА

1. Волхонский В.В. К вопросу повышения вероятности обнаружения несанкционированного проникновения на охраняемый объект // Вестник Воронежского института МВД России. – 2011. – №4. – С. 37-44.

2. Волхонский В.В., Воробьев П.А. Методика оценки вероятности обнаружения несанкционированного проникновения оптикоэлектронным извещателем // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 1(77). – С. 120-123.

3. Волхонский В.В., Воробьев П. А. Анализ характеристик обнаружения нарушителя ПИК датчиками охранной сигнализации // Алгоритм безопасности. – 2012. – № 1. – С. 44-46.

Масалова К.В., Шарлаев Е.В.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИСПДн В ВУЗе

г. Барнаул, Алтайский государственный технический университет

В ВУЗе хранится и обрабатывается огромное количество информации, в том числе персональные данные (ПДн) различных категорий субъектов ПДн. ВУЗы являются операторами ПДн, и соответственно, на них распространяется действие закона о 152-ФЗ «О персональных данных» [1].

Проведя анализ нормативно-правовой базы, практического опыта в области информационной безопасности становится очевидным, что разработать эффективную систему защиты информационных систем можно только в соответствии с действующими требованиями руководящих документов и рекомендаций.

ВУЗы, как правило, обращаются к коммерческим организациям, оказывающим услуги в области защиты информации. Это увеличивает расходы на защиту ПДн, но гарантирует наличие отлаженной системы защиты информации с полным пакетом документации.

Основными проблемами, с которыми сталкиваются при организации защиты ПДн в ВУЗе, являются: территориальная рассредоточенность ресурсов информационных систем, большое количество серверов, к которым привязаны ИСПДн, порой с разными уровнями защищенности, выход многих ИСПДн в сети общего пользования. Поэтому самым разумным подходом будет являться рассмотрение каждой ИСПДн отдельно, а уже затем рассматривать их в совокупности.

В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований..», требования по защите персональных данных в ИСПДн зависят от уровня защищенности ИСПДн[2].

Типичная ситуация для ВУЗа это обработка специальных ПДн субъектов которые могут являться или не являться сотрудниками оператора в количестве до 100 000, актуальные угрозы третьего типа (для АС). Модель угроз строится на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России. То есть, большая часть ИСПДн будет отнесена к 3 УЗ, однако встречаются ИСПДн с другим уровнем защищенности.

В реальном ВУЗе, который брался за основу разработки, ИСПДн имеют 3 УЗ, соответственно для выполнения большинства требований на АРМ и серверах оказалось достаточно установить антивирусное средство, СЗИ НСД с токеном и персональный межсетевой экран соответствующих классов и сертифицированных ФСБ и ФСТЭК России. При выборе данных средств защиты руководствовались как эффективностью, так и экономической целесообразностью.

На данный момент в учебном заведении уже установлена и настроена данная система защиты персональных данных. Все СЗИ настроены в соответствии с матрицей доступа. ВУЗ, как оператор ПДн, успешно прошел проверку государственных регуляторов на предмет выполнения требований закона №152-ФЗ «О персональных данных».

В силу ряда особенностей операторам ПДн сложно самостоятельно разработать, установить и настроить эффективную, отвечающую всем требованиям законодательства систему защиты, поэтому чаще всего прибегают к услугам коммерческих предприятий, занимающихся информационной безопасностью. Они предлагают ВУЗу индивидуальные проекты, которые согласовываются на всех этапах построения и, при наличии жестких рамок, не позволяющих реализовать ни один из предложенных проектов, ищут альтернативные пути защиты или ухода от защиты.

Список использованных источников:

1. О персональных данных: Федеральный закон от 27 июля 2006 № 152-ФЗ (ред. от 23.07.2013 N 205-ФЗ): [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.

2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119: [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые

системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.

3. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18.02.2013 № 21: [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.

Носаль И.А.

ОБОСНОВАНИЕ ОПТИМАЛЬНОГО НАБОРА ПРАВ ДОСТУПА

Санкт-Петербург, ФГБУН Санкт-Петербургский институт информатики и автоматизации РАН

В работе предложен алгоритм обоснования оптимального набора прав доступа для заданных условий. Произведено моделирование защищаемого процесса, предложена математическая модель оценки оптимальности, отражены результаты моделирования и проведен сравнительный анализ для двух наборов данных.

Ключевые слова *– информационная безопасность, моделирование, марковский процесс, разграничение прав доступа.*

Для крупных холдингов и организаций с иерархической территориально – распределенной структурой, в условиях большого колебания уровня компетенции персонала в области безопасности, уровня осознания информационной безопасности (ИБ) руководством и квалификации специалистов в филиалах, структура системы разграничения доступа должна обеспечивать систематизацию, отслеживаемость, подотчетность и контроль предоставления доступа к разным типам ресурсов. Поскольку именно наличием человеческого фактора (инсайдера) объясняется невозможность создания абсолютно защищенной системы, учитывая, что уровень защищенности объекта равен уровню защищенность самого его слабого звена, вопрос выбора системы разграничения доступа и проработки наиболее оптимального набора прав доступа является одним из самых актуальных практических вопросов информационной безопасности.

Необходимо разработать систему моделей и алгоритмы реализации

угроз информационной безопасности актуальных для выбранного процесса, учитывая широкий круг условий, отражающих объективные закономерности реального процесса, что позволит произвести соответствующую оценку.

Для решения поставленной задачи предлагается формализовать выполнение критичной функции организации, возможных деструктивных воздействий для нее и мер по защите в виде графа состояний, такой процесс можно рассматривать как марковский, где дугам графа могут быть поставлены в соответствие интенсивности переходов из состояния в состояние. Они в свою очередь могут задаваться исходя из регламента моделируемого делового процесса, тогда вероятность перехода в состояние нарушения достоверности информации будет обратно пропорционально отражать состояние защищенности процесса. Пример моделирования представлен в работе [1].

Примером описанной выше организации может выступать крупный социально-ответственный институт, предоставляющий государственные услуги, в том числе по предоставлению различных выплат населению. Рассмотрим в качестве примера напрямую связанный с оперированием денежными средствами деловой процесс «Назначение и выплата» и его подпроцесс «Расчет выплат». Актуальной угрозой для этого подпроцесса является возможность корректировки данных персоналом, имеющим доступ к соответствующим записям в базе данных. Но вероятность этой угрозы, помимо изменений периода проверки назначенных сумм и выплатных документов, можно снизить дополнительными мерами, касающимися порядка организации предоставления доступа к защищаемым ресурсам. К примеру, не должны пересекаться права сотрудников, которые осуществляют ввод данных и контролируют формирование выплатных документов.

Построим для указанного подпроцесса граф состояний, учитывающий возможные действия нарушителя и мероприятия по защите. В обобщенном виде он будет выглядеть следующим образом:

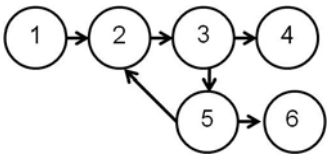


Рис. 1а. Подпроцесс, при условии разделения прав

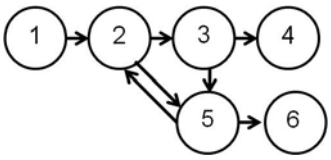


Рис. 1б. Подпроцесс, при условии смешения прав

На рисунках выше состояние 1 – принято решение об удовлетворении заявления; 2 – произведен расчет сумм, полагающихся к выплате в соответствии с последним принятым решением (в т.ч. перерасчет по окончании месяца или «массовый перерасчет»); 3 –

выплатные документы сформированы; 4 – выплаты произведены корректно (в соответствии с решением), 5 – в выплатные документы внесены несанкционированные изменения, 6 – выплаты произведены некорректно.

При этом, как уже было сказано выше, чем меньше процесс находится в состоянии 6, тем выше уровень ИБ. Также он зависит от изменения параметров переходов из состояния 3 в состояния 4 и 5, и из состояния 5 в состояния 2 и 6. Увеличение времени перехода из состояния 5 в состояние 6 связано с улучшением эффективности защитных мер. Заметим, что в случае предоставления пользователям неоптимального набора прав доступа (в данном случае права на ввод и контроль ввода выданы одному и тому же сотруднику), граф состояний будет обладать еще одним ребром перехода из состояния 2 в состояние 5 (рис. 1б.), поскольку несанкционированные изменения могут оказаться не исправленными.

Учитывая особенности рассматриваемого процесса, приведем оптимизационную модель, в соответствии с которой предлагается осуществлять обоснование оптимального набора прав доступа (в зависимости от особенностей защищаемого процесса она может быть переформулирована).

В нашем случае, требуется обеспечить минимальную вероятность некорректной выплаты, вероятность выплаты в соответствии с законодательством не ниже заданного значения и период корректировки сумм в выплатных документах не выше допустимого на заданном интервале времени *T*.

Таким образом, оценку эффективности выданных прав доступа рекомендуется осуществлять согласно модели:

$$P_6(T) = \min_{k \in Q} P_{6_k}(t), \quad (1)$$

$$P_{4_k}(T) \geq P_{зад}, \quad (2)$$

$$T_{52_k}(T) \leq T_{доп}, \quad (3)$$

$$k=1,2. \quad (4)$$

В модели (1) - (4) приняты обозначения: k – число сравниваемых вариантов прав доступа, $P_6(T)$ – вероятность некорректной выплаты на момент времени T (вероятность нахождения процесса в момент времени T в состоянии 6), $P_{4_k}(T)$, $P_{6_k}(T)$ – вероятность того что выплаты произведены в соответствии с законодательством и вероятность некорректной выплаты при к-том варианте доступа на момент времени T, соответственно; $P_{зад}$ – заданная нижняя граница вероятности выплаты в соответствии с законодательством; $T_{52}(T)$ – период корректировки сумм в выплатных документах (период перехода из состояния 5 в состояние 2); $T_{доп}$ – допустимый период корректировки сумм в

выплатных документах.

Все расчеты были осуществлены в программном комплексе MatLab. Результаты моделирования представлены на рисунках ниже, где процесс на момент времени t=0 находился в состоянии 1. Здесь видно, что во втором случае не выполняется условие $P_{4_k}(T) \geq P_{зад}$, при $P_{зад}$=0,8, а также на момент времени T=100 вероятность некорректной выплаты в первом случае значительно ниже $P_{6_1}(T) \leq P_{6_2}(T)$.

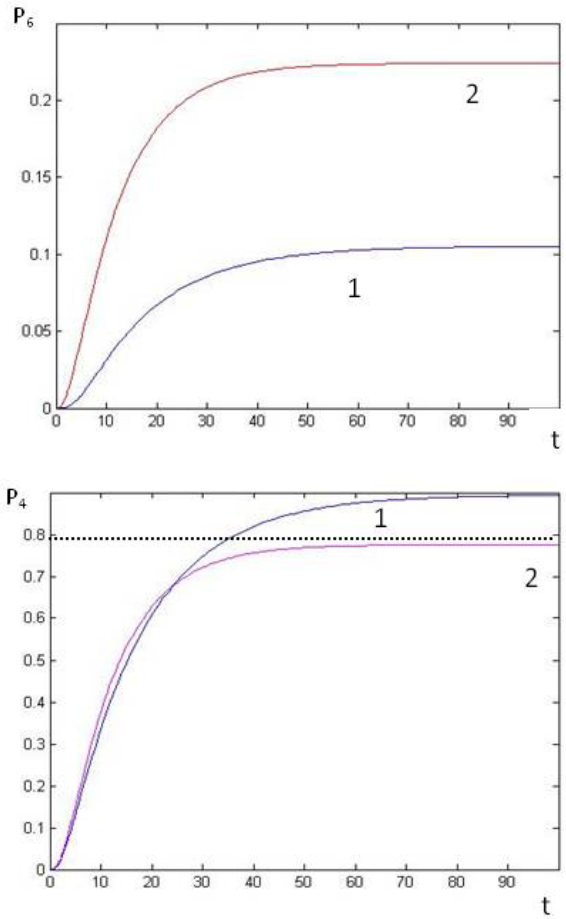


Рис.2. Зависимость вероятности некорректной (а) и корректной (б) выплаты от времени для набора с разделением прав (кривая 1) и для набора со смешением прав (кривая 2).

Интересным представляется поведение функции $P_4(t)$ на промежутке времени [10;40], где сначала превалирует вероятность корректной выплаты для набора со смешением прав, а после T=25 для набора с разделением прав. Это можно объяснить тем, что при смешении прав скорость прохождения проверок в целом возрастает, но со временем количество ошибок (случаев некорректного расчета выплат) накапливается и вероятность корректной выплаты $P_{4_2}(T)$ замирает на показателе 0,78. Тогда как в случае разделения прав доступа при рассмотрении работы процесса на более продолжительном промежутке

времени вероятность корректных выплат $P_{4_1}(T)$ возрастает до 0,9.

Основываясь на полученных результатах, предпочтение следует отдать первому варианту набора прав доступа, который при заданных условиях обеспечивает минимальную вероятность нарушения делового процесса.

Литература:

1. Осипов В. Ю., Носаль И. А. Обоснование периода пересмотра мероприятий по защите информации // Информационно – управляющие системы. 2014. № 1. С. 63-69.
2. Осипов В. Ю., Носаль И. А. Обоснование мероприятий информационной безопасности // Информационно – управляющие системы. 2013. № 2(63). С. 48-53.
3. Миронов В. В., Носаль И.А. Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» // Информация и безопасность. 2011. № 2. С. 209–211.

Сучкова Л.И., Якунин А.Г.

ГИБРИДНЫЙ ИНТЕЛЛЕКТУАЛЬНЫЙ МЕТОД ИДЕНТИФИКАЦИИ СОБЫТИЙ В АКУСТИЧЕСКИХ ПРИБОРАХ ОХРАНЫ

Барнаул, ФГБОУ ВПО «Алтайский государственный технический университет им. И.И. Ползунова»

Аннотация. В статье рассмотрена концепция гибридного нечетко-темпорального и лингвистического метода обработки данных с первичных измерительных преобразователей применительно к акустическим приборам охраны. Показаны преимущества предлагаемого метода по сравнению с традиционными методами.

При проектировании систем охраны зданий особую значимость имеет программно-техническое обеспечение для раннего обнаружения воздействий на заграждающие поверхности. В связи с этим с целью повышения надежности охраны актуальна разработка новых методов анализа сигналов с первичных измерительных преобразователей и приборов, устанавливаемых на дверные полотна, как наиболее уязвимое звено защиты. Такие воздействия на ограждающие конструкции, как удары, высверливание замка, применение отмычки не всегда могут быть обнаружены вибрационными или емкостными приборами что требует

разработки новых алгоритмов анализа их выходных сигналов. Проведенными исследованиями установлено, что осциллограмма сигнала и его амплитудные характеристики имеют характерные особенности для различных типов внешних воздействий на объект контроля, включающих открывание ключом, стук, удар, сверление и применение отмычки.

Для идентификации типа воздействия на ограждающую поверхность предлагается использовать гибридный подход, объединяющий нечетко-темпоральный и лингвистический методы анализа [1]. Анализ временного ряда, отсчетами которого являются значения амплитуд сигнала с пьезоэлектрического первичного измерительного преобразователя, осуществлялся на базе прогнозирующего паттерна поведения, который представляет собой набор следующих компонентов [2]:

$$P = <\boldsymbol{B}, \Psi_B, \boldsymbol{D_B}, \boldsymbol{A}, \Psi_A, \boldsymbol{D_A}, D_P, R>,$$

где $\boldsymbol{B}$ – собственно матрица – шаблон, используемая для сопоставления с ней группы рядов до текущего момента времени; Ψ_B – множество вычислительных процедур, переводящих отсчеты группы рядов в элементы матрицы $\boldsymbol{B'}$, используемой для сопоставления с элементами матрицы $\boldsymbol{B}$; $\boldsymbol{A}$– прогнозирующая матрица, описывающая поведение контролируемого объекта или группы ВР после текущего момента времени; Ψ_A – множество вычислительных процедур, формирующих элементы матрицы $\boldsymbol{A}$; $\boldsymbol{D_B}$ и $\boldsymbol{D_A}$ – дескрипторы матриц $\boldsymbol{B}$ и $\boldsymbol{A}$ соответственно, описывающие процессы преобразований рядов в $\boldsymbol{B'}$ и $\boldsymbol{A}$ посредством Ψ_B и Ψ_A; D_P – вектор –столбец, характеризующий паттерн в целом; R – маркер паттерна, ставящий в соответствие паттерну элемент из множества возможных состояний контролируемого процесса. Применительно к системам охраны различают, во-первых, штатное состояние, когда на заграждающую конструкцию не оказывается никаких воздействий, либо эти воздействия представляют собой шумы, помехи, регламентные воздействия с целью штатного проникновения на охраняемый объект, путем, например, отпирания запорного механизма и открывания дверного полотна; и, во-вторых, нештатное состояние (НС), вызванное тревожным механическим воздействием.

Установлено, что для идентификации простых и фиксированных во времени акустических сигналов метод идентификации НС на основе паттернов поведения обуславливает меньшее количество ошибок по сравнению, например, с дифференциальным методом. Если же структура сигнала сложна, и содержит элементарные фрагменты, последовательность которых для одного и того же типа поведения системы может меняться, целесообразно для идентификации вида воздействия применять гибридно-лингвистический подход, сочетающий

гибкость с простотой и высокой скоростью идентификации [2]. В нем элементарные паттерны поведения служат для формирования лингвистических переменных (ЛП), таких как «Длительность_импульса», «Амплитуда_импульса», «Скорость_нарастания_переднего_фронта_импульса», «Время_заднего_фро-нта_импульса» в разрезе частотных каналов. Для ЛП задавались термы, например, для описания амплитуды огибающей исходного сигнала использовалась ЛП «Амплитуда_ПЭП», для которой были введены нечеткие термы «до20», «от20до100», «от100до150», «от150до250», «более250». Общее число ЛП, подаваемых на вход алгоритмов идентификации, реализующих операции темпоральной логики, составляло 20=4ЛП*5 каналов (3 частотных плюс 2 амплитудных).

В результате экспериментов установлено, что вероятности ложных тревог, пропуска цели и ошибки идентификации при использовании гибридно-лингвистических паттернов анализа темпоральных закономерностей составили 0.7%, 0.7%, 1.0%, что существенно превышает аналогичные показатели других приборов. Такие приборы будут также эффективны при использовании в составе адаптивных подсистем охраны, так как имеют небольшое число ложных срабатываний.

Литература:

1. Сучкова Л.И., Абденов А.Ж. Гибридный подход к идентификации НС и их описанию в системах технологического контроля // Научный вестник Новосибирского государственного технического университета. – 2013. – № 3(52). – С.78-83.

2. Сучкова Л.И., Чумаков И.А., Якунин А.Г. Идентификация воздействий в приборах охраны упреждающего типа. – Deutschland, Saarbrücken, Palmarium Academic Publishing. – 2013. -181 с.

Штрошенко А.В., Загинайлов Ю.Н.

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Барнаул, Алтайский государственный технический университет

Обеспечение безопасности персональных данных необходимо, так как они являются важным и ценным активом организации. Кроме того –

это неотъемлемое требование к современному успешному бизнесу, закрепленное на законодательном уровне Российской Федерации [1].

Основной задачей по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) является построение адекватной системы защиты.

Существует несколько способов решения данной задачи, одним из которых является использование программного обеспечения, позволяющего частично автоматизировать процесс проектирования системы защиты ИСПДн.

Однако анализ рынка показал отсутствие программных продуктов с требующимся функционалом, что предопределило разработку программного обеспечения, которое позволит решить рассматриваемую проблему.

Программный продукт написан на языке программирования высокого уровня C# в среде разработки Microsoft Visual Studio 2013, подсистема формирования документов использует встроенную библиотеку Microsoft Office с наименованием «COM Interop».

Разработаное программное обеспечение имеет модульную структуру, что позволяет работать с требующейся частью функционала: есть два модуля в составе программы – «Модель угроз» и «Определение требуемого уровня защищенности», работа которых базируется на законодательных документах в области защиты персональных данных [2, 3].

К модулю «Модель угроз» относятся такие функции, как:

– определение типа ИСПДн на основе ответов пользователя;

– определение общего (предварительного) перечня угроз безопасности персональных данных на основе типа ИСПДн;

– определение актуальных угроз безопасности персональных данных, включающее в себя:

а) определение уровня исходной защищенности на основе ответов пользователя;

б) определение возможности реализации угрозы;

в) оценка опасности каждой угрозы и выявление актуальных угроз;

– определение типа угроз безопасности персональных данных.

К модулю «Определение требуемого уровня защищенности» относятся такие функции, как:

– определение типа угроз безопасности персональных данных;

– определение требуемого уровня защищенности персональных данных;

– определение мер по обеспечению безопасности персональных данных.

Разработанное программное обеспечение позволяет сэкономить деньги организации, время специалистов компании, а также позволяет избежать ошибок в расчетах (которые возможны при ручной обработке данных). Программа незаменима в случае проектирования системы защиты ИСПДн собственными силами, также может использоваться организациями, предлагающими услуги по защите персональных данных, для упрощения и автоматизации своей деятельности.

На данный момент учтены последние изменения в законодательстве в области защиты персональных данных, имеющиеся на первый квартал 2014 года.

Список используемых источников:

1. Федеральный закон №152-ФЗ от 27.07.2006 «О персональных данных» [Электронный ресурс] / Режим доступа: http://www.consultant.ru/document/cons_doc_LAW _149747/, свободный – Загл. с экрана. – Яз. рус.

2. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] / Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/, свободный – Загл. с экрана. – Яз. рус.

3. Приказ ФСТЭК №21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] / Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_146520/, свободный – Загл. с экрана. – Яз. рус.

СЕКЦИЯ 2
МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Tugberk Kara

PROCESSING CANNY'S EDGE DETECTION ALGORITHM INTO A COMPACT FORM USING WAVELETS

St.Petersburg, Saint Petersburg State Polytechnical University
tugberkkara@gmail.com

1. INTRODUCTION

The changes in brightness in a digital image produces some set of discontinuities and a set of curved line segments called edges. The method of selecting these segments is edge detection which is highly used in image processing, machine vision and computer vision. Determining image components in a digital image after applying edge detection algorithm is much more simple and straightforward.[7]

If the image intensity function changes rapidly in an image, it forms an edge.[2,7]

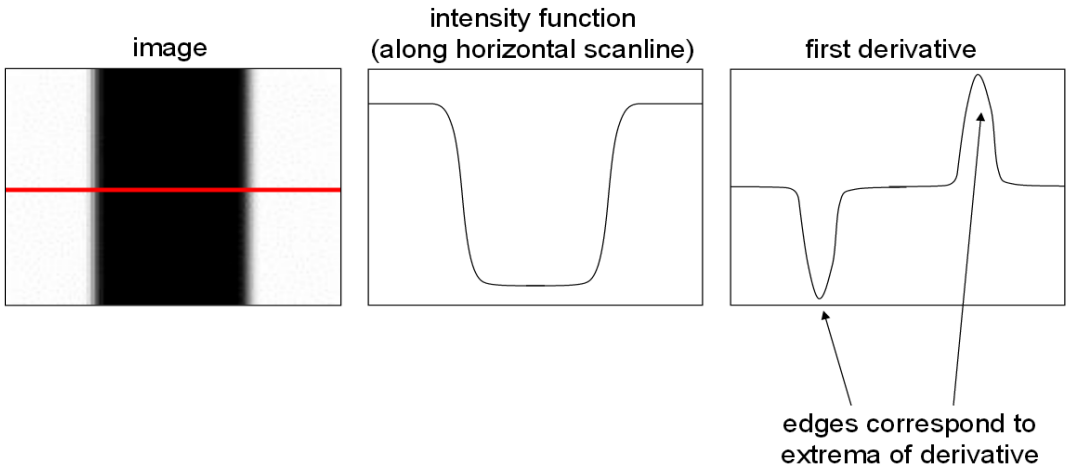


Figure 1: Intensity function and its first derivative example[2]

Scientists can divide edge detection algorithms into two groups. Search-based and zero-crossing based. In search-based methods, scientists find edge strength, usually a first derivative expression, such as a gradient magnitude. They then search for the local directional maxima of the gradient magnitude

using usually gradient direction. Zero-crossing algorithms look for zero crossings in a second order derivative expression computed from the image to find edges, usually the Laplacian or the zero-crossings of a non-linear differential equation. [2,7]

Before edge detection as usual, a smoothing stage such as Gaussian smoothing is used, because both digital cameras and conventional film camera images have noise from different source types. Scientists need to remove the noise partially in the domain of computer vision. Thus, they enhance image structure at different scales. The edge detection algorithms published up to this time differ in the types of smoothing filters and measuring ways of edge strengths applied to the image. Canny's algorithm is the most state of the art solution. His detector uses first order derivatives of Gaussian. He divides his algorithm into four stages which are noise reduction, finding intensity gradient of an image, non-maximum suppression and hysteresis thresholding.[2,7]

Although Canny used Gaussian filtering, it is known that, in edge detection, it does not give good results. Hence Gaussian filtering combines parallel and crossing lines. In Canny's edge detection algorithm, a pixel is determined whether it is on a line or not by looking its neighbors. However, in images filtered with Gaussian, finding a local maximum among pixels hampers in detecting particular lines. Thus, Canny's method is more sensitive to delicate lines. This situation expresses itself in finding wrong lines and flickers on the lines. Using small sized windows such as 3*3 and 5*5 in noisy images result in fake and discrete lines. Canny in his edge detection study highlights this to use small size windows as signal noise rate allows. Basic aim in that is to detect local changes in the closest distance to their places. If researchers use a bigger operator, it would touch neighboring lines and respond according to that. Therefore to prevent close edges to mix up, we concede from using large operators and their suppressing property of noise.[6]

2. TOPOLOGICAL GRADIENT OPERATORS

In this study, initial smoothing is applied based on connectivity level maps using larger operators without any problem by the method of fuzzy topology. This proposed Topological Gradient decreases the problem of overflowing to the neighboring lines and generates a value only on the place where change occurs.Therefore, combining lines of close object problems are eliminated.[6]

3. WAVELET BASED SMOOTHING APPROACHES:

Wavelet functions are limited in space. Wavelets' frequency's limiting property, when a wavelet is transformed to its definition area, produces lots of functions and operators that use sparse wavelets. However by inversely looking, this sparsity results in lots of useful applications such as data compression, finding features in images and resolving problems in time series.

Another advantage of wavelet transforms is that windows in time frequency domain can be alterable. To differentiate frequency discontinuities, there is needed some short base functions. To obtain this, scientists need to have short high frequency and long high frequency base functions. Thus, researchers exactly gain by wavelet transformations. [2,5]

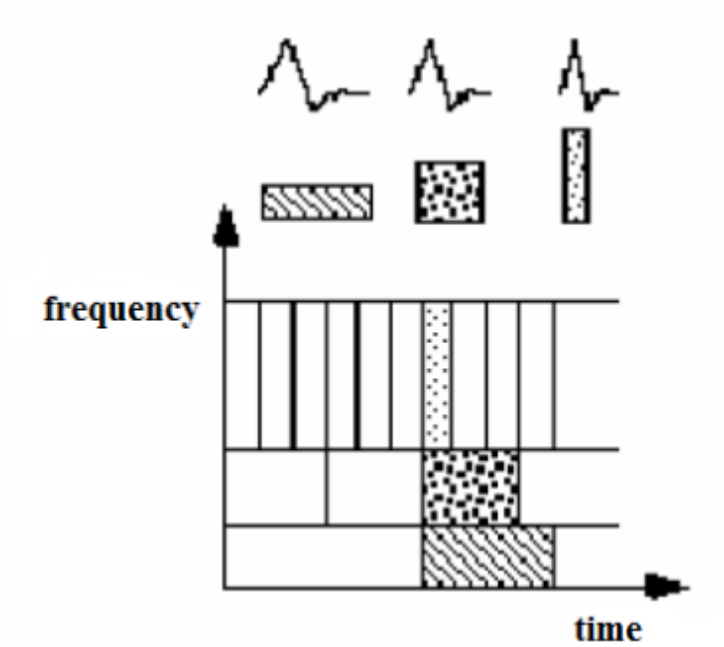


Figure 2: Time Frequency domain example of Daubechies wavelet base function[1]

Wavelet transformations have an infinite number of base function clusters. Thus, wavelet analysis has access to hidden information where other methods such as Fourier analysis can not approach. In wavelet transformation, scientists can have horizontal, vertical and diagonal outputs; therefore, we can have more commenting options. They can see the outputs in the three contexts more clearly by looking at the orientation of discontinuity boundaries. While using wavelet methods, 2-D or 3-D filtering studies can be done. For this approach, we can use several coefficients and hence we can obtain remaining parts more precisely.[3,5]

Wavelets are capable of resolving the uncertainties and changes of image gray-scale levels territorially. Using wavelets, scientists can extract a new image showing only the edges. The steps to edge detection with wavelets are as:[3]

1. Select an appropriate wavelet function.
2. Convert the image to decomposition levels using the function
3. Noisy scales containing significant energy are not selected and removed.
4. Detect the edges from the strained exhaustive coefficients.[3]

From up to this point, I will study on several methods proposed on edge detection with MATLAB software package and try to solve which wavelet

function can be best applied on a noisy image for noise reduction and image smoothening. In my opinion, the idea of changing coefficients would be beneficial in my aim. I will use an image of two sportsmen in a judo match and analyze their positions in terms of strikes, joint locks, prearranged forms and their timings.

4.CONCLUSIONS:

Using Gaussian filtering previous edge detection methods are not very efficient and successful. Therefore, Canny proposed a multilevel algorithm for edge detection including such as non-maximum suppression and hysteresis thresholding to eliminate false edges and to connect the gaps between the real edges. By using wavelet transformation, after smoothening and edge detection phases, there would be less unwanted and false results for our sample test images that Canny's method is not very successful at that point. Hopefully, by the proposed method there would not be needed a multi level algorithm in terms of better efficiency and less time; hence it would be more compact.

5.REFERENCES:

1.ALP, H., AKINCI, T. Ç., ALBORA, M. (2008). Comparison of Fourier and Wavelet Transforms in Geophysical Applications. *Journal of Engineering Sciences*. 14(1), pp. 67-76.

2.HAYS, J. (2013, September 18th).*Edge Boundary Detection.*[Powerpoint Slides] Presented at CS143 lecture at Brown University.

3.Kaur A.,Singh R., J 2010,'Wavelets for Edge Detection in Noisy Images',paper presented at *NCCI 2010-National Conference on Computational Instrumentation conference*,CSIO Chandigarh,India, 19-20 March 2010, <http://www.csio.res.in:8085/ncci/ICCIpdfDoc/Wavelets%20for%20edge%20detection.pdf>

5.POLIKAR, R. (1999). *The Engineer's Ultimate Guide to Wavelet Analysis-The Wavelet Tutorial.* Rowan University.Available at: College of Engineering website.<http://users.rowan.edu/~polikar/WAVELETS/WTtutorial.html>(updated 12 January 2001, accessed 29 April 2014)

6.ŞENEL H. G. (2007). Topological Gradient Operators for Edge Detection. *Eng&Arch.Fac.Eskişehir Osmangazi University*. XX(2), pp. 136-156.

7. WIKIPEDIA, THE FREE ENCYCLOPEDIA(2003). *Edge Detection*. Available at:<http://en.wikipedia.org/wiki/Edge_detection>(Updated 09 April 2014, accessed 29 April 2014)

Боровский А.С.

ОСНОВЫ КОМПЛЕКСНОГО ТЕОРЕТИЧЕСКОГО ПОДХОДА К ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЗАДАЧАХ УПРАВЛЕНИЯ ПРОЕКТИРОВАНИЕМ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ

г.Оренбург, Институт управления рисками и комплексной безопасности - Оренбургский государственный аграрный университет

Актуальность. Построение нового теоретического подхода к поддержки принятия решений в задачах управления проектированием СФЗ на основе интеграции принятия проектных решений, моделирования и оптимизации в условиях неопределенности требует разработки модели, обобщающей результаты оценки инженерно – технической защищенности (ИТЗ) объекта (О – модель) и размещения точек контроля (ТК – логическое понятие) на графовой модели объекта с последующей оптимизацией (S – модель). Процесс согласования О - модели и S - модели назовем процессом формирования обобщенной модели системы физической защиты (СФЗ) объекта. Обоснованием (доказательством) правильности принимаемого проектного решения служат рассуждения о том, что проектирование СФЗ критически важных объектов (КВО) должно в итоге опираться на два этапа: - концептуальное (системное) проектирование и рабочее проектирование [1]. Важность концептуального (системного) проектирования определяется целями и задачами, стоящими перед ним, от качества этого этапа зависит выполнение следующего этапа - рабочего проектирования. В связи с этим не может не возникнуть вопрос о качестве исследований (математического моделирования СФЗ) на этапе концептуального проектирования, в ходе которых производится оценка системы безопасности (оценки уязвимости (защищенности) объекта). Очевидным является то, что получение более точных оценок позволит избежать излишних материальных затрат. Таким образом, анализу качества методического и математического аппарата применяемого на стадии концептуального проектирования отводится ведущая роль, так как цена ошибки может быть очень высока.

Рассмотрим методологию построения математической модели объекта и модели технических средств защиты. Модель объекта назовем О – моделью. О – модель является теоретической базой для построения средств автоматизированного проектирования СФЗ и включает следующие уровни описания:

- структурно – логический уровень, описывает структуру объекта, его зоны и переходы между ними – теоретической основой является графовая модель объекта (SL – уровень);

- функциональный уровень, описывает данные производственного процесса объекта и выявляет его критические элементы (КЭ) (F – уровень).

Модель технических средств назовем S – моделью. S – модель включает следующие уровни:

- уровень ТК, описывает состав и виды ТК, используемых для защиты КЭ (ТК – уровень);

- уровень структурной защищенности, описывает экспертные оценки защищенности зон, рубежей и ТК (SZ – уровень).

Рассмотрим методологию, метод и алгоритмы формирования слияния О-модели с S – моделью на основе генетической оптимизации. Можно выделить следующие основные этапы поддержки принятия решения при проектировании СФЗ:

1.Разработка О – модели для проектирования, т.е. описание объекта защиты в виде двух моделей: структурно – логической и функциональной. На структурно – логической модели описываются зоны и рубежи перехода между ними. На функциональной - описывается производственный процесс с целью выявления КЭ объекта и их влияния друг на друга. Слияние этих двух моделей покажет, в каких зонах объекта имеются КЭ и их требуемый уровень защищенности. Для построения О – модели используется стандарт DFD, модифицированный под данную предметную область.

2.*Разработка S – модели для проектирования,* т.е. описание технических средств защиты в виде ТК. На этом этапе все средства защиты представлены в виде ТК. Каждая ТК вносит свой вклад в защищенность объекта, т.е. вводится понятие значимость ТК. Для определения значимости ТК использовался метод нечеткого многокритериального анализа вариантов [2]. Для оценки уровня защищенности объекта в данной модели рассчитывалась структурная защищенность с использованием нечетких чисел, т.е. экспертно определялись вероятности задержки и обнаружения каждого рубежа и зоны. Использование специального разработанного алгоритма позволило рассчитать меру структурной защищенности для каждого КЭ, и соответственно всего объекта.

3.*Формирование OS – модели.* На данном этапе подразумевается автоматическое размещение ТК на графовой модели объекта, т.е. фактически происходит слияние О –модели с S – моделью и определения оптимального уровня возможностей ТК (возможности обнаружения и задержки) через анализ структурной защищенности объекта. За

расстановку ТК и определения оптимального уровня их возможностей отвечает адаптированный генетический алгоритм (ГА) к данной предметной области.

Основная часть. В данной статье рассмотрим метод определения оптимального уровня возможностей ТК через анализ структурной защищенности объекта

Описание исходных данных задачи оптимизации. Рассмотрим процесс решения задачи оптимального уровня возможностей ТК с помощью стандартного ГА.

Экспертами задаются следующие исходные данные:

1. Граф объекта, в котором кроме зон и рубежей указываются КЭ и возможные точки проникновения.

2. Требуемые вероятности обнаружения и задержки для каждого КЭ.

Например: склад сырья - $P_{обн} = 0,9$; $P_{зад} = 0,85$.

Обозначим эти данные следующими переменными:

Для 1 КЭ - $(Y^{O}_{1}, Y^{З}_{1}) = (0,9, 0,85)$

Для 2 КЭ - $(Y^{O}_{2}, Y^{З}_{2}) = \ldots$ и т. д.

3. Возможные нечеткие значения для вероятностей обнаружения и задержки - набор термов $T_{обн}$ и $T_{зад}$.

Например $T_{обн}$ = {«очень низкая»; «низкая»; «средняя»; «высокая»; «очень высокая»} и $T_{зад}$ = {«очень низкая»; «низкая»; «средняя»; «высокая»; «очень высокая»}. Каждый терм задается функцией принадлежности в виде нечеткого множества, например «средняя» - {(0,2, 0,05) (0,3, 0,2) (0,35, 0,3) (0,4, 0,5) (0,43, 0,7) (0,45, 0,9) (0,5, 1) (0,55, 0,9) (0,57, 0,7) (0,6, 0,5) (0,65, 0,3) (0,7, 0,2) (0,8, 0,05)}. Элементы множества состоят из двух чисел: первое - значение элемента, второе вероятность того, что элемент принадлежит множеству. Для хранения данных задачи используем вместо имен термов их порядковые номера: 1 - «очень низкая»; 2 - «низкая»; и т. д. Обязательно должен присутствовать терм для обозначения отсутствия средств защиты на участке пути, т. е. нечеткое число, описывающее нулевую вероятность. Например, терм с номером 0 - «нулевая».

4. Условные стоимости средств защиты.

Каждое средство защиты, которое может быть в составе СФЗ, должно характеризоваться материальными затратами на установку и эксплуатацию, для подсчета стоимости всего СФЗ. Все участвующие в задаче средства защиты характеризуются только вероятностями обнаружения или задержки. Поэтому достаточно сопоставить каждому нечеткому значению вероятностей свою условную стоимость (разную для средств обнаружения и средств задержки), и далее считать, что все

средства с данной вероятностью обнаружения или задержки стоят одинаково. Используем переменные:

- $С_{обн}^{1}$ для $Р_{обн}$ = «низкая», $С_{обн}^{2}$ для $Р_{обн}$ = «средняя», $С_{обн}^{3}$ для $Р_{обн}$ = «высокая» … - стоимости средств обнаружения;

- $С_{зад}^{1}$ для $Р_{зад}$ = «низкая», $С_{зад}^{2}$ для $Р_{зад}$ = «средняя», $С_{зад}^{3}$ для $Р_{зад}$ = «высокая» … - стоимости средств задержки.

Простейший способ задания стоимостей – приравнять количество условных единиц к номеру нечеткого значения с условием, что нулевая вероятность имеет номер 0 (отсутствие средств защиты – нет затрат) и остальные вероятности нумеруются по возрастанию нечеткого значения, начиная с 1. Тогда, как ранее описывалось, стоимость будет приблизительно пропорциональна вероятностям и средство с самой низкой вероятностью будет самым дешевым - одна условная единица:

- $С_{обн}^{1} = 1$ для $Р_{обн}$ = «очень низкая», $С_{обн}^{2} = 2$ для $Р_{обн}$ = «низкая», $С_{обн}^{3} = 3$ для $Р_{обн}$ = «средняя», $С_{обн}^{4} = 4$ для $Р_{обн}$ = «высокая», $С_{обн}^{5} = 5$ для $Р_{обн}$ = «очень высокая»;

- $С_{зад}^{1} = 1$ для $Р_{зад}$ = «очень низкая», $С_{зад}^{2} = 2$ для $Р_{зад}$ = «низкая», $С_{зад}^{3} = 3$ для $Р_{зад}$ = «средняя», $С_{зад}^{4} = 4$ для $Р_{зад}$ = «высокая», $С_{зад}^{5} = 5$ для $Р_{зад}$ = «очень высокая».

5. Ограничения на вероятности обнаружения и задержки средств защиты в каждой зоне и в каждом рубеже объекта.

Вероятности обнаружения и задержки средств защиты в одной зоне или рубеже должны соответствовать заданным ограничениям в виде минимума и максимума. Ограничения могут задаваться как в нечеткой (номера термов), так и в четкой форме (числа от 0 до 1). Возможные ограничения: минимальные значения вероятностей для зон контроля больше 0, так как зона контроля подразумевает обязательную установку средства защиты, а максимальное значение ограничено возможностями имеющихся средств защиты, например 0,9 (табл. 1).

Набор ограничений:

($Р_{обн\ min}^{1}$, $Р_{обн\ min}^{2}$, $Р_{обн\ min}^{3}$, …, $Р_{зад\ min}^{1}$, $Р_{зад\ min}^{2}$, $Р_{зад\ min}^{3}$, …, $Р_{обн\ max}^{1}$, $Р_{обн\ max}^{2}$, $Р_{обн\ max}^{3}$, …, $Р_{зад\ max}^{1}$, $Р_{зад\ max}^{2}$, $Р_{зад\ max}^{3}$, …)

опишем через переменные:

($X^{О}_{1\ min}$, $X^{О}_{2\ min}$, $X^{О}_{3\ min}$, …, $X^{З}_{1\ min}$, $X^{З}_{2\ min}$, $X^{З}_{3\ min}$, …, $X^{О}_{1\ max}$, $X^{О}_{2\ max}$, $X^{О}_{3\ max}$, …, $X^{З}_{1\ max}$, $X^{З}_{2\ max}$, $X^{З}_{3\ max}$, …)

6. В исходные данные также включается результат работы алгоритма поиска путей. Определяются пути в графе объекта от каждой точки проникновения до каждого КЭ. Все найденные пути сохраняются в базу данных в виде последовательностей номеров зон и рубежей. Например, по таблице 2 первый путь идет через входную дверь, коридор, дверь лаборатории и заканчивается в КЭ - лаборатории: W_1 – (1, 2, 3, 5). Второй путь идет в лабораторию через окно W_2 – (6, 4, 5) и т. д.

Таблица 1

Пример ограничений на вероятности обнаружения и задержки

имя зоны или рубежа	минимальная вероятность		максимальная вероятность	
	средств обнаружения	средств задержки	средств обнаружения	средств задержки
Входная дверь	№0 нулевая (0)	№0 нулевая (0)	№4 высокая (0,7)	№3 средняя (0,5)
Коридор	№0 нулевая (0)	№0 нулевая (0)	№5 очень высокая (0,9)	№1 очень низкая (0,1)
Дверь в лабораторию	№0 нулевая (0)	№1 очень низкая (0,1)	№4 высокая (0,7)	№2 низкая (0,3)
Окно в лаборатории	№0 нулевая (0)	№1 очень низкая (0,1)	№5 очень высокая (0,9)	№3 средняя (0,5)
Лаборатория	№1 очень низкая (0,1)	№0 нулевая (0)	№5 очень высокая (0,9)	№2 низкая (0,3)
Прилегающая к окну территория	№0 нулевая (0)	№0 нулевая (0)	№5 очень высокая (0,9)	№0 нулевая (0)

7. Количество используемых хромосом, также является важной переменной для ГА, но может выбираться независимо от свойств объекта защиты. Экспертная информация здесь не требуется, количество хромосом может повлиять только на скорость получения конечного результата.

Возможные решения (хромосомы) включают в себя информацию о вероятностях обнаружения и защиты на каждом рубеже и в каждой зоне объекта.

Хромосома представляет собой вектор h_i , элементами решения являются части вектора – гены.

Все зоны и рубежи обозначаются именем или порядковым номером, и указываются вероятности в виде номеров термов (табл. 2).

Таблица 2

Пример информации в одной хромосоме

номер	имя	Обнаружение	Задержка
1	Входная дверь (рубеж 1)	№2 низкая	№0 нулевая
2	Коридор (зона 1)	№0 нулевая	№1 очень низкая
3	Дверь в лабораторию (рубеж 2)	№1 очень низкая	№1 очень низкая
4	Окно в лаборатории (рубеж 3)	№0 нулевая	№0 нулевая
5	Лаборатория (зона 2)	№0 нулевая	№2 низкая
6	Прилегающая к окну территория (зона 3)	№0 нулевая	№0 нулевая

Описываем хромосомы через массивы переменных:

$h_1 = (X^O_1, X^3_1, X^O_2, X^3_2, X^O_3, X^3_3, X^O_4, X^3_4, X^O_5, X^3_5, X^O_6, X^3_6,) = (2, 0, 0, 1, 1, 1, 0, 0, 0, 2, 0, 0)$

Один ген данной хромосомы содержит два целых числа X^O_1, X^3_1. Используем для записи решений десятичную систему счисления.

Процесс поиска решения. Перед генерацией нового поколения хромосом по каждому возможному решению (для каждой хромосомы) проводятся расчеты:

1. Для объекта в целом определяется стоимость средств защиты во всех зонах и рубежах. Например, по таблице 2 получаем всего 7 условных единиц, записывается переменная $C_{общая} = C_{обн}^{\ 2} + C_{обн}^{\ 0} + C_{обн}^{\ 1} + C_{обн}^{\ 0} + C_{обн}^{\ 0} + C_{обн}^{\ 0} + C_{зад}^{\ 0} + C_{зад}^{\ 1} + C_{зад}^{\ 1} + C_{зад}^{\ 0} + C_{зад}^{\ 2} + C_{зад}^{\ 0} = 7$.

2. Для каждого пути получаем массивы-вектора (начало вектора – точка проникновения, конец – защищаемый КЭ) с нечетким значением вероятностей обнаружения и задержки на каждом участке пути. Используем следующие переменные:

Путь 1: средства обнаружения: W^O_1 - $(X^O_1, X^O_2, X^O_3, X^O_5) = (2, 0, 1, 0)$

средства задержки: W^3_1 - $(X^3_1, X^3_2, X^3_3, X^3_5) = (0, 1, 1, 2)$

Путь 2: средства обнаружения: W^O_2 - … и т. п.

Определяем вероятность обнаружения S^O и вероятность задержки S^3 на всем пути по формулам [3]. В задаче применяется α-уровневый принцип обобщения с количеством α-уровней 50 и дефаззификация для получения четких значении вероятностей. Четкие значения требуются для операции сравнения рассчитанных вероятностей путей с требуемыми вероятностями.

Например, получены четкие значения для первого пути W_1 - $(S^O_1, S^3_1) = (0{,}7456, 0{,}9931)$

3. Проверяются целевые функции для оценки эффективности решения (качества хромосомы) и выбора следующей популяции генетического алгоритма.

В данной задаче проверяем две целевые функции.

Первая функция - F_1 использует критерий: вероятности обнаружения и вероятности задержки на каждом из всех возможных путей к КЭ должны соответствовать требуемым вероятностям для данного КЭ или превышать их. Если некоторые вероятности меньше чем требуемые, то значение функции будет равно суммарной разнице между требуемыми и имеющимися вероятностями на всех путях. Если все вероятности превышают требуемые, значение функции равно нулю.

Приведем формулы анализа первой хромосомы, используя вышеописанные переменные.

Требования 1 КЭ - (Y^O_1, Y^3_1) сравниваем с вероятностями первого пути (S^O_1, S^3_1) для хромосомы h_1.

Оценка первого пути - $F_1^1(h_1)$ рассчитывается как:

$F_1^1(h_1) = No_1^1 + Nз_1^1$,

где

$$No_1^1 = \begin{cases} 0, \text{ если } Y^O_1 <= S^O_1 \\ (Y^O_1 - S^O_1), \text{ если } Y^O_1 > S^O_1 \end{cases}$$

$$Nз_1^1 = \begin{cases} 0, \text{ если } Y^3_1 <= S^3_1 \\ (Y^3_1 - S^3_1), \text{ если } Y^O_1 > S^3_1 \end{cases}$$

Аналогично оцениваются остальные пути. Получаем значения для второго пути $F_1^2(h_1)$, для третьего $F_1^3(h_1)$ и т. д.

Значение первой целевой функции для текущей хромосомы h_1 равняется сумме оценок всех путей:

$F_1(h_1) = F_1^1(h_1) + F_1^2(h_1) + F_1^3(h_1) + \ldots$

Вторая целевая функция - F_2 использует критерий: суммарная стоимость средств защиты на объекте стремится к минимуму. Значение функции равно этому количеству:

$F_2(h_1) = C_{общая}$.

Таким образом, чем больше значения целевых функций, тем менее эффективно решение. Большая разность между требуемыми и имеющимися вероятностями означает недостаточную защиту объекта, а большая суммарная стоимость это лишние затраты на создание и обслуживание СФЗ.

4. Соответствие решения каждой целевой функции влияет на эффективность (приспособленность) $\mu(h_i)$ хромосомы. Формулы расчета эффективности задаются отдельно для каждой целевой функции.

Значение эффективности для первой функции рассчитывается следующим образом:

$$\mu_1(h_i) = (F_1(h_{\max}) - F_1(h_i)) / \sum_{k=1}^{n} (F_1(h_{\max}) - F_1(h_k)),$$

где h_{max} хромосома с максимальным значением целевой функции, n – общее количество хромосом.

При использовании данной формулы хромосома с максимальным значением получает эффективность равную 0 (и в дальнейшем никогда не попадет в родительский пул). Эффективности остальных хромосом распределяются в диапазоне от 0 до 1, причем сумма $\mu_1(h_i)$ будет равна 1. Если обнаруживается равенство эффективностей всех хромосом, то формула неприменима (деление на ноль). В этом случае все $\mu_1(h_i)$ равны и рассчитываются как единица, деленная на количество хромосом: $\mu_1(h_i) = 1 / n$.

Для второй функции действуем аналогично:

$\mu_2(h_i) = (F_2(h_{\max}) - F_2(h_i)) / \sum_{k=1}^{n} (F_2(h_{\max}) - F_2(h_k))$, в случае равенства эффективностей $\mu_2(h_i) = 1 / n$.

Общая эффективность хромосомы является средним значением эффективностей для целевых функций:

$\mu(h_i) = (\mu_1(h_i) + \mu_2(h_i)) / 2$

Для устранения противоречия целевых функций вводим в задачу понятия «уровень влияния целевой функции». Два числа (A, B), соотношение которых задает превышение значения одной целевой функции над другой, участвуют в расчете эффективности хромосомы:

$\mu(h_i) = (\mu_1(h_i) \times A + \mu_2(h_i) \times B) / (A + B)$

Таким образом, уровень влияния первой функции равен A/(A+B), а второй B/(A+B). В случае равенства уровней влияния (A=B), формула вырождается в вышеописанную: $\mu(h_i) = (\mu_1(h_i) + \mu_2(h_i)) / 2$

Чем больше разница между числами, тем сильнее одна целевая функция влияет на эффективность хромосомы (и на получаемые решения). При равенстве одного числа 0, целевая функция исключается из задачи, что можно использовать при анализе работоспособности алгоритма.

В итоге каждой хромосоме присваивается вероятность воспроизведения P_i для получения следующей популяции, которая зависит от эффективности $\mu(h_i)$ данной хромосомы. Используем пропорциональный отбор:

$P_i = \mu(h_i) / \sum_{i=1}^{n} \mu(h_i)$, т. к. сумма $\mu(h_i)$ равна единице, то $P_i = \mu(h_i)$

В соответствии с полученными вероятностями происходит случайный выбор хромосом в промежуточную популяцию (родительский пул) для последующего кроссинговера. Используем одноточечный кроссинговер со случайным выбором точки. После проведения кроссинговера и мутаций новая популяция полностью заменяет собой старую, и весь процесс повторяется, начиная с оценки хромосом.

Критериями остановки в данной задаче можно принять следующие условия:

1. Ограничение на число итераций. Это стандартное для ГА условие остановки и может быть определено экспериментально.

2. Отсутствия изменений по прошествии большого числа итераций в эффективности получаемых хромосом. Это показатель попадания алгоритма в локальный оптимум, что возможно является лучшим решением.

3. Получение решения близкого к оптимальному. Применимо, если свойства оптимального решения удалось определить с достаточной уверенностью.

Последний шаг - выбор среди хромосом решения с набольшим соответствием целевым функциям.

В условном примере использовалось пятьдесят хромосом в популяции. Список используемых в примере нечетких чисел отображен в таблице 3. Для поиска четкого аналога использовался метод дефаззификации - центр тяжести.

Далее был проведен поиск путей в графе. Количество всех возможных путей между точками проникновения и КЭ составило 665. После отсева путей, включающих в себя более чем одну точку проникновения, осталось 226. До запуска поиска решения выбраны уровни влияния целевых функций 1 для первой и 0,75 для второй и вероятность мутации равная 0,3.

Таблица 3

Нечеткие числа, используемые в примере

Имя нечеткого числа (терма)	Четкое значение (четкий аналог)	Цена средств обнаружения (условные единицы)	Цена средств задержки (условные единицы)
нулевая	0	0	0
почти 0	0,0542	1	1
очень низкая	0,1093	2	2
низкая	0,2	3	3
ниже средней	0,3	4	4
средняя	0,5	5	5
выше средней	0,7	6	6
высокая	0,8	7	7
очень высокая	0,8907	8	8
почти 1	0,9458	9	9

Найдено наилучшее решение после 46762 итераций (произошло 263858 мутаций): защищены все пути, общая стоимость равна 106 условных единиц. В течение последующих итераций полученные решения показывали соответствие целевым функциям меньшее или равное наилучшему найденному. Сделан вывод о попадании в локальный оптимум. Поиск решения был прерван после 80000 итераций.

Выводы. Представление модели СФЗ как объекта поддержки принятия решений в задачах управления его проектированием обосновано требованием к анализу качества методического и математического аппарата применяемого на стадии концептуального проектирования, которому отводится ведущая роль, так как цена ошибки в дальнейшем может быть очень высока.

Окончательная цель концептуального проектирования формирование слияния О- модели и S – модели, фактически расстановка ТК на структурно – логической модели объекта. За поиск наилучшего варианта отвечает адаптированный стандартный ГА.

Список литературы

1.Алаухов С.Ф., Коцеруба В.Я.Концепция безопасности и принципы создания систем физической защиты важных промышленных объектов // Системы безопасности, связи и телекоммуникаций. – М., 2002. – №41.

2.Ротштейн А.П., Штовба С.Д. Нечеткий многокритериальный анализ вариантов с применением парных сравнений // Известия РАН. Теория и системы управления. – 2001. - №3. – с.150-154.

3.Боровский А.С. Адаптация стандартного генетического алгоритма в задачах проектирования систем физической защиты потенциально-опасных объектов // Труды ИСА РАН, Спецвыпуск, 2013. Стр.26-33.

Демченко М.В., Борисов А.П.

БИОМЕТРИЧЕСКАЯ ЗАЩИТА НА ОСНОВЕ ПРОВЕДЕНИЯ АУТЕНТИФИКАЦИИ ПО ТЕМБРУ ГОЛОСА

г. Барнаул, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Алтайский государственный технический университет им И.И. Ползунова»

Несмотря на бурное развитие Интернета, и как следствие угрозу кражи хранимой в нем информации, остается актуальным непосредственный контроль доступа в помещения, в которых осуществляется хранение и обработка информации. С этой задачей справляются системы контроля и управления доступом (СКУД).

В настоящие время основным способом разграничения доступа в помещение являются обычные замки, или наличие охранников на входе в здание. По мере развития техники СКУД также развивались и на данный момент повсеместно вводят в эксплуатацию турникеты с бесконтактными картами, или электромеханические замки с использованием контактной памяти.

Основным недостатком таких систем является отчужденность носителя ключей от самого ключа (человека от ключа), или простота

взлома замков, по средствам подмены или кражи ключей. Этого недостатка лишены системы, использующие биологические характеристики человеческого организма.

Преимущества биометрических систем безопасности [2] очевидны: уникальные человеческие качества хороши тем, что их трудно подделать, биометрические характеристики не могут быть забыты или потеряны. В качестве измеряемого параметра в современных системах используются такие аутентификаторы, как голос человека, отпечатки пальцев, узор радужки. В данной работе будет использоваться голос человека.

Для обработки голоса [1] необходимо предварительно его записать в оперативную память компьютера или машинный носитель. Он представляет собой устройство состоящие из микрофона с усилителем, фильтра и аналогово-цифрового преобразователя.

Цифровой сигнал передается на компьютер по проводной линии. При прохождении по проводам, под действием внешних электромагнитных полей, сигнал может измениться, что приведет к неправильному распознаванию аутентификатора пользователя (его голоса) в дальнейшем, или злоумышленник может послать сигнал, который будет распознан системой, как сигнал успешной аутентификации. Для избегания этого проводные линии, по которым будет проходить информация между конечным устройством и компьютером, необходимо экранировать.

После прохождения по линий связи цифровой сигнал передается в память компьютера, на вход блока обработки сигнала. Блок обработки сигналов представляет собой программу схема, которой представлена на рисунке 1.

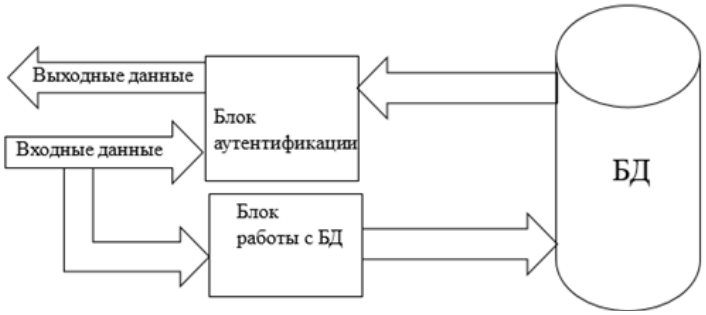


Рисунок 1 – Схема программы

На вход программы подается записанный голос. В зависимости от режима работы программы либо происходит запись в БД информации, либо происходит чтение из базы данных информации и сравнение ее с входными данными.

Блок аутентификации фильтрует входные данные от шумов, спектральное преобразование сигнала, фильтрация спектра, и наложение

на него окна Кайзера, непосредственное сравнение с эталонными образцами в базе данных и выдача сигнала на оконечное устройство. Блок работы с базой данных предназначен для добавления и удаления пользователей и просмотра статистики. В базе данных программы хранится образец голоса, статическая информация о лицах, допущенных в помещение информация о пользователях системы. Для защиты информации хранящейся в БД необходимо обеспечить надежную парольную аутентификацию, при доступе к консоли администратора. Сами таблицы БД и файлы эталоны будут шифроваться.

В конце выполнения работы планируется создать законченное программноаппаратное средство защиты информации – систему контроля и управления доступом на основе голосовой аутентификации. В комплекс будет входить оконечное устройство – блок записи сигналов и программа для работы администратора.

Список литературы

1. Идентификация пользователя по голосу [Электронный ресурс] – Режим доступа: habrahabr.ru/post/144580

2. Попов М. Биометрические системы безопасности [Электронный ресурс]/М. Попов. – Электрон. текстовые дан. 2002. – 20 мая. Режим доступа: http://daily.sec.ru/2002/05/20/print-Biometricheskie-sistemi-bezopasnosti.html

Кизько Б. А.

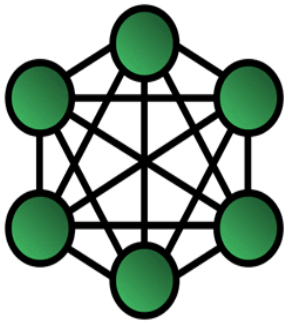
БЕСПРОВОДНЫЕ СЕТИ СТАНДАРТА 802.11S. ВОПРОСЫ МАРШРУТИЗАЦИИ И БЕЗОПАСНОСТИ

Санкт-Петербург, СПбГПУ, кафедра «Измерительные информационные технологии»

В последние годы развитие технологий привело к широкому распространению беспроводных сетей, которые принято называть Meshсетями. Mesh-сети (ячеистые сети, WMN — Wireless Mesh Networks) — это беспроводные одноранговые сети [1], топология которых получена из полносвязной топологии за счет удаления некоторого количества связей. В Mesh-сетях узлы равноправны, и каждый из них может выступать в качестве маршрутизатора. Топология сетей изменяется во времени, поэтому маршрутизация должна осуществляться динамически, а протоколы обмена данными в такой сети должны гарантировать доставку сообщений. Беспроводные Meshсети,

чаще всего, применяются для установления связи между устройствами, которые проблематично или невозможно соединить проводным подключением. Схематичный рисунок одного из вариантов Meshсети представлен на рис. 1.

Рис. 1. Пример топологии Mesh-сети



В настоящем докладе рассмотрены вопросы, связанные с маршрутизацией пакетов и безопасностью передачи информации в Meshсетях, построенных на основе стандарта IEEE 802.11s.

Стандарт IEEE 802.11s [2] дополняет семейство 802.11 (Wi-Fi) и предусматривает автоматическую установку соединения нескольких аналогичных устройств между собой, без участия какого-либо главного устройства-маршрутизатора.

IEEE 802.11s делает возможной автоматическую маршрутизацию между узлами сети Wi-Fi, в которой узлы для передачи информации могут задействовать своих соседей, используя прыжковый (multi-hop) механизм перенаправления трафика. Стандарт IEEE 802.11s регламентирует протоколы обнаружения, идентификации и установления соединения между соседними устройствами. Принцип его работы: в случае, если ближайшая точка доступа перегружена, данные перенаправляются к ближайшему незагруженному узлу. При этом пакет передается между узлами сети, пока не достигнет конечного места назначения. В документе введены новые протоколы на канальном уровне модели OSI, которые поддерживают широковещательную и многоадресную передачу, а также одноадресную посылку по автоматически перестраивающейся беспроводной сети.

IEEE 802.11s подразумевает [2] использование разных протоколов маршрутизации, но основным принято считать HWMP (Hybrid Wireless Mesh Protocol). К сожалению, не всё существующее беспроводное Wi-Fi оборудование позволяет организовать Meshсеть, работающую согласно принципам вышеуказанного стандарта, т.к. в данном случае от всех устройств-участников сети требуется поддержка метрики времени передачи в канале (Airtime Link Metric). Данная метрика определяется формулой ALM = (O + Bt/r)/(1-ef), где O и Bt – константы, определенные стандартом для различных физических реализаций (802.11a, 802.11b): Bt – число битов в тестовом пакете, O – накладные расходы доступа к

каналу, которые включают в себя заголовки пакетов, кадры протоколов доступа и т.д.; r – скорость передачи данных в канале (Мбит/с); ef – вероятность возникновения ошибки (измеряется экспериментально на пакетах длиной Bt). Эта метрика представляет собой оценку времени передачи (в секундах) пакета длиной Bt бит с учетом возможных ретрансляций при потерях в канале.

Протокол HWMP объединяет [3] в себе два режима построения маршрутов, которые могут быть использованы как по отдельности, так и одновременно в одной сети:

1. Реактивный режим – построение маршрутных таблиц по запросу, при необходимости инициировать обмен информацией между узлами.

2. Проактивный режим – регулярное обновление информации о маршрутах для всех узлов сети.

Доставка пакетов в Meshсети, построенной в соответствии с рассматриваемым стандартом, подтверждается. Кроме того, для повышения надежности передачи вводится так называемый MCCA-доступ [7] к среде (помимо распространенного CSMA), при котором предварительно резервируется множество интервалов времени, в течение которых возможна передача данных без конкуренции и коллизий пакетов.

Беспроводные Mesh-сети из-за особенностей своей организации уязвимы по отношению к нескольким видам атак:

1. Пассивное прослушивание сетевого трафика (нарушается конфиденциальность информационной системы).

2. Создание поддельных сообщений.

3. Создание «черных дыр» [6], то есть перенаправление входящих или исходящих пакетов атакуемого узла по неоптимальному маршруту. Злоумышленник после успешно проведенной атаки может реализовать атаку вида «человек посередине» (Man in the Middle, MitM).

5. Посылка сообщений с целью восстановления топологии сети. Нарушитель может инициировать передачу тестового сообщения, по которому узнает цепочку узлов, находящихся в пределах Meshсети.

6. Зашумление канала связи, то есть создание бессмысленных сообщений (спам), передаваемых по сети.

Сети, построенные в соответствии с IEEE 802.11s, в дополнение к протоколам TKIP и стандартам WEP и WPA2 (стандарт 802.11i), должны использовать протокол SAE (Simultaneous Authentication of Equals – одновременная проверка подлинности одинаковых узлов) [2], который обеспечивает проверку по паролю. SAE основан на протоколе Диффи-Хеллмана установления ключа шифрования. Для аутентификации участников сети и борьбы с атаками класса MitM используются MAC-адреса узлов.

Поддержка 802.11s заложена в ядро Linux, начиная с версии 2.6.26 [8]. Также операционная система FreeBSD 8 (и более новые версии) содержит [9] всё необходимое для работы с технологией.

Сеть, организованная по стандарту 802.11s, теоретически может объединить сколь угодно большое количество клиентов, крайние из которых могут находиться на расстоянии нескольких километров друг от друга. Однако развертывание ячеистой сети, состоящей из тысяч узлов, возможно, потребует создания масштабируемой централизованной системы управления [7], способной устанавливать и проверять соблюдение политик информационной безопасности и качество обслуживания (Quality of Service, QoS) в рамках целой сети. Ещё одной нерешённой проблемой IEEE 802.11s остаётся распределение IP-адресов внутри информационной системы, так как не документ не определяет, каким образом должна осуществляться децентрализованная генерация и выдача IP-адресов. В настоящее время считается невозможным [5] объединить несколько Mesh-сетей через существующие каналы связи (например, через сеть Интернет), но это не считается критичным.

Внедрение рассмотренного стандарта повышает пригодность беспроводных сетей Wi-Fi для приложений, которым требуется устойчивость к перегрузкам и избыточность (сенсорные сети, промышленные системы, системы поддержки общественной безопасности), а также быстрое развертывание и простота использования (например, в ходе подготовки массовых мероприятий).

ЛИТЕРАТУРА:

1. Cordeiro C.M. Ad hoc & sensor networks Theory and Applications / C.M. Cordeiro, D.P. Agrawal. – Singapore: World Scientific Publishing Co., 2006.

2. IEEE P802.11s/D1.08. Amendment: Mesh Networking. – IEEE, January 2008.

3. Шпилев С. А. Проактивная маршрутизация в IEEE 802.11s Mesh-сетях. – Третья всероссийская молодежная научная конференция по проблемам управления (ВМКПУ-2008) – 2008.

4. Вишневский В., Лаконцев Д., Сафонов А., Шпилев С. Mesh-сети: в ожидании стандарта IEEE 802.11s. // ЭЛЕКТРОНИКА: НТБ – 2008. – №3. – с. 98–106.

5. Осипов И.Е. Mesh-сети: технологии, приложения, оборудование // Технологии и средства связи. – 2006. – №4. – с. 39–45.

6. Perkins C., Bhagwat P. Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers. // Computer Communication Review. – 1994. – №4. – с. 234–244.

7. Khorov Evgeny, Lyakhov Andrey, Safonov Alexander. Flexibility of Routing Framework Architecture in IEEE 802.11s Mesh Networks // Proceedings of the 8th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS). 2011. Pp. 777–782.

8. 802.11s – Linux Wireless. // Режим доступа: http://wireless.kernel.org/en/developers/Documentation/ieee80211/802.11s – свободный — Загл. с экрана. — Яз. англ.

9. WifiMesh – FreeBSD Wiki. // Режим доступа: https://wiki.freebsd.org/WifiMesh – свободный — Загл. с экрана. — Яз. англ.

Королёв М.М.

МОДЕЛИ ТЕОРИИ ИГР В ЗАДАЧЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В УСЛОВИЯХ НЕПОЛНОТЫ ИНФОРМАЦИИ

Санкт-Петербургский государственный политехнический университет

Современное развитие информационных технологий позволяет осуществлять математическое моделирование задач, связанных с обеспечением безопасности на технических объектах и объектах стратегического значения. Расчёты, связанные с противодействием возможным нарушителям, могут быть построены на основе теории игр.

Ключевым результатом таких расчетов на практике является ответ на вопрос, каким образом следует распределить имеющиеся ресурсы для сведения рисков от внешних угроз к минимально возможным значениям. Теория игр позволяет получить такой ответ при выполнении ряда предположений о поведении возможного злоумышленника и преследуемых им целей.

В последнее время в научной литературе заметен рост публикаций, связанных с применением теории игр в задачах обеспечения безопасности (как теоретического плана, так и касающихся практического применения разработанных математических моделей). На

сегодняшний день модели теории игр используются во многих системах обеспечения безопасности на крупных объектах, например, таких как система LAX [1], применяемая в международном аэропорту Лос-Анджелеса. Используемые в них теоретико-игровые модели позволяют сориентировать поведение полиции при возможных действиях злоумышленников на основе доступной статистической информации и информации другого рода.

Важным фактором использования моделей теории игр для решения практических задач обеспечения безопасности является то обстоятельство, что для их применения необходима очень точная информация о возможностях и предпочтениях сторон игры [2]. На практике эти модели строятся с использованием экспертной информации о доступных ресурсах, которые могут быть использованы для защиты объекта от угроз, о рисках безопасности, об уязвимости возможных целей и о мотивации нападающих. При этом часто эти данные весьма неполны и сопряжены со значительной неопределенностью. К примеру, нельзя точно оценить, какой именно выигрыш получит злоумышленник при успешной атаке той или иной цели (при этом, правда, может быть ясно, какие цели являются для него более предпочтительными). Поскольку все эмпирические и субъективные данные априори неточны, эту неточность обязательно необходимо учитывать при принятии решений при обеспечении безопасности [3]. Невыполнение этого требования может привести к неконтролируемому изменению вероятности совершить ошибку при принятии решения.

Наиболее простым и широко используемым на практике способом ввести в рассмотрение неточность исходных данных является их интервальное описание. В настоящем докладе представлены теоретико-игровые модели, работающие с заданными интервалами возможных значений для исходных данных. Представлены примеры применения таких моделей для практических задач.

В работе [3] представлена модель решения задачи о распределении ресурсов в условиях интервальной формализации неопределенности о предпочтениях злоумышленника при выборе целей для атаки. Решение сводится к задаче оптимизации целевой функции специального вида, учитывающей интервальный характер исходных данных. В докладе показано, что результатов, согласующихся с результатами работы [3], можно добиться с помощью традиционных моделей теории игр (изначально игнорирующих неточность исходных данных), если применить для вычислений в их рамках интервальную арифметику. Внесения изменений в содержательную часть моделей при этом не требуется.

ЛИТЕРАТУРА

1. Pita J. et al. Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport // Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track. – International Foundation for Autonomous Agents and Multiagent Systems, 2008. – С. 125-132.
2. Kiekintveld C., Marecki J., Tambe M. Approximation methods for infinite Bayesian Stackelberg games: Modeling distributional payoff uncertainty //The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3. – International Foundation for Autonomous Agents and Multiagent Systems, 2011. – С. 1005-1012.
3. Kiekintveld C., Islam T., Kreinovich V. Security games with interval uncertainty //Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems. – International Foundation for Autonomous Agents and Multiagent Systems, 2013. – С. 231-238.

Ложкин В.Н., Ложкин Н.Н., Цветков В.А.

БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ ДЛЯ ОБНАРУЖЕНИЯ ЧРЕЗВЫЧАЙНО ОПАСНЫХ ЯВЛЕНИЙ

Санкт-Петербург
СПбГПУ, Университет государственной противопожарной службы

Безопасность различных объектов в настоящее время часто обеспечивается установкой WEB-камер на территории охраняемого или контролируемого объекта. Однако при осуществлении мониторинга протяженных объектов, таких как газопроводы, лесные массивы такой подход экономически не целесообразен или не может быть практически реализован. С другой стороны спутниковые и космические данные не всегда позволяют во время обнаруживать начальные стадии аварийной ситуации, например, утечки газопроводов, локальные очаги пожаров и другие стихийные и техногенные аварии. В таких случаях первостепенное значение приобретают передвижные станции и в первую очередь радиоуправляемые летающие лаборатории - беспилотные летательные аппараты (БПЛА).

История появления и развития БПЛА ведет начало еще с опытов Никола Тесла [1] в 1899 году по демонстрации миниатюрного

радиоуправ-ляемого судна. Исторически сложилось так, что изначальное применение БПЛА определялось как боевое. К настоящему времени США являются одним из признанных лидеров по разработке и производству БПЛА. К началу 2012 года БПЛА составили почти треть парка стоявших на вооружении летательных аппаратов (количество беспилотников в составе вооруженных сил США, достигло 7494 единиц, в то время как количество пилотируемых аппаратов — 10767 единиц) [1]. Россия сильно отстает в этом плане от ведущих стран, в 2010 году компания «Оборонпром», входящая в состав госкорпорации «Ростехнологии», подписала с ведущей израильской компанией IAI контракт, согласно которому в России будет создано совместное предприятие по сборке беспилотных летательных аппаратов[2]. Министр обороны России Сергей Шойгу заявил, что министерство обороны России потратит около 320 миллиардов рублей на программу оснащения Вооруженных сил беспилотными летательными аппаратами, выделение средств предусмотрено госпрограммой вооружений России на период до 2020 года [3]. Таким образом можно сделать вывод, что развитие БПЛА ожидает в нашей страну интенсивное развитие.

С начала 2000-х годов колоссальное значение стали приобретать «микробеспилотники», разрабатываемые не для военных, а сугубо гражданских целей[4]. Здесь следует отметить, что БПЛА принято делить по таким взаимосвязанным параметрам, как масса, время, дальность и высота полёта. Выделяют следующие классы аппаратов:

- микро— массой до 10 килограммов, временем полёта около 1 часа и высотой до 1 километра;
- мини — массой до 50 килограммов, временем полёта несколько часов и высотой до 3—5 километров;
- средние (миди) — до 1 000 килограммов, временем 10—12 часов и высотой до 9—10 километров;
- тяжёлые — с высотами полёта до 20 километров и временем полёта 24 часа и более.

Гражданская область применения БПЛА весьма обширна: от сельского хозяйства и строительства до нефтегазового сектора и сектора безопасности. «Дроны» гражданского назначения могут использоваться в работе служб по чрезвычайным ситуациям - оперативное наблюдение за распространением пожаров и стихийных бедствий, поиск потерпевших бедствие в труднодоступных местах, георазведка местности, мониторинг чрезвычайного загрязнения атмосферы и многие другие сферы применения.

С учетом перечисленного выше широкого спектра использования летательных аппаратов представляется целесообразным разрабатывать базовую модель БПЛА, подразумевая под этим возможность изменения конфигурации и состава электронной начинки, быстро меняющейся номенклатуры и комплектации датчиковой и микроконтроллерной аппаратуры обработки и передачи информации.

Кафедра измерительных информационных технологий СПбГПУ совместно с Санкт-Петербургским университетом ГПС МЧС России начала совместные поисковые работы по созданию такой базовой модели, способной решать широкий круг задач. При этом смена первичных датчиков позволяет оперативно изменять функциональные возможности БПЛА – экологические, пожарные, охранные и другие.

Новейшей совместной прикладной разработкой университета ГПС МЧС России является беспилотный радиоуправляемый аппарат для обнаружения пожаров и стихийных бедствий. Он может быть использован также для: поиска потерпевших бедствие в трудно доступных местах, ведения оперативной геологической разведки местности и мониторинга чрезвычайного загрязнения воздушной среды промышленными и транспортными объектами. Основными преимуществами разработки по отношению к известным отечественным и зарубежным аналогам являются:

- низкая стоимость изделия и дешевизна в эксплуатации (предположительная стоимость базовой модели не превысит 100 000 руб., модели с тепловизором, – 500 000 руб. Ориентировочная стоимость 30-минутного полёта составит, приблизительно, 10 руб.);
- мобильность (полный вес модели не превысит 5 кг);
- простота использования (требуется только выбор на карте места проведения оперативной разведки);
- неприхотливость к условиям выполнения взлёта и посадки аппарата (запуск «с места» и посадка, практически, «в точку» позволит запустить модель в самых сложных рельефных условиях местности). Аппарат будет оснащаться визуальными и измерительными техническими средствами наблюдения: видеокамера, тепловизор, видео передатчик; датчики дыма, концентрации веществ и физического излучения, в частности, – ионизирующего.

Полный контроль положения изделия в пространстве во время полета будут обеспечивать соответствующие аппаратно-программные средства управления: акселерометр, гироскоп, магнитный компас, GPS и (или) ГЛОНАСС, высотомер, ультразвуковой сонар, датчик воздушного потока, пульт дистанционного управления. Электронная начинка будет вписываться в уже разработанный планер, который имеет следующие тактико-технические характеристики:

- размах крыла	1,5-2,5 м;
- длина	1,5 м;
- потолок действия	до 4 км;
- скорость полета	до 150 км/ч;
- время полета	до 60 мин;
- дальность полета	до 20 км;
- угол обзора	360 град.;
- питание	аккумуляторная батарея.

Список литературы

1.Беспилотный летательный аппарат *http://ru.wikipedia.org/wiki/*
2. Беспилотники в современной войне http://www.modernarmy.ru/article/333/bespilotniki-rossii-sovremenniye-i-perspektivniye-modeli
3. Россия потратит на беспилотники 320 миллиардов рублей http://lenta.ru/news/2014/02/13/uavs
4. Гражданские беспилотники http://www.ato.ru/content/grazhdanskie-bespilotniki

Малыхина Г.Ф., Кислицына И.А.

ОСОБЕННОСТИ ИЗМЕРЕНИЯ ВЫСОТЫ НАД ЛУННОЙ ПОВЕРХНОСТЬЮ С ПОМОЩЬЮ РАЗЛИЧНЫХ ВИДОВ ИСТОЧНИКОВ РАДИОАКТИВНОГО ИЗЛУЧЕНИЯ

Санкт-Петербург, СПбГПУ

Для измерения текущей высоты спускаемого аппарата над лунной поверхностью возможно использование фотонного высотомера, в состав которого входит излучатель гамма-квантов и приемник обратно рассеянного подстилающей поверхностью излучения. Мерой высоты является регистрируемая приемником интенсивность излучения. В качестве источника излучения приемника используется радиоактивный изотоп.

Существует несколько потенциальных источников радиоактивного излучения, которые могут быть использованы в качестве излучателей для посадки спускаемого аппарата на лунную поверхность. В связи с этим первоначальной задачей при проектировании фотонного высотомера является выбор источника гамма-излучения. Источник должен удовлетворять двум условиям: интенсивность обратно

рассеянных гамма-квантов на заданной высоте должна существенно превышать естественный фон радиации, а период полураспада изотопа должен быть больше срока эксплуатации аппаратуры.

В данном случае процесс взаимодействия гамма-квантов с веществом носит характер упругого центрального рассеяния. Вероятность рассеяния фотона под углом Θ_s в телесном угле Ω определяется формулой Клейна-Нишины-Тамма [1]:

$$\frac{d\sigma_{\Theta s}}{d\Omega} = \frac{r_o^2}{2}\,[1/(1+\alpha(1-\cos\Theta s))]^2 \cdot [1+\cos^2\Theta_s + \frac{(\alpha(1-\cos\Theta_s))^2}{1+\alpha\,(1-\cos\Theta_s)}], \qquad (1)$$

где $r_0 = e^2/ m_e c^2$ - классический радиус электрона;

e, m_e- заряд и масса электрона;

c - скорость света;

$\alpha = \frac{E_0}{m_0 \cdot c^2}$;

E_o - энергия гамма-кванта;

m_o - масса электрона;

Θ_s - угол рассеяния (угол между направлениями первичного и рассеянного фотонов).

Графики зависимости сечения рассеяния от угла рассеяния для различных источников излучения: Ba^{133}, Cs^{137}, Co^{60}, U^{232}, Pu^{238} (Таблица 1) показаны на рисунке 1. Из графиков следует, что с увеличением энергии фотона угловое распределение становится все более направленным вперед.

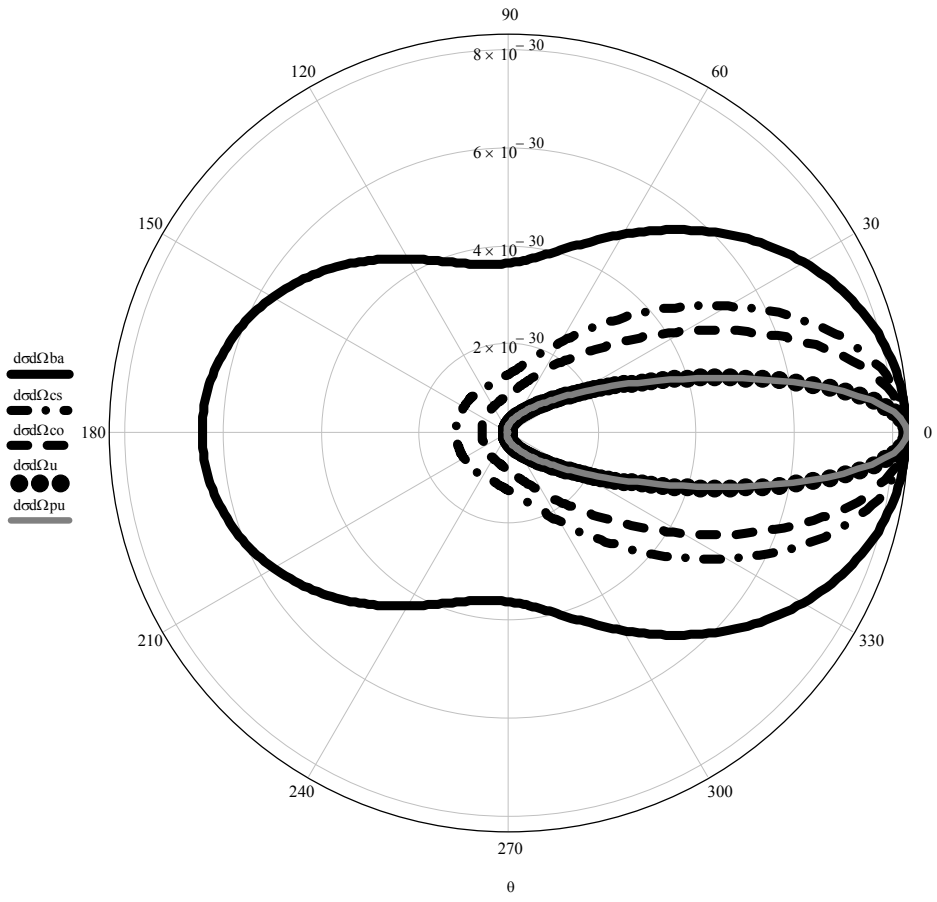


Рис. 1 - Дифференциальное сечение комптоновского рассеяния для различных источников излучения (Ba^{133}, Cs^{137}, Co^{60}, U^{232}, Pu^{238})

Таблица 1 – Источники радиоактивного излучения [2]

Изотоп	Энергия, кэВ	Период полураспада
^{133}Ba	36	10,54 лет
^{137}Cs	661	30 лет
^{60}Co	$1{,}25 \cdot 10^3$	5 лет
^{232}U	$5{,}4 \cdot 10^3$	69 лет
^{238}Pu	$5{,}59 \cdot 10^3$	87 лет

Наибольшей вероятностью обратного рассеяния обладают изотопы ^{133}Ba и ^{137}Cs. Для изотопов U^{232}, Pu^{238} обратное рассеяние отсутствует.

Интенсивность рассеянных гамма-квантов рассчитывается по формуле:

$$I = I_0 \cdot \frac{3 \cdot \sigma_0}{16 \cdot \pi \cdot R^2} \cdot \frac{(1+cos^2\theta)}{[1+\alpha(1-cos\theta)]^3} \cdot \left[1 + \frac{\alpha^2 \cdot (1-cos^2\theta)}{[1+\alpha(1-cos\theta)] \cdot (1-cos\theta)}\right], \quad (2)$$

где I_0 – интенсивность излучения источника;

R – расстояние от точки рассеивания до детектора;

θ – угол рассеяния;

$\sigma_0 = 6{,}65 \cdot 10^{-25} \cdot n_e \cdot Z_{\text{эфф}}$;

$\alpha = \frac{E_0}{m_0 \cdot c^2}$;

n_e – концентрация электронов;

$Z_{\text{эфф}}$ – эффективный атомный номер вещества поверхности (грунта).

Уменьшение интенсивности излучения при прохождении через слой поглотителя описывается уравнением [3]:

$$I = e^{-\mu\rho\Delta h} \cdot I_0 \quad (3)$$

где μ – массовый коэффициент поглощения;

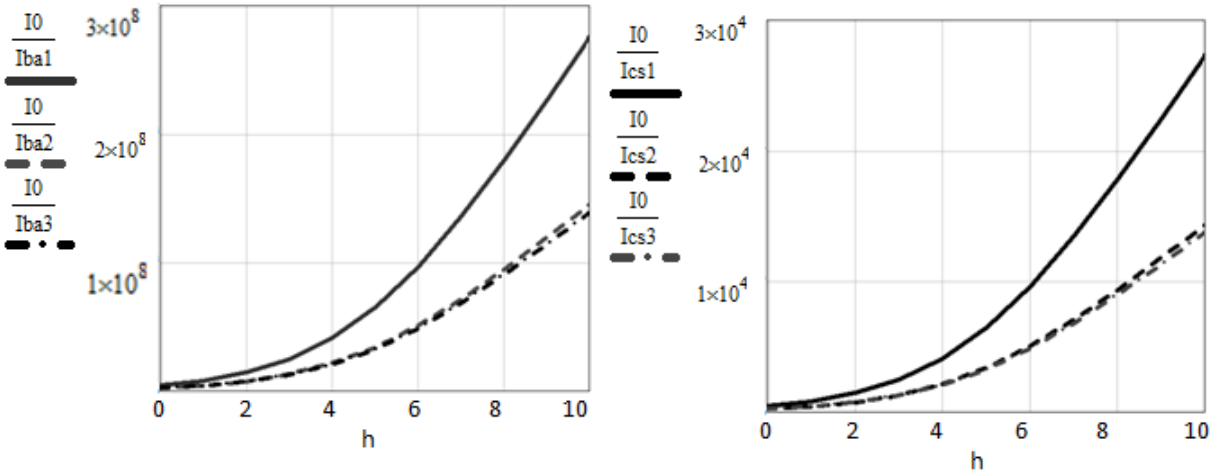
ρ – плотность вещества;

Δh - слой поглотителя.

С учетом поглощения излучения при прохождении через слой реголита и слой грунта выражение для расчета интенсивности рассеяния имеет вид:

$$I = e^{-2\mu\rho h} \cdot I(h) + e^{-2\mu_1\rho_{\text{реголита}}\Delta h_{\text{реголита}}} \cdot I\left(\Delta h_{\text{реголита}}\right) + e^{-2\mu_2\rho_{\text{грунта}}\Delta h_{\text{грунта}}} \cdot I\left(\Delta h_{\text{грунта}}\right) \quad (4)$$

По формуле (4) получены графики зависимости ослабления интенсивности рассеянных гамма-квантов по сравнению с первичной интенсивностью источника от высоты над подстилающей поверхностью:



а) б)

Рис. 2 - Зависимость ослабления интенсивности обратно рассеянных гамма-квантов от высоты для разных типов грунтов (1 – альбит, 2 - оливин, 3 – ильменит): а) - изотоп ^{133}Ba, б) - изотоп ^{137}Cs

Из графиков видно, что интенсивность рассеянного излученния ослабевает с уменьшением первичной энергии фотонов (в 10^4 для ^{137}Cs равна, в 10^8 для ^{133}Ba).

В связи с тем, что ослабление интенсивности обратного рассения ^{137}Cs меньше, чем интенсивность обратного рассения ^{133}Ba и период полураспада ^{137}Cs ($T_{½}$ = 30 лет) больше периода полураспада ^{133}Ba ($T_{½}$ = 10,54 лет), то из рассмотренных источников радиоактивного излучения наилучшими характеристиками для определения высоты над лунной поверхностью обладает изотоп ^{137}Cs.

Список литературы:

1. Кузьмичев В.Е. Законы и формулы физики/Отв. ред. В.К. Тартаковский. – Киев: «Наук. думка» 1989. – 864 с.

2. О.Ф. Немец, Ю.В. Гофман Справочник по ядерной физике – Киев: «Наукова думка» 1975

3. Ю.М. Широков, Н.П. Юдин Ядерная физика – М: «Наука», 1980 – 728 стр.

4. В.П. Легостаев, В.А.Лопота «Луна - шаг к технологиям освоения Солнечной системы» – М:РКК «Энергия», 2011- стр. 584

Малыхина Г.Ф., Милицын А.В., Гусева А.С.

РАСПОЗНАВАНИЕ ОБЪЕКТОВ НА ПОДСТИЛАЮЩЕЙ ПОВЕРХНОСТИ ПРИ КОМПЛЕКСНОЙ ЗАЩИТЕ ОБЪЕКТОВ

ФГБОУ ВПО Санкт-Петербургский государственный политехнический университет

Автоматическое распознавание на кадрах аэрофотосъемки объектов, представляющих интерес для исследователя, является актуальной задачей, решение которой позволяет уменьшить объем информации при передаче и хранении и увеличить оперативность работы системы. В работе приведен сценарий обработки кадров аэрофотосъемки, включающий бинаризацию кадров изображений, определение положения объектов, представляющих интерес, положение дорог и привязку к местности на основе максимума взаимной корреляционной функции бинарных изображений.

Видеопоследовательности получены разными регистраторами в разных условиях по освещенности, поэтому изображения могут быть как цветными, так и в градациях серого. Одни и те же объекты на разных изображениях могут иметь разный цвет и интенсивность. Особенностью задачи является отсутствие библиотеки образов, представляющих интерес для поиска, известен только диапазон размеров и прямоугольная форма объектов.

Бинаризация изображений. Для поиска расположения объектов необходимо преобразовать изображение к бинарному виду с удалением всех несущественных деталей. В зависимости от класса изображений применены два метода бинаризации: пороговая обработка изображений в градациях серого цвета, и определение контуров объектов с последующим заполнением замкнутых контуров. Бинаризация является критическим этапом обработки, от решения которого зависит результат поиска. Разработана библиотека функций бинаризации, которая реализует следующие методы:

- гистограммные, анализирующие минимумы сглаженных гистограмм;
- кластерные, основанные на разделении областей на два класса, относящихся к переднему плану и к фону;
- энтропийные, вычисляющие взаимную энтропию исходного и бинарного изображения, включающего области переднего плана и фона;
- основанные на атрибутах объектов, форме, границах объектов и нечетких мерах подобия исходного и бинарного изображения;

- пространственные методы, учитывающие корреляцию между пикселями изображения;

- локальные методы, использующие скользящее окно и адаптивный порог.

Бинарная пороговая обработка выполняется по следующим формулам:

Åñëè $I(i,j) < \theta(i,j)$ $I_\theta(i,j) = 0;$

Åñëè $I(i,j) \geq \theta(i,j)$ $I_\theta(i,j) = 1;$

где $\theta(i,j)$- порог, $I(i,j)$ пиксель исходного изображения, который преобразуется в пиксель результирующего бинарного изображения $I_\theta(i,j)$.

Метод Рамеша. Для вычисления порога применен метод Рамеша, основанный на оценке функции распределения вероятностей (ФРВ) интенсивностей пикселей изображения $P(g) = \sum_{i=0}^{g} p(i)$. Характеристикой фона является плотность распределения вероятностей (ПРВ) интенсивностей пикселей $p_b(g),\ 0 \leq g \leq \theta,$ характеристикой объекта – ПРВ $p_f(g), \theta + 1 \leq g \leq G,$ θ – величина порога. Вероятности фона и объекта определяется с использованием гистограммы изображения по формулам:

$$P_b(\theta) = P_b = \sum_{g=0}^{\theta} p(g)$$

$$P_f(\theta) = P_f = \sum_{g=\theta+1}^{G} p(g)$$

где G - максимальное значение интенсивности. При переходе к бинарному виду ФРВ $P(g)$ аппроксимирована функцией с двумя градациями $b_1(\theta)$ и $b_2(\theta)$. Аппроксимация получается таким образом, что сумма квадратов отклонений аппроксимирующей функции от исходной функции минимальна. При использовании функции с двумя градациями пороговое значение определяется по следующим формулам:

$$\theta_{opt} = \min\left[\sum_{g=0}^{\theta} (b_1(\theta) - g)^2 + \sum_{g=\theta+1}^{G} (b_2(\theta) - g)^2 \right] \quad (1)$$

$$\begin{cases} b_1(\theta) = \dfrac{\sum\limits_{g=0}^{\theta} gp(g)}{\sum\limits_{g=0}^{\theta} p(g)}, & 0 \le g \le \theta \\ b_2(\theta) = \dfrac{\sum\limits_{g=\theta+1}^{G} g\,p(g)}{\sum\limits_{g=\theta+1}^{G} p(g)}, & \theta+1 \le g \le G \end{cases} \qquad (2)$$

Решение θ_{opt} может быть получено методом итерационного поиска по формулам (1,2). Применение метода Рамеша позволило выделить на исходном изображении небольшие объекты, расположенные на значительном удалении.

Бинаризация с использованием контуров объектов основана на методе Кенни, позволяющем выделить контуры объектов и заполнить замкнутые контуры объектов.

Морфологическая фильтрация бинарных изображений. Поскольку интересующие нас объекты не обладают высокой контрастностью, то вместе с ними программа выделяет некоторые объекты фона, которые должны быть удалены полностью или их влияние должно быть максимально уменьшено. Для этих целей предложено использовать эрозию бинарных изображений. В процессе эрозии происходит удаление пикселей с границ объектов.

Эрозия множества пикселей объекта A по множеству пикселей структурирующего элемента B:

$$A \oplus B = \{z / (B)_z \subseteq A\}$$

где $(B)_z$ - центральное отображение и сдвиг структурирующего элемента. Результат эрозии – это множество всех точек z, при сдвиге в которые множество B целиком содержится в A.

Для восстановления интересующих нас объектов после эрозии применяем дилатацию объекта A по множеству пикселей структурирующего элемента B определяется по формуле:

$$A \oplus B = \left\{z / \left[\left(\hat{B}\right)_z \cap A\right] \subseteq A\right\}$$

где $\hat{B}$ - центральное отражение множества B. Положительный эффект эрозии состоит в уменьшении влияния шумов, что приводит также к уменьшению ширины и прерывистости полезных объектов. Поэтому после эрозии целесообразно восстановить непрерывность линий объектов.

Фильтрация обнаруженных объектов по размеру основана на поиске прямоугольных объектов заданной длины и соотношения сторон. Размер объектов в пикселях $d_{\min},...d_{\max}$ зависит от размера N изображения в пикселях, текущей высоты полета h, угла обзора видеокамеры α и заданного диапазона длин $l_{\min}...l_{\max}$ объектов, представляющих интерес:

$$d_{\min} = \frac{N}{2h\,\mathrm{tg}\,\alpha} l_{\min}; \qquad d_{\max} = \frac{N}{2h\,\mathrm{tg}\,\alpha} l_{\max};$$

Для того чтобы исключить обнаружение дорог как объектов, было введено ограничение на соотношение длины d и ширины w прямоугольных объектов:

$$\left(d/w\right)_{\min} ... \left(d/w\right)_{\max}$$

Фильтрация обнаруженных объектов по форме использует цепной код, который кодирует границу объекта в виде последовательности отрезков прямых линий определённой длины и направления. Последовательность направлений отрезков кодируют последовательностью чисел, для которых вычисляется первая конечная разность. Минимальное значение числа, представляющего конечную разность, является инвариантным к начальной точке вычисления кода, к повороту объекта относительно изображения и к масштабу объекта благодаря изменению длин отрезков.

Фильтрация обнаруженных объектов по цвету и текстуре. Алгоритм позволяет выделять не только объекты, представляющие интерес (дома, автомобили), но и другие объекты (облака, дым, деревья, блики на водной поверхности). Разделение рукотворных объектов и объектов, не представляющих интерес при распознавании, основано на анализе цвета и текстуры объектов. Цветовая компонента найденных объектов получается путем преобразования RGB – объекта в HSV – объект и выделения H - компоненты. Изучение текстуры H-компоненты выделенного объекта позволяет различать блики на воде и полезные объекты, облака и особенности поверхности.

Выделение дорог на основе преобразования Радона. Дороги представляют собой прямолинейные участки. Прямолинейные участки, выделенные на бинарном изображении после морфологической фильтрации, представляются облаками точек. Для определения положения дороги как облака точек, целесообразно найти проекции изображения под разными углами. Проекция на ось, перпендикулярную линии дороги, достигает максимального значения. Для вычисления проекций используется преобразование Радона:

$$R_\theta(x') = \int_{-\infty}^{\infty} I_\theta\left(x'\cos(\Theta) - y'\sin(\Theta), x'\sin(\Theta) + y'\cos(\Theta)\right)\cdot dy'$$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} \cos(\Theta) & \sin(\Theta) \\ -\sin(\Theta) & \cos(\Theta) \end{bmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

где $I_\theta(x,y)$ - бинарное изображение, x, y - его координаты, Θ - угол проецирования, x', y' - координаты, повернутые на угол Θ. Результат преобразования Радона представлен в полярных координатах $\{\rho,\Theta\}$, где ρ - расстояние до центра изображения, Θ - угол.

Прямая линия, проходящая через центр изображения, имеет начальное и конечное значение со следующими координатами:

$$x: \left(\frac{M}{2} + \frac{N}{2}tg(\alpha) - \frac{\rho}{\cos(\alpha)}\right) \ldots \left(\frac{M}{2} - \frac{N}{2}tg(\alpha) + \frac{\rho}{\cos(\alpha)}\right) \quad y: \left(-\frac{N}{2}\right) \ldots \left(\frac{N}{2}\right)$$

Экстремально-корреляционная навигация основана на вычислении взаимной корреляционной функции изображений. Однако такие вычислительные процедуры выполняются довольно медленно. Чтобы сделать вычисления более быстрыми, используются бинарные изображения. Взаимная корреляция между бинарным изображением карты местности и подстилающей поверхности с нанесенными дорогами основано на логических операциях умножения единиц и нулей по формуле:

$$I_\theta(x,y) \circ H_\theta(x,y) = \frac{1}{MN} \cdot \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I_\theta(m,n) H_\theta(x+m, y+n)$$

где $I_\theta(x,y)$, $H_\theta(x,y)$ - бинарные изображения наблюдаемой поверхности и бинарное изображение карты.

Заключение. Предложенные методы обработки изображений подстилающей поверхности, позволяющие определять наличие объектов, без предварительного предъявления их образов, и определять координаты полученных объектов.

Литература

1. Ramesh, J.H. Yoo, I.K. Sethi, Thresholding Based on Histogram Approximation, IEEProc. Vis. Image, Signal Proc., 142(5) (1995) 271-279.

Михайлова А.Ю., Борисов А.П.

ИСПОЛЬЗОВАНИЕ СТАНДАРТА GSM ПРИ ОБУЧЕНИИ СТУДЕНТОВ БАКАЛАВРИАТА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

г. Барнаул, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Алтайский государственный технический университет им И.И. Ползунова»

Сегодня информация настолько ценна, что стоит намного дороже других ресурсов. Злоумышленники с каждым днем становятся все изобретательнее и выискивают новые способы осуществления незаконного доступа к ней. Поэтому каждый специалист по защите информации должен уметь грамотно организовать ее защиту. Важным аспектом обеспечения информационной безопасности является недопущение утечки информации по акустическому и виброакустическому каналу, в частности, обеспечение безопасности телефонных и иных переговоров.

Благодаря стремительному развитию GSM технологий [1] злоумышленники могут использовать большое количество разнообразных подслушивающих устройств, работающих в ее частотном диапазоне. Поэтому необходимость обеспечения защиты информации от перехвата по каналам GSM как никогда актуальна.

На сегодняшний день рынок предлагает большое количество приборов, разработанных для защиты информации от утечки по каналам GSM. Такие приборы можно разделить на два вида: устройства, которые блокируют передачу данных по каналу связи (подавители сигналов, генераторы шумов) и устройства, позволяющие передавать информацию в зашифрованном виде (скремблеры, криптофоны и цифровые шифраторы).

Глушение GSM сигнала применяется в организациях для глушения прослушивающих устройств и жучков. Все устройства для глушения сигнала основаны на том, что они генерируют белый шум на той же частоте, что и прибор, работу которого необходимо остановить. Эффективность таких устройств огромная: сигнал не может выйти за пределы контролируемой зоны. Однако такие устройства полностью блокируют связь на радиусе своего действия.

Более универсальным способом защиты информации от утечки и использования третьими лицами является ее шифрование. Есть два типа устройств, предназначенных для полного шифрования трафика:

аналоговые скремблеры и цифровые шифраторы. Использование подобных устройств позволяет защитить переговоры от прослушивания на любом участке передачи (кроме непосредственного прослушивания микрофонами).

Скремблеры [2-3] выполняют шифрование разбиением спектра звукового сигнала на части и дальнейшей частотной инверсией каждой из этих частей. Скремблер присоединяется прямо к телефону и принимает сигналы, идущие с микрофона, шифрует их и только после этого отсылает на выход. Декодирование речи происходит в обратном порядке. Для того чтобы собеседник мог слышать Вас, у него должен быть скремблер с тем же алгоритмом скремблирования, что и на передающей стороне. Таким образом, ведущие между собой переговоры люди понимают друг друга, в отличие от тех, кто подключился к их разговору.

Основным достоинством скремблеров является высокая надежность защиты. Кроме того, скремблеры позволяют защититься от любого способа прослушивания сотовых телефонов, в том числе и от специального оборудования, установленного у оператора. Основным недостатком скремблеров является необходимость обоим абонентам иметь совместимые устройства для проведения приватной беседы.

Относительно недавно на рынке появились качественно новые устройства шифрования – *криптофоны*. Это обычные смартфоны с дополнительным программным обеспечением. В принципе, принцип работы криптофона аналогичен принципу работы скремблеров: сигналы с микрофона оцифровываются, кодируются и отправляются в сеть сотовой связи в зашифрованном виде. Вся разница заключается в способе реализации. Главным преимуществом криптофонов является использование более длинного ключа, что обеспечивает исключительную защиту, но цена таких приборов высока.

Для реализации методов передачи информации по GSM-технологии предполагается использовать Arduino с модулем GSM, на котором возможно организовать скремблирование и передачу сигнала, а также создать прибор для глушения GSM частоты методом белого шума, что позволит будущим специалистам по защите информации более детально рассмотреть способы передачи и защиты по GSM-каналу.

Список литературы:

1. Попов В.И. Основы сотовой связи стандарта GSM: Учебное пособие. [Текст] М.: «Эко-Трэндз», 2005г.

2. Скремблер – Описание GSM и ее взлом [Электронный ресурс]. Режим доступа: http://www.skrembler.ru/st10.html

3. Телекоммуникационные технологии. Введение в технологии GSM. С. Б. Макаров, Н. В. Певцов, Е. А. Попов, М. А. Сиверс. [Текст] М.: Академия, 2008 г.

Моногаров К.Е.

ОПРЕДЕЛЕНИЕ ОРИЕНТАЦИИ ОБЪЕКТОВ НА ОСНОВЕ ДАННЫХ ЛИДАРНОЙ ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ

Санкт-Петербург, ФГБОУ ВПО СПбГПУ

В настоящее время различные робототехнические системы начали активно входить во многие сферы жизни человека. Всевозможные роботы начинают активно применяться в быту, промышленности, военном деле и даже при полетах в космос. Часто для подобных систем встает задача определения ориентации относительно каких-либо объектов и планирование траектории при сближении с ними. В данной работе предлагается алгоритм для определения ориентации робототехнической системы относительно заданного объекта на основе трехмерных данных, полученных посредством измерения лидарными измерительными системами (ЛИС), так же известными, как лидары [1, с. 52].

Сканирование поверхности объекта осуществляется следующим образом: лидар посылает лучи лазерного света в пространство, которые, встретившись с какой-либо поверхностью, отражаются от нее и возвращаются назад в прибор на светочувствительный приемник. Таким образом, зная скорость света, можно определить расстояние до точки на объекте, от которой отразился посланный луч, по следующей формуле:

$$d = \frac{ct}{2}, \qquad (1)$$

где c - скорость света,
t - время, между моментами отправки и приема луча.

Каждое измерение лидаром представляет собой точку, которая характеризуется тремя параметрами - двумя углами в поле зрения лидара и расстоянием до нее. Таким образом, положение каждой точки, заданной двумя углами и расстоянием, после измерения может быть представлено в сферической системе координат (Рис. 1):

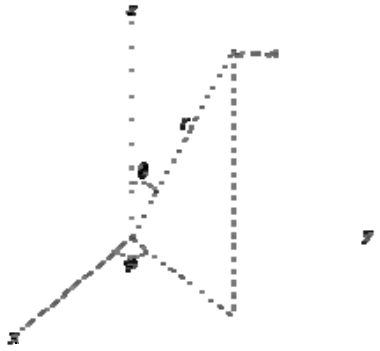


Рис. 1

Для дальнейшего удобства обработки точки, она переводится в Декартову систему координат с использованием следующих выражений:

$$\begin{cases} x = r\sin\theta\cos\varphi \\ y = r\sin\theta\sin\varphi \\ z = r\cos\theta \end{cases} \quad (2)$$

Просканировав таким образом поверхность объекта, можно получить его трехмерное изображение, которое будет представлено в виде набора точек, часто именуемого облаком точек.

В данном случае задача определения ориентации объекта сводится к задаче регистрации [2, с. 69] облаков точек, полученных путем измерений объекта лидарной измерительной системой.

Под регистрацией облаков точек понимается их последовательное выравнивание друг относительно друга. Необходимым условием регистрации является то, что облака точек должны иметь в своем составе одинаковую перекрывающуюся часть, по которой и осуществляется регистрация. Результатом регистрации двух облаков точек являются матрица поворота R и вектор перемещения t, которые должны быть применены к одному из наборов данных, чтобы тот был выровнен относительно другого [3].

Итак, для определения ориентации объекта требуется набор снимков модели объекта, по которым будет определяться ориентация. Ключевая идея метода заключается в том, что имея такой набор снимков модели и получая очередной снимок объекта с ЛИС, мы осуществляем регистрации этого полученного снимка поочередно с набором снимков модели и выбираем из них, посредством метода регистрации, наиболее "близкий". Каждый снимок модели должен быть сделан из строго определенного положения. Таким образом, определив самый похожий снимок модели на снимок, полученный с ЛИС мы можем сделать выводы о положении объекта с ЛИС относительно объекта, ориентация которого определяется, имея в результате наборы углов поворота ориентируемого объекта и расстояние до него. Следовательно,

появляется возможность корректировки траектории движения объекта с ЛИС.

Литература

[1] Теоретические основы оптико-электронных приборов / М. Мирошников – Ленинград.: Машиностроение, 1977. – 600 с.
[2] Semantic 3D Object Maps for Everyday Manipulation in Human Living Environments / Radu Bogdan Rusu – Munchen, 2009. – 260 с.
[3] Robust Global Registration / N. Gelfandn, N. Mitra, J. Guibas, H. Pottmann, In Proceedings of the Symphosium of Geometric Processing, 2005

Яковенко А.А., Малыхина Г.Ф.

ТЕКСТОНЕЗАВИСИМОЕ РАСПОЗНАВАНИЕ ЛИЧНОСТИ ПО ГОЛОСУ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ ФУНКЦИЙ РАДИАЛЬНОГО БАЗИСА

Санкт-Петербург, СПбГПУ, кафедра «Измерительные информационные технологии»

Интенсивное развитие систем голосового распознавания личности обусловлено возможностью их применения в различных сферах современной жизни. В последние годы наблюдается повышенный интерес к применению голосовой биометрии [4, 5]. Это объясняется востребованностью в областях организации разграничения прав доступа к информации с помощью голосовой биометрии, решения задач биометрического поиска и криминалистического учёта, внедрения таких систем в инновационных технологических решениях, например при организации голосовой верификации водителя и пассажиров, в управлении элементами умного дома, применение голосовой биометрии банковскими системами, контакт-центрами и т.д. Идентификация диктора по голосу предоставляет уникальные возможности для защиты доступа к информации, удалённого обслуживания и экспертизы по установлению личности.

Задача идентификации и верификации личности по голосу включает в себя целый комплекс родственных задач, объединяемых термином распознавание диктора [3], целью которых в общем смысле является определение различий между людьми по данному параметру. Системы идентификации и верификации дикторов делятся по постановке задачи и методам работы на текстозависимые и текстонезависимые, а также могут

работать на основе открытого или закрытого множества дикторов [4]. В случае закрытого множества дикторов, тестируемая фонограмма будет заведомо принадлежать конкретной идентифицируемой личности, если же фонограмма не принадлежит ни одному из кандидатов, то говорят, что задача решается на открытом множестве дикторов. Если система идентификации предполагает для успешного взаимодействия распознавание определённой парольной фразы, произнесённой диктором, которой она будет заранее обучена, то речь идёт о текстозависимой системе идентификации. Моделирование информации о словарном и фонемном составе фразы в таком случае требует меньший объем обучающих речевых данных, при увеличении эффективности распознавания [4], но необходимость произнесения парольной фразы при тренировке и в процессе эксплуатации системы ограничивает практическую область её применения. Система распознавания на основе текстонезависимого подхода, не содержит информации о произносимой фразе и обучается, а затем тестируется, на произвольных голосовых и речевых данных. В следствии, эффективность распознавания систем идентификации такого рода сравнительно ниже, по отношению к текстозависимым, но голосовая идентификация в таком случае ничем не ограничена и имеет широкие возможности применения, поскольку знание об использовании речи в процессе идентификации для диктора не является обязательным.

Голосовая идентификации это задача принятия решения кому из множества кандидатов наиболее вероятно принадлежит тестируемая фонограмма, т.е. поскольку человеческая речь рассматривается как акустический сигнал, происходит анализ этого сигнала при помощи методов цифровой обработки. Построение системы идентификации, происходит в три этапа [3]: на первом выделяются первичные признаки, затем происходит моделирование дикторов и на третьем этапе осуществляется принятие решений. Таким образом, в общем случае, стандартные системы распознавания диктора по голосу содержат блок выделения первичных признак-векторов речевого сигнала и блок построения модели голоса диктора, которые разделяются в зависимости от обрабатываемой в них информации и решаемых задач.

Текстонезависимое распознавание диктора основано на выделении речи из фонограмм и последующем попарном сравнении её биометрических признаков, т.е. содержащихся в голосе идентификационно значимых, индивидуальных признаков личности. Поскольку на реальных записях, сделанных в обычных условиях, часто присутствует множество посторонних сигналов, различного рода шумов, импульсных и мультитональных помех, и перегруженных участков речи, предварительная обработка непригодных для анализа участков

фонограммы позволяет повысить эффективность дальнейшей обработки. Выделение речевых сегментов можно организовать за счёт использования специальных алгоритмов предварительной обработки всего сигнала, что в дальнейшем благоприятно скажется в процессе анализа и выделения речевых признаков [2]. Таким образом, работа системы автоматического текстонезависимого распознавания личности по голосовым признакам происходит в несколько этапов:

1. Выделение на фонограмме речевых сегментов
2. Извлечение на речевых сегментах уникальных речевых признаков
3. Моделирование диктора
4. Сравнение построенных моделей диктора. Т.е. сопоставление диктора-кандидата с эталонной фонограммой, в результате чего определяется, принадлежат ли записи речи одному человеку или разным людям.

Речь существенно отличается от всех акустических сигналов, поскольку она произносится и воспринимается человеком и служит для обмена информацией между людьми, поэтому, при анализе речевого сигнала, необходимо осуществлять его цифровую обработку, целью которой является извлечение первичных речевых информационных признаков на речевых сегментах, уникальных для данного диктора.

Современные системы голосового распознавания личности основываются на моделях идентификации диктора [5]. Для решения задачи такого распознавания, существуют соответствующие способы [3] построения голосовой модели диктора. Выбор модели зависит от различных параметров: от типа используемой речи, желаемой степени эффективности системы идентификации, простоты обучения и распознавания, объёмов используемой памяти и скорости вычислений.

Процесс выделения признаков по своей сути не является специфическим для задач идентификации диктора и скорее является общим для большинства направлений речевых технологий. Для анализа речевого сигнала в работе предполагается использовать спектральный анализ на основе гребёнки фильтров, коэффициенты линейного предсказания и кепстральные коэффициенты на их базе, как наиболее исчерпывающие характеристики. Несмотря на некоторые недостатки [5], определение модели диктора предлагается организовать на основе использования нейронной сети функций радиального базиса, что при определённых условиях позволит осуществлять наиболее качественный процесс распознавания. В этом случае выделенные уникальные признаки будут представлять собой облака точек (Рис.1), разделение которых будет осуществляться посредством RBF-сети. Графики сравнения расстояния между уникальными точками облаков данных эталонной модели диктора и диктора-кандидата представлены на рисунке 2. В случае не удачного

сопоставления фонограмм, диаграммы примут такой вид, который продемонстрирован на рисунке 3.1, а в случае успешной идентификации диаграммы будут сопоставимы с минимальными погрешностями (Рис. 3.2).

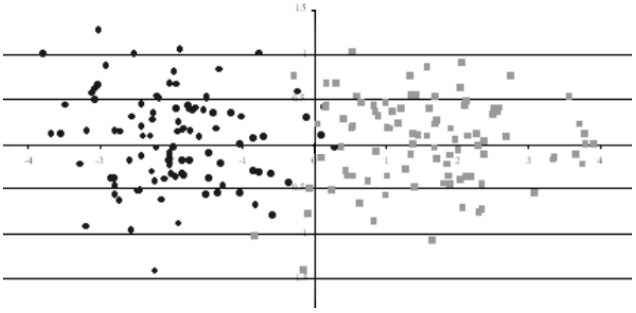


Рис. 1. Исходное распределение уникальных речевых признаков дикторов в виде облаков данных

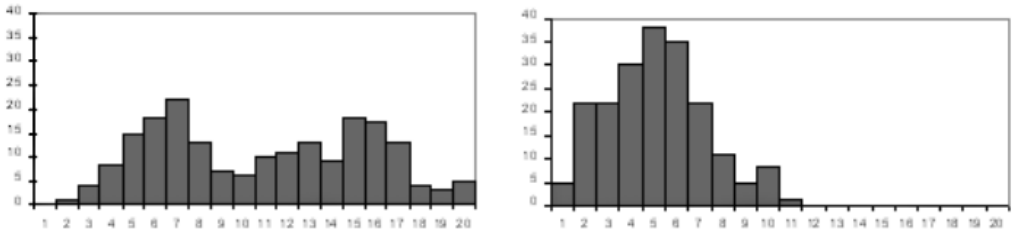


Рис. 2. Диаграммы распределения расстояний между точками облаков данных сравниваемых речевых сегментов

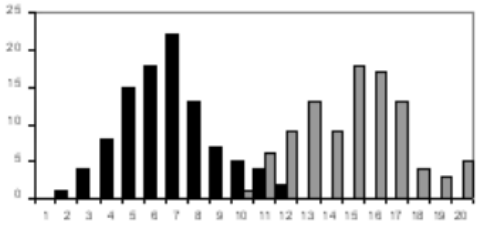


Рис. 3.1. Диаграмма сравнения построенных моделей диктора-кандидата с эталонной фонограммой

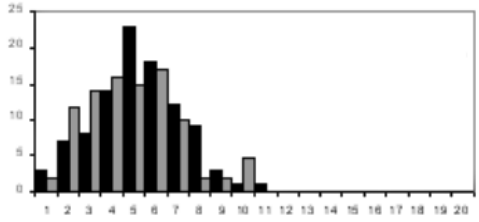


Рис. 3.2. Диаграмма сравнения модели диктора-кандидата с эталонной фонограммой в случае успешной идентификации

ЛИТЕРАТУРА:

1. Васильев А.Н., Тархов Д.А. Нейросетевое моделирование: Принципы. Алгоритмы. Приложения : Научное издание / СПбГПУ. СПб: Изд-во СПбГПУ, 2009, 527 с.

2. Котов В.В. Автоматическая текстонезависимая идентификация диктора на основе телефонного разговора. XXXIX Неделя науки СПбГПУ: материалы международной научно-практической конференции. Ч. VIII. – СПб.: Изд-во Политехн. ун-та, 2010, С. 122-124
3. Малыхина Г.Ф. Инженерно-техническая защита информации: Речевые технологии: Учеб. пособие / СПбГПУ. СПб: Изд-во СПбГПУ, 2004, 243 с.
4. Первушин Е.А. Обзор основных методов распознавания дикторов // Математические структуры и моделирование. – Омск, 2011, N Вып. 24. – С. 41-54
5. Сорокин В.Н., Вьюгин В.В., Танькин А.А. Информационные технологии в технических и социально-экономических системах. Распознавание личности по голосу: аналитический обзор // Информационные процессы. – Москва, 2012, Том 12, N 1. – С. 1-30

СЕКЦИЯ 3
ИЗМЕРИТЕЛЬНЫЕ ТЕХНОЛОГИИ

Алексеев В.А., Усольцев В.П., Юран С.И.

ФОРМИРОВАНИЕ БАЗЫ ДАННЫХ КРИВЫХ ИЗМЕНЕНИЯ ОПТИЧЕСКОЙ ПЛОТНОСТИ НЕОДНОРОДНЫХ ЖИДКИХ СРЕД

Ижевск, ФГБОУ ВПО «Ижевский государственный технический университет имени М.Т. Калашникова»

Построение аппаратуры контроля изменения оптической плотности водных сред, необходимой для автоматического обнаружения аварийных выбросов в водную среду [1–3], требует создания эталонов изменения оптической плотности сред, предназначенных для настройки данной аппаратуры.

Методика формирования базы данных кривых изменения оптической плотности жидких сред рассматривалась как конкретное воплощение способа взаимодействия полученных результатов тестирования и формы их представления в виде конкретной процедуры. Для этого в базе данных отдельно выделены массивы для лабораторного тестирования, тестирования в реальных условиях, условий технологии, аппаратуры тестирования и структурированных связей информационных массивов.

Выделены основные требования при создании базы данных:

– разрешение неоднородности программной среды (использование для решения конкретных задач различных программ и программного обеспечения);

– обеспечение распределенного характера организации информационных ресурсов;

– повышенная безопасность хранения и использования данных;

– наличие многоуровневых режимов управления и справочников;

– эффективность хранения и обработки очень больших объемов информации.

На основе анализа возможных основ и путей реализации с учетом потребностей и возможностей пользователей выбраны средства управления базой данных с использованием программных продуктов фирмы Microsoft.

При разработке структуры базы данных использована методика обеспечения быстрого доступа к объектам по заданным требованиям. Для этого предложена иерархическая структура [4], основанная на

разбиении диапазона изменения оптической плотности жидких сред и рабочих режимов при всех возможных разновидностях примесей и концентрациях растворов всех уровней.

Изменение оптической плотности неоднородных жидких сред в базе данных с учетом полной структуры связей информационных массивов в виде иерархической модели представлено в следующем виде [5].

Первый уровень охватывает все жидкие среды. *Второй* уровень охватывает воду и водные растворы. *Третий* уровень, полученный путем разделения второго уровня, содержит шесть основных видов: три вида воды – 0.1 Дистиллированная вода, 0.2 Водопроводная вода, 0.3 Вода из природных источников; и три вида растворов – 1.1 Механическое загрязнение, 1.2 Химическое загрязнение, 1.3 Биологическое и бактериологическое загрязнение.

Последующие уровни получаются путем деления предыдущего уровня на соответствующее количество частей согласно уровню детализации, а именно:

1.1 Механические примеси – 1.1.1 Песок, 1.1.2 Рудные включения, 1.1.3 Глинистые включения, 1.1.4 Растворы минеральных солей, 1.1.5 Растворы щелочей, 1.1.6 Растворы кислот.

1.2 Химические примеси – 1.2.1 Неорганические примеси, 1.2.2 Органические примеси.

1.3 Биологические и бактериологические примеси – 1.3.1 Патогенные микроорганизмы, 1.3.2 Грибы, 1.3.3 Мелкие водоросли.

Пятый уровень получается путем деления предыдущего уровня на соответствующее количество частей. 1.2.2 Органические примеси: 1.2.2.1 Фенолы, 1.2.2.2 Альдегиды, 1.2.2.3 Смолы, 1.2.2.4 Аммиак, 1.2.2.5 Нефтепродукты. Аналогично можно детализировать другие уровни.

При формировании базы данных кривых изменения оптической плотности жидких сред для каждого диапазона был протестирован наиболее характерный, типичный и распространенный вид кривой, на который было составлено стандартизированное описание кривой изменения оптической плотности, проведено индексирование и унификация записи (введены классификационные индексы, предметные рубрики, ключевые слова, дескрипторы), составлена аннотация, сформирован блок дополнительной (уточняющей) информации (концентрация водных растворов, температурный режим, виды и режимы работы измерительной аппаратуры и т.д.).

Полученные данные введены в базу, составлена пояснительная запись (вид, метод, условия измерений, погрешность, достоверность, воспроизводимость результатов, чувствительность, номинальное значение, диапазон изменения контролируемых величин, измерительная аппаратура, уровень автоматизации измерений и т.д.) на

машиночитаемом носителе (ввод данных, заполнение полей экранной формы в избранном формате), установлены контроль и редактирование записи (проверка правильности введенной информации).

В итоге проделанной работы разработана методика, с использованием которой создана универсальная база данных. Применение сформированной базы данных для обработки результатов экспериментов показало полную ее пригодность и работоспособность при контроле изменений оптической плотности неоднородных жидких сред в решении поставленных задач по выбору режимов и отработке технологии контроля данных сред. Аппаратная часть и программное обеспечение согласованы по протоколам обмена данными и полностью адаптированы между собой.

Уровень сформированной базы данных полон и достаточен для учета начальных условий, индивидуальных особенностей, погрешностей и помех при контроле жидких сред и смесей, записи и хранения кривых изменения оптической плотности тестируемых жидких сред.

База данных позволяет задать условия для обнаружения наличия неоднородностей и, при необходимости, может служить основой для установления предельно допустимых сбросов при контроле аварийных выбросы промышленных предприятий в сточные воды. Для повышения информативности, применяемости и универсальности необходима дальнейшая доработка аппаратной части, совершенствование программного обеспечения, формирование дополнительных информационных массивов.

Список литературы

1. Алексеев В.А., Козаченко Е.М., Юран С.И. Управление аварийными сбросами в технологическом процессе очистки сточных вод предприятия / Приборостроение–2012: материалы пятой междунар. науч.-техн. конф. (21–23 ноября 2012 г.) – Минск: Изд-во Бел.Нац.Техн.Ун-та, 2012. – С.5 – 6.
2. Алексеев В.А., Козаченко Е.М., Юран С.И. Автоматическая установка для устранения аварийного выброса в системах фильтрации сточных вод // Интеллектуальные системы в производстве. – Ижевск: Изд. ИжГТУ. – 2011. – № 2. – С. 239 – 243.
3. Алексеев В.А., Усольцев В.П., Юран С.И. Идентификация аварийных выбросов в системах фильтрации сточных вод в явно выраженных условиях многомерности и неопределенности // Интеллектуальные системы в производстве. – 2013. – № 2(22) – Ижевск : Изд-во ИжГТУ, 2013. – С.173-177.
4. Дейт К.Д. Введение в системы баз данных / Пер. с англ. Гордиенко Ю.Г. 7-е изд. – М: Изд. дом «Вильямс», 2008. – 1072 с.
5. Снакин В. В. Экология и охрана природы : Словарь-справочник. – М. : Академия, 2000. – 384 с.

Валугин И.Г., Дьяченко Ю.Н.

АДАПТИВНЫЙ АНАЛОГОВЫЙ ПРЕОБРАЗОВАТЕЛЬ ДЛЯ УСТРОЙСТВ ИЗМЕРЕНИЯ ЧАСТОТЫ СИГНАЛОВ

г. Санкт-Петербург, ФГБОУ ВПО «СПбГПУ»

Аналоговый преобразователь формирует из входного переменного напряжения $U_{вх}$, имеющего произвольную форму и амплитуду от 50мВ до 30В, последовательность прямоугольных импульсов $U_{вых}$ с уровнем стандартных логических сигналов.

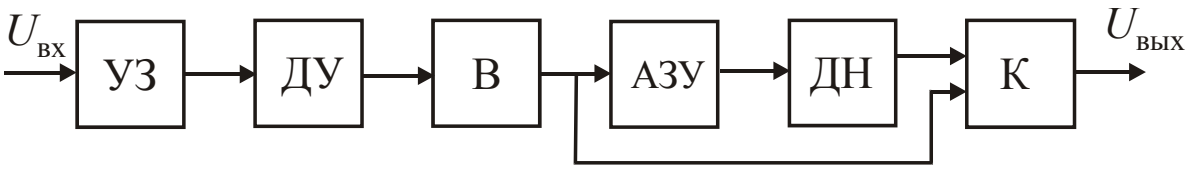


Рис 1. Структурная схема преобразователя

Устройство защиты УЗ ограничивает амплитуду входного напряжения, дифференциальный усилитель ДУ позволяет измерять частоту сигнала на фоне значительной синфазной помехи, выпрямитель В формирует импульсы положительной полярности, поступающие на один вход компаратора К. С целью защиты преобразователя от сбоев из-за наложенных на сигнал помех, порог срабатывания компаратора следует устанавливать в пределах 40-60% от амплитуды $U_{вх}$. Подстройку порога в широких пределах обеспечивает аналоговое запоминающее устройство АЗУ с делителем напряжения ДН, автоматически формирующие постоянное напряжение пропорциональное амплитуде $U_{вх}$, поступающее на второй вход компаратора и задающее его порог срабатывания.

Исследование работы схемы преобразователя с использованием компьютерного моделирования и экспериментального исследования макетного образца показало его устойчивую работу в широком диапазоне частот и амплитуд $U_{вх}$ при наличии входной помехи до 50% от амплитуды $U_{вх}$.

Аналоговый адаптивный преобразователь использован в составе измерительной системы в каналах измерения частоты сигналов.

На основе полученных результатов разработаны две лабораторные работы: первая по моделированию функционирования преобразователя в программе Multisim, вторая по его экспериментальному исследованию на макетном стенде NI ELVIS II.

Вытовтов А.А., Малютенкова С.М.

ОЦЕНКА ПОГРЕШНОСТИ И НЕОПРЕДЕЛЕННОСТИ РЕЗУЛЬТАТОВ ОПРЕДЕЛЕНИЯ ФИЗИКО-ХИМИЧЕСКИХ ПОКАЗАТЕЛЕЙ ПРОДУКТОВ ПИТАНИЯ

Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

Эффективное сотрудничество России с другими странами, совместные разработки научно-технических программ (например, в области освоения космоса, медицины, охраны окружающей среды и др.), дальнейшее развитие торговых отношений требует растущего взаимного доверия к измерительной информации, являющейся по существу основным объектом обмена при совместном решении научно-технических проблем, основой взаимных расчетов при торговых операциях, заключении контрактов на поставку материалов, изделий, оборудования. Создание единого подхода к измерениям гарантирует взаимопонимание, возможность унификации и стандартизации методов и средств измерений, взаимного признания результатов измерений и испытаний продукции в международной системе товарообмена.

Для решения перечисленных задач в России:

- введены в действие Федеральные законы «О техническом регулировании», « Об обеспечении единства измерений » и др.;
- все шире в практику метрологических работ внедряются нормативные документы (НД), в которых результаты измерений описываются в концепции «неопределенности», а не «погрешности» измерений.

Именно последнее из перечисленных нововведений и является наиболее сложной проблемой. В действующих отечественных и международных НД описаны подходы, основанные как на неопределенности, так и на погрешности измерений.

В 1993-году под эгидой международных организаций по метрологии, опубликовано “Руководство по выражению неопределенности измерения”, а в 1999-году его перевод на русский язык [2].

Концепция «неопределенности» уже широко применяется во многих странах мира, в России находится на стадии внедрения.

Руководство должно найти применение, практически во всех областях измерений, включая, в первую очередь, измерения, выполняемые:

- при решении задач обеспечения качества продукции;

- при контроле качества продукции в процессе ее производства;

- при проведении фундаментальных и прикладных исследований и разработок в науке и технике.

В силу объективных причин не все специалисты ознакомлены с методологией применения этой концепции.

Качество измерений характеризуется: *точностью, достоверностью, правильностью, сходимостью и воспроизводимостью измерений.*

Точность измерения зависит от погрешностей, возникающих в процессе их проведения.

Погрешность возникает из-за несовершенства процесса измерений. Хотя погрешность не может быть точно известна (из-за неизвестности истинного значения), это понятие удобно использовать для статистического описания процесса измерений.

Неопределенность - *это «параметр, связанный с результатом измерения и характеризующий разброс значений, которые с достаточным основанием могут быть приписаны измеряемой величине. Этим параметром может быть, например, стандартное отклонение (или кратное ему число) или ширина доверительного интервала».*

Между описанием результатов измерений с использованием погрешности и с использованием неопределенности имеется точное соответствие. Эксперты, исследователи, испытательные лаборатории должны уметь применять «Руководство по выражению неопределенности измерения», в котором весьма подробно и с множеством примеров разъяснены способы оценки неопределенности.

Целью данной работы является демонстрация применения концепции «погрешности» и концепции «неопределенности» к оцениванию и представлению результатов измерения при оценке показателей качества и безопасности товаров народного потребления на примере оценки физико-химических показателей светлого пива.

В таблице 1 приведены результаты измерения показателей качества светлого пива методами предусмотренными ГОСТ Р 51174 – Пиво. Общие технические условия и оценки их погрешности и неопределенности.

Таблица 1.

№ п/п	Показатели качества	(X ± Δ) погрешность	(X±U) неопределенность
1.	Объемная доля спирта, %, не менее - 4,5	(5,20□0,03)	(5,2□0,1)
2.	Экстрактивность начального сусла, %, - не менее 12	(12,30□0,04)	(12,3□0,2)
3.	Кислотность, к.ед., не более, - 3,2	(2,7±0,1)	(2,7 ± 0.2)
4.	pH 3,8 – 4,8	(4, 1 ± 0,1)	(4, 1 ± 0,1)
5.	Цвет, ц.ед., 0,2 – 2,5	(0,290000±0,000435)	(0,29±0,02)
6.	Массовая доля двуокиси углерода, %, не менее – 0,4	(0,42±0,03)	(0,42±0,04)

Кислотность пива *(X)* в $см^3$ раствора гидроксида натрия концентрацией 1 моль/$дм^3$ на 100 $см^3$ пива (к.ед.) измеряли по ГОСТ 12787 – Пиво. Методы определения кислотности. В тексте ГОСТ отсутствуют сведения о неопределённости результатов, но имеются некоторые исходные данные, по которым можно провести её оценку:

- окончательно приводимый результат есть результат единичного измерения;
- диапазон определения кислотности пива от 0.3 до 6.0 к.ед.;
- предел повторяемости (максимально допустимое расхождение между двумя параллельными определениями, полученными в условиях повторяемости) *r=0.1 к.ед.*;
- предел воспроизводимости (максимально допустимое расхождение между результатами, полученными в двух лабораториях) *R=0.3 к.ед.*;

Сведения о пределах повторяемости и воспроизводимости приведены в абсолютных величинах. Для вычисления неопределённости необходимо перейти от пределов повторяемости и воспроизводимости к соответствующим стандартным отклонениям. Это легко сделать, пользуясь известными соотношениями:

$R = 2.77\ \sigma_R \approx 2.8\ \sigma_R$; $r = 2.77\ \sigma_r \approx 2.8\ \sigma_r$

Получаем: стандартное отклонение повторяемости $\sigma_r = \frac{0.1}{2.8} \approx 0.036$;

стандартное отклонение воспроизводимости $\sigma_R = \frac{0.3}{2.8} \approx 0.107$.

Результаты вычисления расширенной неопределённости U приведены в табл. 2.

Таблица 2.

к.ед.	$u = \sqrt{\sigma_R^2 + \sigma_r^2}$	$U = 2u$	Запись результата
1,3	0.113	0.226	1,3 ± 0.2
6,0	0.113	0.226	6.0 ± 0.2
2,7	**0.113**	**0.226**	**2,7 ± 0.2**

Активную кислотность – pH измеряли по ГОСТ Р 53070 – Пиво. Метод определения pH. В стандарте сказано - границы абсолютной погрешности измерений pH пива при помощи pH-метра с электродной системой составляют ±0,1 ед. pH при P = 0,95. Из «Руководства» следует что эта величина является и погрешностью и неопределенностью измерения и никаких дополнительных исследований и оценок проводить не требуется. Измеренное значение pH = 4,1. Тогда результат можно записать либо как 4,1, либо как (4,1 ± 0,1) pH.

Массовая доля двуокиси углерода измерялась по ГОСТ Р 51154 - Пиво. Методы определения двуокиси углерода и стойкости. Для измерения использовался афрометр АМ-01 с манометром класса точности 1,0, предел измерения 1,0 МПа (10 кг/см^3, 10 атм.) и термометр ртутный стеклянный лабораторный, пределом измерения 0-50 °С, класса точности 0,5.

Показание манометра при температуре 22^{0}С составило 1,8 кг/см^3, что по прилагаемой к ГОСТ таблице соответствует 0,42 % содержания двуокиси углерода.

Точность средств измерений может быть представлена приведенной погрешностью:

$$\Delta_{пр} = \frac{\Delta_{max}}{X_{норм}} * 10_0$$

В качестве нормируемого значения может быть конечное значение прибора. Это дает возможность вычислить наибольшую погрешность данного средства измерения.

$$\Delta_{max} = \frac{\Delta_{пр} * X_{норм}}{100\%}$$

Рассчитаем погрешность косвенного измерения, где $\Delta_{терм}$ - погрешность термометра 0,25^{0}С, а $\Delta_{маном}$ - погрешность манометра = 0,1 кг/см^3. Погрешность косвенного измерения равна 0,03. Массовая доля двуокиси углерода (0,42 ± 0,03)%.

Рассчитываем неопределенность измерения. Найденная максимальная погрешность позволяет нам представить точность измерений в терминах неопределенности измерений, используя найденную наибольшую погрешность по всей шкале прибора. Поэтому, полагая, что найденная наибольшая погрешность лежит в определенных

границах, можно определить стандартную неопределенность, оцениваемую по типу В, по формуле:

$$U_B = \frac{\Delta_{max}}{\sqrt{12}}$$

$U_{B\ (терм)} = 0{,}072$; $U_{B(маном)} = 0{,}029$.

Кроме того точность средств измерений может быть представлена относительной погрешностью на каждой отметке шкалы средства измерения. Это дает возможность представить точность средства измерения в терминах неопределенности измерений на каждой отметке шкалы прибора. Известно, что относительная погрешность на оцифрованной отметке шкалы средства измерений равна $\delta_{o1} = \frac{\Delta_1}{X_1}$.

$\delta_{o\ (маном)} = 0{,}06$; $\delta_{o\ (терм)} = 0{,}01$.

В терминах неопределенностей можно оценить относительную стандартную неопределенность, оцениваемую по типу В, на каждой оцифрованной отметке шкалы манометра и термометра по формуле:

$$U_B = \frac{\delta_{oi}}{\sqrt{12}}.$$

$U_{B(маном)} = 0{,}017$; $U_{B(терм)} = 0{,}003$.

$$U_{B(метод)} = \frac{\Delta_{метод}}{2\sqrt{3}} = 0.009$$

$$U_{суммарн} = \sqrt{U^2_{B(маном)} + U^2_{B(терм)} + U^2_{B(метод)}} = 0{,}0198 = 0{,}02$$

Расширенную неопределенность вычисляют по формуле:

$U_{расш} = k_{p=0.95} * U_{суммарн} = 2*0{,}02 = 0{,}04$.

Цвет пива определяли по ГОСТ 12789 - Пиво. Методы определения цвета. Методика выполнения измерения обеспечивает получение достоверных данных при определении цвета пива в диапазоне 0,1-4,0 см^3 раствора йода концентрацией 0,1 моль/дм^3 на 100 см^3 воды. Результат измерения цвета образца пива составил 0,29 ц.ед.

Предел допустимого среднеквадратического отклонения случайной составляющей основной абсолютной погрешности используемого фотометра КФК-3 составляет не более 0,15%.

Погрешность измерения цвета равна 0,000435 ц.ед.

Относительное допускаемое расхождение между результатами двух параллельных определений, а также результатами двух определений, полученными в разных лабораториях для одной и той же пробы, для доверительной вероятности Р=0,95 не должно превышать 3%.

Для перехода от предела повторяемости и воспроизводимости к соответствующему стандартному отклонению воспользуемся известным соотношением:

$$R = 2.77\ \sigma_R \approx 2.8\ \sigma_R$$

Стандартное отклонение повторяемости $\sigma_r = \frac{0.15}{2.8} \approx 0.054$ или в единицах измерения 0,0005.

Относительное стандартное отклонение воспроизводимости (оно же – относительная стандартная неопределённость) $\sigma_R = \frac{3\%}{2.8} \approx 1{,}07\%$

или в единицах измерения 0,0107 = 0,01.

Суммарная неопределенность определения равна

$U_B = \sqrt{\sigma_R^2 + \sigma_r^2} = 0{,}01$

Соответственно расширенная неопределённость при коэффициенте охвата равном *2* * U_B= 0,01×2=0,02

При представлении результата допускается использование, как стандартной неопределённости, так и расширенной неопределённости.

В первом случае результат определения цвета может быть выражен следующим образом: 0,29±0,01 (одно стандартное отклонение)

Во втором случае: цвет (0,29±0,02) (при коэффициенте охвата 2)

Предпочтительным – является второй вариант.

Определение спирта и массовую долю сухих веществ в начальном сусле проводили по ГОСТ 12787 – Пиво. Методы определения спирта, действительного экстракта и расчет сухих веществ в начальном сусле. Объемная доля спирта в исследуемом образце составила - 5,2% об., экстрактивность начального сусла составила – 12,3%.

Абсолютная погрешность определения спирта составила – □0,03%об., а абсолютная погрешность определения экстрактивности начального сусла - □0,04%.

Расхождение между результатами двух параллельных определений одной и той же пробы пива при доверительной вероятности Р=0,95 по абсолютной величине не должно превышать в процентах: 0,06 - для массовой доли спирта; 0,03 - для массовой доли действительного экстракта.

Расхождение между результатами определений одной и той же пробы пива в разных лабораториях при доверительной вероятности Р=0,95 по абсолютной величине не должно превышать в процентах: 0,14 - для массовой доли спирта; 0,07 - для массовой доли действительного экстракта.

- стандартное отклонение повторяемости определения массовой доли спирта: $\sigma_{r(спирта)} = \frac{0.06}{2{,}8} \approx 0.02$; массовой доли действительного экстракта $\sigma_{r(экстракт)} = \frac{0.03}{2{,}8} \approx 0.01$;

- стандартное отклонение воспроизводимости определения массовой доли спирта: $\sigma_{R(спирта)} = \frac{0.14}{2,8} \approx 0.05$; массовой доли действительного экстракта $\sigma_{R(экстракт)} = \frac{0.07}{2,8} = 0,025 \approx 0,03$.

- стандартное отклонение определения объемной доли спирта - □=0,004,

- стандартное отклонение определения сухих веществ в начальном сусле □=0,107

Результаты вычисления расширенной неопределённости U приведены в табл. 3.

Таблица 3.

	$u = \sqrt{\sigma_R^2 + \sigma_r^2 + \delta^2}$	$U = 2u$	Запись результата
Спирта 5,2	0,054	0,108	5,200□0,108 5,2□0,1
Экстракта 12,3	0.112	0.224	12,300□0,224 12,3□0,2

Таким образом, показано, что алгоритмы, приведенные в «Руководстве по выражению неопределенности измерений» и других сопутствующих НД **приемлемы для практического использования, позволяют достоверно оценить качество результатов измерений** предусмотренных процедурами товарной экспертизы, подтверждения соответствия товаров народного потребления и оформить их в соответствии с международными требованиями.

Применение «Руководства» и других сопутствующих регламентирующих документов не вызывает затруднений у пользователей имеющих минимальные знания в области отечественной метрологии, в частности теории погрешностей и соответствующей терминологии.

Список использованной литературы

1. Международная рекомендация GUM, «Руководство по выражению неопределенности измерений».

2. Руководство по выражению неопределенности измерения. Перевод с англ. под науч. ред. проф. В.А. Слаева, С.П.б.: ГП ВНИИМ им. Д.И. Менделеева, 1999, Рекомендация ГСИ «Применение «Руководства по выражению неопределенности измерения», С.П.б.: ГП ВНИИМ им. Д.И. Менделеева, 1999.

3. Количественное описание неопределенности в аналитических измерениях. Руководство ЕВРАХИМ / СИТАК. 2- е изд. / Под ред. А. Конопелько. СПб.: ВНИИМ им. Д .И. Менделеева, 2003.

4. Рекомендации по метрологии Р 50.2.038-2004. Измерения однократные прямые. Оценивание погрешностей и неопределенности результата измерений. ИПК Издательство стандартов, 2004.

5. ГОСТ Р 51174-2009 – Пиво. Общие технические условия.

Гайвоненко А.Е.

МЕТОДИКА РАСЧЕТА ПРОДОЛЬНОЙ СОСТОВЛЯЮЩЕЙ ПОТЕНЦИАЛА ВЛИЯЮЩЕЙ НА ВОК

Новосибирск, СибГУТИ

В тезисе рассмотрена методика расчета продольной составляющей потенциала электромагнитного поля контактной сети, оказывающей весьма значительное влияние на волоконно-оптический кабель, подвешенный на этих опорах.

На железной дороге очень часто применяется подвеска волоконно-оптического кабеля (ВОК) на опорах контактной сети с электротягой переменного тока. При эксплуатации вблизи заземленных конструкций в результате искажения формы электрического поля возникает продольная составляющая потенциала (U), которая оказывает значительное влияние на процесс повреждения кабеля в узле ВОК – поддерживающий зажим. Величина наводимого потенциала зависит от влияния самой опоры, поддерживающего зажима, а также и от типа поддерживающих конструкций контактной сети, в частности от типа консолей (заземлённые консоли либо изолированные консоли) [1].

Были получены эмпирические формулы определения продольной составляющей потенциала с погрешностью, не превышающей 8% в зоне подвески ВОК на расстоянии от 30 до 60 см от поверхности опоры.

В случае если на рассматриваемом участке применены неизолированные (заземлённые) консоли, формула для определения потенциала имеет вид [1]:

$$U = U_{Э} \cdot \frac{1{,}69 - 1{,}69 \cdot e^{-(1{,}3 \cdot l)}}{1{,}69}, \qquad (1)$$

где l – расстояние от оси опоры до точки, где определяется потенциал ВОК, измеренное вдоль пролета, в метрах;

$U_{Э}$ - потенциал поля в данной точке, при отсутствии опоры и других конструкций, искажающих форму плоскопараллельного электрического поля.

В случае если на рассматриваемом участке применены изолированные консоли, формула для определения потенциала имеет вид [1]:

$$U = U_Э \cdot \frac{2{,}48 - 2{,}48 \cdot e^{-(2{,}2 \cdot l)}}{2{,}48}. \qquad (2)$$

Для достоверной картины влияния продольной составляющей потенциала, наводимого вдоль поверхности ВОК, необходимо определить не менее пяти значений с шагом не более 10 см. При этом место выхода кабеля из поддерживающего зажима необходимо считать начальной точкой отсчета и принять в этой точке расстояние $l = 0$ см.

Величина $U_Э$ определяется выражением [1]:

$$U_Э = 27{,}5 \cdot k_2 \cdot \frac{H_K \cdot H_A}{a^2 \cdot H_K^2 \cdot H_A^2}, \qquad (3)$$

где $H_К$ - расстояние от уровня головки рельса до эквивалентного контактного провода, м (принимается при расчете равной 6,8 м);

$H_А$ – средняя высота подвески волоконно-оптического кабеля, м;

a - ширина сближения, м;

k_2 - защитный коэффициент определяется из таблицы 1.

Таблица 1.

Коэффициент k_2 из приложения 12 «Правил защиты устройств проводной связи и проводного вещания от влияния тяговой сети электрифицированных железных дорог переменного тока».

Число дополнительных влияющих проводов		k_2
Однопутный участок	0	0,4
	1	0,5
	2	0,6
Двупутный участок	0	0,6
	1	0,7
	2	0,8

Полученное значение $U_Э$ должно быть не более 12 кВ. Изменение продольной составляющей потенциала вдоль ВОК не должно быть больше 50 вольт на 1 см, либо 500 вольт на 10 см, что соответствует напряженности поля 5 кВ/м – безопасной для кабеля. В противном случае необходимо рассмотреть другой вариант подвески ВОК, с увеличением его расстояния до высоковольтных проводов.

Данная методика расчета продольной составляющей потенциала используется на участках железных дорог ЗАО «Транстелеком Западная Сибирь» при выборе места расположения ВОК на опорах контактной сети, марок ВОК и способах их подвески при новом строительстве, реконструкции, и капитальном ремонте.

Литература

1. Инструкция по предотвращению электротермической деградации волоконно-оптических кабелей, подвешенных на опорах контактной сети участков железных дорог ОАО «РЖД» с электротягой переменного тока.

Гатчин Ю.А., Сухостат В.В.

МЕТОД ОЦЕНКИ ЗАЩИЩЕННОСТИ IT-СПЕЦИАЛИСТА В УСЛОВИЯХ ВНЕШНИХ ВОЗДЕЙСТВИЙ

г. Санкт-Петербург,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Аннотация

В рамках статьи на основе новых физических принципов, технических средств для оценки состояния организма и современных методов компьютерной обработки данных предложен новый подход к решению обозначенной проблемы – использование технологии газоразрядной визуализации (ГРВ). Это способ получения новой характеристики состояния человека.

Анализ существующего состояния и тенденций цивилизационных изменений показывает, что информация приобрела статус одного из важнейших национальных ресурсов, определяющих экономический, научно-технический и оборонительный потенциал страны [1]. В первую очередь, это проявляется в создании целой индустрии производства информации для обеспечения потребностей социально-зкономичской практики в условиях конкуренции. Основной характерной чертой в этих обстоятельствах является создание единого информационного поля, за счет которого и предполагается обеспечить информационное превосходство над конкурентами.

Наряду с резким повышением роли информационных процессов растут и информационные нагрузки на IT-специалиста сложных комплексов, как со стороны среды, так и со стороны профессиональной деятельности.

В конкурентной борьбе широко распространены разнообразные действия, направленные на получение конфиденциальной информации, с помощью технических средств промышленного шпионажа [2].

Помимо использования радиоэлектронного подавления восходящих и нисходящих каналов связи центров обеспечения данными, организации вирусных атак на серверы баз данных, специалистами развитых стран уделяется значительное внимание и другим способам обеспечения информационного превосходства – информационно-психологическому воздействию на органы управления различного уровня и их руководителей, и непосредственно на IT-специалистов. Причем последний способ является основным в комплексе угроз информационной безопасности, в частности, и информационно-психологической безопасности (ИПБ).

Исследования в области теории информационной безопасности и методологии защиты информации [3], в области информационной безопасности [1, 2], изучения человеко-машинных систем в инженерной психологии и эргономике [4], опыт внедрения динамических методов анализа психофизиологического и функционального состояния человека на основе полипараметрической функциональной экспресс-диагностики в спорте [5-7] подтверждают взаимосвязь факторов, определяющих эффективность обеспечения ИПБ IT-специалиста, с наличием средств и методов выявления их индивидуально-личностных реакций в режиме реального времени в условиях внешних информационных воздействий [8, 9]. При этом конечной целью оценки состояния IT-специалиста должна быть его нормализация (управление состоянием). А именно: предотвращение неблагоприятных состояний оператора, предупреждение ошибок и сохранение здоровья IT-специалиста.

Поэтому методы оценки психофизиологического состояния IT-специалиста должны удовлетворять основным требованиям таким, как:

- информативность, специфическая для деятельности IT-специалиста;
- объективность, независимость от оператора и условий съема данных;
- простота реализации, малое время измерения и анализа;
- возможность использования в широком диапазоне условий, вплоть до полевых;
- надежное хранение больших массивов информации; возможность быстрого освоения непрофессиональными операторами, вплоть до самоконтроля IT-специалистами; наглядный и понятный характер предоставляемой информации.

Аналогичным условиям могут удовлетворять только современные компьютеризированные комплексы. Одним из таких методов, активно развивающихся в последнее время в медицине и психологии является метод газоразрядной визуализации (ГРВ) [5-7].

Метод ГРВ создан в последние годы в России на базе современных компьютерных технологий и позволяет проводить исследования динамики психофизиологического состояния испытуемых за счет регистрации характеристик газоразрядного свечения, индуцируемого в электромагнитном поле высокой напряженности (ГРВ биоэлектрография) [5-7].

Метод получения газоразрядного изображения заключается в следующем. Между исследуемым объектом и диэлектрической пластиной, на которой размещается объект, подаются импульсы напряжения от генератора электромагнитного поля, для чего на обратную сторону пластины нанесено прозрачное токопроводящее покрытие. При высокой напряженности поля в газовой среде пространства контакта объекта и пластины развивается скользящий газовый разряд, параметры которого определяются свойствами объекта. Пространственное распределение свечения разряда с помощью оптической системы и прибора с зарядовой связью преобразуется в видеосигнал. Полученные изображения, переводятся в цифровой формат и записываются в виде одиночных кадров (ГРВ-грамм) или видеофайлов. Специализированный программный комплекс позволяет проводить обработку изображений, представляющих собой пространственное распределение пикселей различной яркости, и вычислять набор параметров, описывающих поле излучения разряда.

Состояние биологического объекта сказывается на ГРВ параметрах в основном за счет вариации следующих характеристик объекта: импеданса; импеданса участков поверхности; структурных свойств; эмиссионных свойств [6]. Анализ характеристик двумерного изображения приводит к формированию набора параметров, который является параметрическим описанием поля излучения разряда.

На сегодняшний день разработано несколько десятков различных ГРВ-параметров. Накопленный в течение ряда последних лет опыт их использования для анализа ГРВ-грамм спортсменов [5-7] позволяет выделить набор из нескольких наиболее информативных параметров [7]:

- площадь свечения (S) – количество точек изображения с ненулевой интенсивностью (не удаленных при фильтрации шума);
- нормализованная площадь свечения – отношение площади изображения к площади внутреннего овала;
- средняя интенсивность свечения ($\overline{I}$) – средняя интенсивность точек изображения с ненулевой интенсивностью;
- количество фрагментов (N_F) – количество восьмисвязных групп точек с ненулевой интенсивностью;
- средняя площадь фрагмента ($\overline{S}_F$) – среднее количество точек в каждом фрагменте;

- среднее расстояние фрагментов до центра ($\overline{D}_F$) – среднее расстояние от центра тяжести фрагмента до центра свечения;

- средний радиус свечения ($\overline{R}$);

- нормализованное среднеквадратическое отклонение радиуса ($\sigma_{\overline{R}}$);

- коэффициент формы (K) – мера изрезанности внешнего контура свечения, минимальное значение равно 1 – соответствует свечению в форме окружности или кольца, большие значения – сильно изрезанное изображение, с большим количеством разрывов контура;

- энтропия (H) – мера информативности изображения – возрастает при увеличении множества значений радиуса контура.

Для расчета среднего радиуса свечения, нормализованного среднеквадратического отклонения радиуса и коэффициента формы строится функция R(α), значения которой равны расстоянию между первой и последней точками ненулевой интенсивности, лежащими на луче, выходящем из центра свечения под углом α∈[0;2: π) к вертикали (рисунок 1). Как правило, функция R(α) неоднородна и меняется достаточно хаотически. Без больших погрешностей можно рассматривать ее как последовательность реализаций случайной величины и применить аппарат описания статистических зависимостей, что позволяет вычислить ряд параметров.

Средний радиус свечения ($\overline{R}$) – является математическим ожиданием значений функции R(a). Нормализованное отклонение вычисляется как $\sigma_{\overline{R}} = \frac{\sigma_R}{(\overline{R})}$, где σ_R – среднеквадратическое отклонение функции R(α).

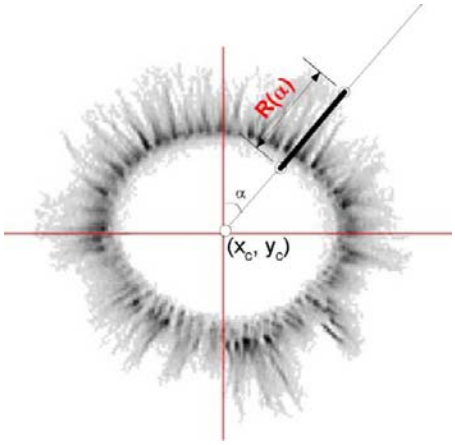


Рисунок 1. - Вычисление функции R(α) [7].

Коэффициент формы $K = \frac{L}{2\pi\overline{R}}$, где L – длина кривой функции *R(α)*.

Энтропийный анализ позволяет вычислить меру «информативности» контура свечения. Величина энтропии вычисляется

на основании вероятностей p_j получения функцией $R(\alpha)$ значения X_j по формуле:

$$\mathrm{H}\left(R(\alpha)\right) = -\sum_{\mathrm{j}=1}^{\mathrm{M}} p_j\left(R(\alpha_j)\right) \ln\left[p_j\left(R\left(\alpha_j\right)\right)\right],$$

где $p_j\left(R\left(\alpha_j\right)\right) = \frac{N\left(R(\alpha_j)\right)}{N_\Sigma}$, $N\left(R\left(\alpha_j\right)\right)$ – общее количество значений величины $R\left(\alpha_j\right)$, а N_Σ – количество всех значений $R(\alpha)$.

Каждый из перечисленных параметров может быть рассчитан не только для всего изображения, но и для отдельных угловых секторов.

ГРВ Метод может служить в качестве первого этапа скрининговой экспресс-диагностики состояния группы IT-специалистов как основы прогностической оценки ее психофизиологической готовности к профессиональной деятельности. Ключевым аргументом использования технологии ГРВ в исследовании являются ее свойства как быстрого, неинвазивного и чувствительного способа системной оценки психофизиологического состояния IT-специалиста.

Библиографический список

1. Шакин Д.Н. Информационная безопасность [Текст] / Д.Н. Шакин, Е.Г. Бунев, С.М. Доценко, А.П. Ильин, П.С. Марголин, В.С. Пирумов, С.И. Тынянкин. – М.: ЗАО «Издательский дом «Оружие и технологии»», 2009. – 256 с.

2. Ярочкин В.И. Информационная безопасность [Текст] / В.И. Ярочкин – М.: Академический проект, 2008. – 544 с.

3. Гатчин Ю.А. Теория информационной безопасности и методология защиты информации [Текст] / Ю.А. Гатчин, В.В. Сухостат – СПб., СПбГУ ИТМО, 2010. – 98 с.

4. Ломов Б.Ф. Основы инженерной психологии / Б.А. Душков, Б.Ф. Ломов, В.Ф. Рубахин. – М.: Высшая школа, 1986. – 448 с.

5. Короткова А.К. Метод газоразрядной визуализации биоэлектрографии в исследованиях психофизиологического состояния квалифицированных спортсменов [Текст]: дисс. канд псих. наук: 13.00.04: защищена 27.04.2006 / Короткова Анна Константиновна. СПб, 2006. – 145 с. Библиогр.: с. 132-145.

6. Коротков К.Г. Принципы анализа ГРВ биоэлектрографии. [Текст] / К.Г. Коротков. – СПб.: Изд-во «Реноме», 2007. – 286 с.

7. Величко Е. Н. Программно-аппаратный комплекс оценки психофизиологического состояния спортсмена [Текст]: дисс. к.т.н.: 05.11.17: / Е. Н. Величко. – СПб, 2010. – 137 с. Библиогр.: с. 124-137.

8. Гатчин Ю.А., Величко Е.Н., Сухостат В.В. Методология информационно-психологической безопасности личности [Текст] / Ю.А.

Гатчин, Е.Н. Величко, В.В. Сухостат // Труды Конгресса по интеллектуальным системам и информационным технологиям "IS&IT" Научное издание в 4-х томах. – Москва: Физматлит, 2011. – Т. 2. – 415 с. – С. 338-344

9. Гатчин Ю.А., Сухостат В.В., Тушканов Е. Имитационная модель оценки информационно-психологических воздействий на IT-специалиста [Текст] // научн. ж-л «Научное обозрение». – 2014. – № 3. – С. 169-175.

Груздев В.В.

БУДУЩЕЕ РОССИЙСКОЙ ПРОМЫШЛЕННОСТИ - В РУКАХ КВАЛИФИЦИРОВАННЫХ КАДРОВ

Гатчина, ОАО «Завод «Кризо»

На ОАО «Завод «Кризо» начала функционировать первая в Ленинградской области базовая кафедра «Управление безопасностью технических объектов» Санкт-Петербургского Государственного политехнического университета (далее СПб ГПУ).

Залог успешного развития государства - в соединении научно-технологического потенциала и высококвалифицированных специалистов, способных решать задачи на высокотехнологичном оборудовании: без этого превращения нашей страны из поставщика сырьевых ресурсов в разработчика и производителя высокотехнологичных систем и технологий невозможно.

В начале 2013 года руководством завода - генеральным директором Ягубковым В.Г. и советником генерального директора, доктором технических наук, профессором Богдановым С.С, было принято концептуальное решение о создании при заводе структуры по подготовке кадров высшего и среднего специального образования, а именно:

- создание совместно с СПб ГПУ базовой кафедры и студенческой лаборатории на производственной площадке предприятия для подготовки специалистов с высшим образованием;
- под эгидой Правительства Ленинградской области создание «Регионального ресурсного кадрового центра профессиональной ориентации, допрофессиональной и профессиональной подготовки и переподготовки» (далее РРКЦ) - для подготовки специалистов технических специальностей со средним специальным образованием.

И сразу началась работа:

- 06.06.2014 г. при научно-техническом совете предприятия был проведён Круглый стол на тему «Создание регионального учебно-

производственного центра подготовки кадров для северо-западного региона».

- Были проведены неоднократные встречи и консультации с руководителями и специалистами учебных заведений г. Санкт-Петербурга: профильными колледжами, лицеями и СПб ГПУ.
- Были проведены переговоры с российским филиалом станкостроительной компании DMG/MORI SEIKI и получен официальный положительный ответ по оснащению будущего центра современным оборудованием и учебно-методическими материалами.
- Силами работников кафедры «Системный анализ и управление» и предприятия под руководством зав. кафедрой Козловым В.Н. и генеральным директором Богдановым С.С. (возглавил завод с августа 2014 г.) началась подготовка документов по созданию базовой кафедры СПб ГПУ при ОАО «Завод «Кризо».

Везде мы находили понимание, поддержку и помощь в получении необходимых информационно-методических материалов. При активной поддержке председателя профсоюза работников профобразования Яушева В.Г. предложение по созданию при заводе РРКЦ было вынесено на рассмотрение в профильную комиссию по науке и высшей школе г. Санкт-Петербурга (председатель комиссии – депутат Воронцов А.В.), где было принято решение о поддержке данного начинания.

Активизировалась работа и в рамках предприятия: при поддержке Администраций г. Гатчины и Гатчинского муниципального района возобновилось проведение экскурсий по заводу для старшеклассников школ г. Гатчины и Гатчинского района с целью профориентации, стала расширяться работа по прохождению практики студентами Государственного политехнического университета.

На сегодняшний день работа принесла результаты: подписан договор о сотрудничестве с СПб ГПУ. Решением Ученого совета университета и на основании приказа по университету № 283 от 28.03.2014 г. создана базовая кафедра «Управление безопасностью технических объектов» в составе «Института информационных технологий и управления» на производственной площадке ОАО «Завод «Кризо». Заведующим кафедрой назначен генеральный директор предприятия - д.т.н., профессор кафедры «Системный анализ и управление» Богданов С.С.

Проведены конструктивные переговоры по привлечению к участию в проекте по созданию РРКЦ учебных заведений Ленинградской области – это Тосненский политехнический техникум (решено проводить совместную подготовку кадров и создать при заводе филиал техникума по подготовке специалистов для работы на станках с ЧПУ) и Кировский политехнический техникум (решено в рамках стратегического

партнёрства участвовать в создании сети ресурсных кадровых центров по Ленинградской области).

Решение о создании на производственной площадке завода «Кризо» первого РРКЦ запланировано принять на совещании профильной комиссии при Правительстве Ленинградской области, возглавляемой заместителем председателя Густовым В.А. В заключении надо отметить, что очень ценным аспектом в данном проекте является соединение науки с производством, а именно: сочетание в одном лице научного руководителя базовой кафедры и генерального директора завода.

Мешалкина М.Н., Борисов А.В., Потапов И.В., Потапов С.В.

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ОБРАЗОВАНИЯ ПАРНИКОВЫХ ГАЗОВ В ВОДОХРАНИЛИЩАХ ДЛЯ ОЦЕНКИ ИХ ВОЗДЕЙСТВИЯ НА АТМОСФЕРУ ЗЕМЛИ

Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

Проблема обеспечения населения Земли энергоресурсами стоит достаточно остро. При этом наряду с использованием традиционных источников энергии, таких как уголь, нефтепродукты и природный газ, используется энергия гидроэлектростанций. Гидроэлектроэнергетика в настоящий момент обеспечивает 19% объема мирового электропотребления и развивается более чем в 150 странах.

Традиционно гидроэнергетика считалась источником энергии, не загрязняющим атмосферу. В последние несколько десятилетий обсуждается вопрос выбросов парниковых газов в атмосферу с поверхности водохранилищ. Особое внимание к водохранилищам, как источникам парниковых газов, вызвано тем, что при затоплении территорий, на которых были ранее расположены леса и поля с растениями, при их перегнивании на дне вновь образовавшихся водоемов, образуются такие парниковые газы как углекислый газ и метан. Эти газы через толщу воды поднимаются в атмосферу. При этом выбросы парниковых газов сопоставимы с выбросами тепловых станций на ископаемом топливе при пересчете на 1 кВт·ч вырабатываемой электроэнергии [1]. Межправительственной группой экспертов по изменению климата в 2006 году была признана необходимость проведения дополнительных исследований по оценке выбросов парниковых газов (особенно метана) с водохранилищ ГЭС. В 2008 г.

ЮНЕСКО и другие международные организации начали международный исследовательский проект с целью разработки методологии по точности оценки эффекта по выбросам парниковых газов, вызванным созданием водохранилищ.

Этой проблемой также в настоящее время занимаются в СПбГПУ. Летом 2014 года планируется проведение исследований выбросов парниковых газов на водохранилище Саяно-Шушенской ГЭС. Перед проведением исследований необходимо отработать методику измерения выделений парниковых газов в лабораторных условиях. Для этого была создана установка, моделирующая процесс проведения исследований на водохранилище. Схема установки изображена на рис. 1. Установка представляет собой большую емкость с водой (3), на поверхности которой плавает камера (4), в которую через толщу воды поступает проба газа. Проба известного объема и состава, подается шприцом (1) в отверстие снизу емкости с водой через 2 клапана, при этом пузырьки пробы попадают в плавучую камеру. Отбор пробы происходит при открытых клапанах (5) шприцом (6). Во время измерений фиксируется давление с помощью диффузного манометра (7) и температура с помощью термометра (8). Было проверено, что камера герметична.

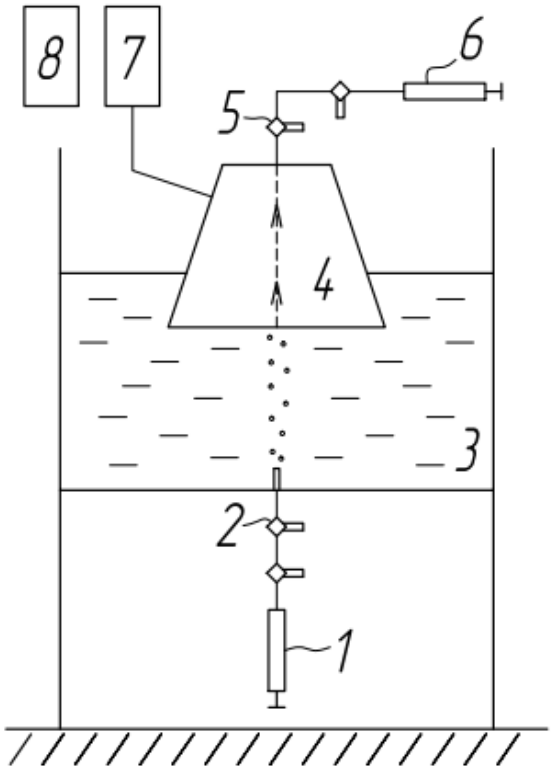


Рис. 1 Установка для моделирования выделений парниковых газов с водохранилищ в лабораторных условиях

Газы, выделяющиеся из толщи воды водохранилищ, по своему составу представляют собой смесь углекислого газа и метана. На сегодняшний день вклад CO_2 в парниковый эффект составляет более 60%, на метан приходится около 20% и примерно 20% на другие парниковые газы. Но при этом молекула CH_4 в десятки раз эффективнее поглощает инфракрасное излучение, чем молекула CO_2. В исследованиях было основное внимание уделено метану, поскольку он практически не поглощается в воде, в отличие от углекислого газа, и полностью достигает объема камеры.

Для моделирования пробы необходимо было опираться на ранее проведенные исследования. Были взяты данные по исследованию процесса образования метана в грунтах водохранилищ России в расчете 5 мл метана/дм^3 в сутки, что составляет усредненные результаты по различным водохранилищам РФ [2]. В шприц вводился объем 130 мл пробы стандартного образца 1% метана в азоте. Пробы подавалась в отверстие внизу емкости с водой, и после некоторого времени отбиралась из плавучей камеры. Измерения газового состава пробы проводились на инфракрасном фурье-спектрометре ФСМ1202. Спектр пробы, отобранной из камеры представлен на рис. 2.

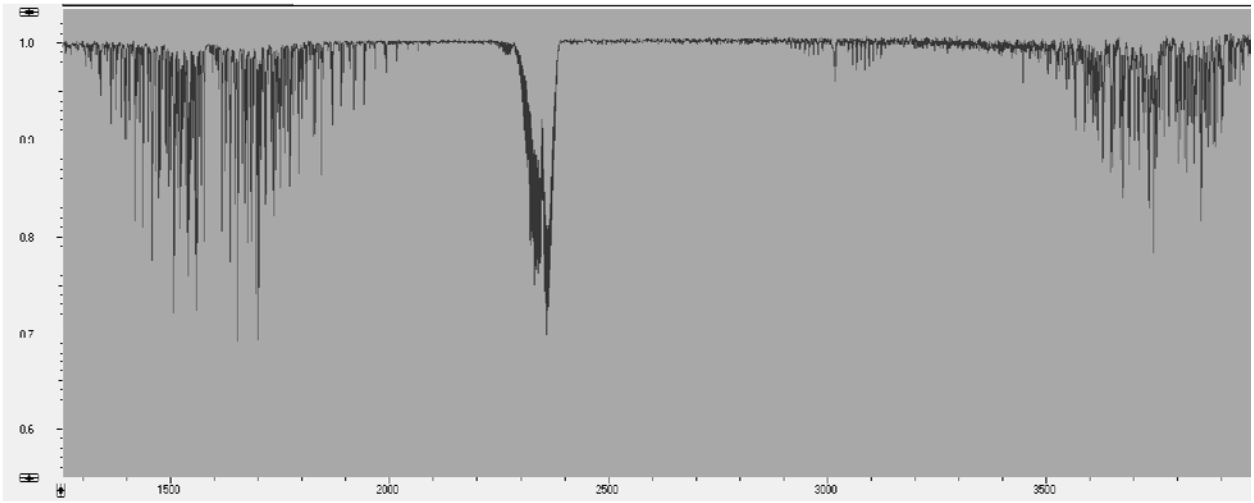


Рис. 2 Окно программы FSpec, на котором изображен спектр пробы, имитирующей выделение парниковых газов с поверхности водоема

На рис. 2 слева направо: полосы поглощения воды (1300-2040 см-1), полоса поглощения углекислого газа (2250-2400 см-1), полоса поглощения метана (2900-3140 см-1), полоса поглощения воды (3400 – 4000 см-1).

Особую сложность и ценность представляют собой измерения в области малых концентраций метана. Процесс накопления метана в камере неравномерен. После достижения некой концентрации метана в камере, будет достигнуто равновесие, из-за диффузии метана обратно в толщу воды. Для определения концентрации пробы метана в области

малых концентраций был построен градуировочный график на основной линии поглощения метана 3018 $см^{-1}$ зависимости концентрации метана от оптической плотности, изображенный на рис. 3.

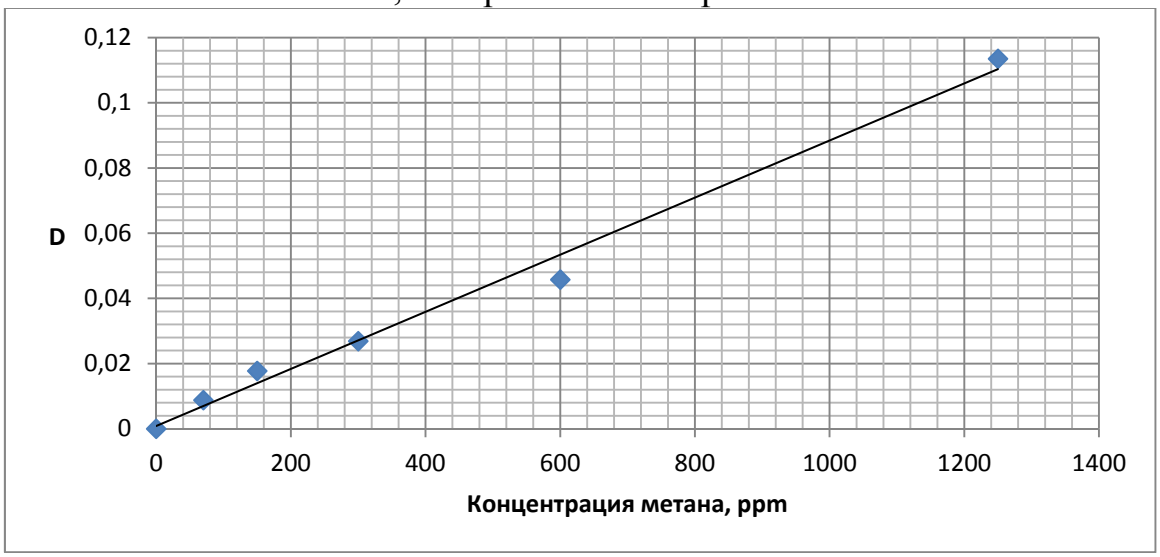


Рис. 3 Градуировочный график, построенный с помощью стандартного образца 1% метана в азоте

Разбавление стандарта 1% метана в азоте производилось с помощью шприцов, заполненных чистым азотом. Погрешность разбавления составила 15%. Аналогичные графики построены для больших концентраций метана с помощью стандартных образцов. С помощью градуировочного графика была определена концентрация метана в объеме камеры. Проба, подаваемая снизу в камеру, имитировала эмиссию метана со дна водоема. Концентрация пробы метана в объеме камеры составила 150 ppm, предел обнаружения этим способом составляет 100 ppm. Проба будет представительной для проведения достоверного анализа с помощью инфракрасного спектрального анализа, если она будет отбираться из подобной камеры на водохранилище с промежутком не менее 12 часов. В настоящее время подбирается мобильный аппаратный комплекс для проведения измерений на водохранилище.

В данной работе приведены результаты модельных исследований в лаборатории для отработки методики отбора и измерения проб из плавучей камеры в условиях реального водохранилища ГЭС. Данные исследований смогут уточнить вклад, вносимый водохранилищами в парниковый эффект планеты Земли и выработать меры для его уменьшения.

Литература

1. Kelly. C. A., Rudd, J. W. M., St. Louis, V., and Moore, T., Turning attention to reservoir surfaces, a neglected area in greenhouse studies, *EOS, Trans. Am. Geophys. Union*, 1994, vol. 75, pp. 332–333.

2. Дзюбан А.Н. Экологические аспекты исследований содержания метана в природных водах // Вода: химия и экология. – 2012. – №11. – С. 10-15.

Молодцов В.О. [2]***, Смирнов В.Ю.*** [2]***, Солнушкин С.Д.*** [1]***, Чихман В.Н.*** [1]

ИЗМЕРЕНИЕ ФУНКЦИОНАЛЬНЫХ ПАРАМЕТРОВ ДЫХАТЕЛЬНЫХ МЫШЦ

С.Петербург, [1]Институт физиологии им. И.П. Павлова РАН,
[2]Электротехнический университет (ЛЭТИ)

Эффективность вентиляционной функции дыхания человека в значительной степени определяется работой дыхательных мышц. Наиболее полная оценка состояния дыхательных мышц обеспечивается путем измерения давления в дыхательном тракте во время перекрытия воздушного потока в первые 100 мс естественного вдоха пациента (окклюзия), а также вычисления времени полезного дыхательного цикла (отношение длительности инспираторной активности дыхательных мышц к общей длительности дыхательного цикла).

Разработано устройство MD245, предназначенное для регистрации параметров сократительной активности инспираторных дыхательных мышц в функциональной диагностике и в научных исследованиях. Структурная схема устройства MD245 показана на рис.1.

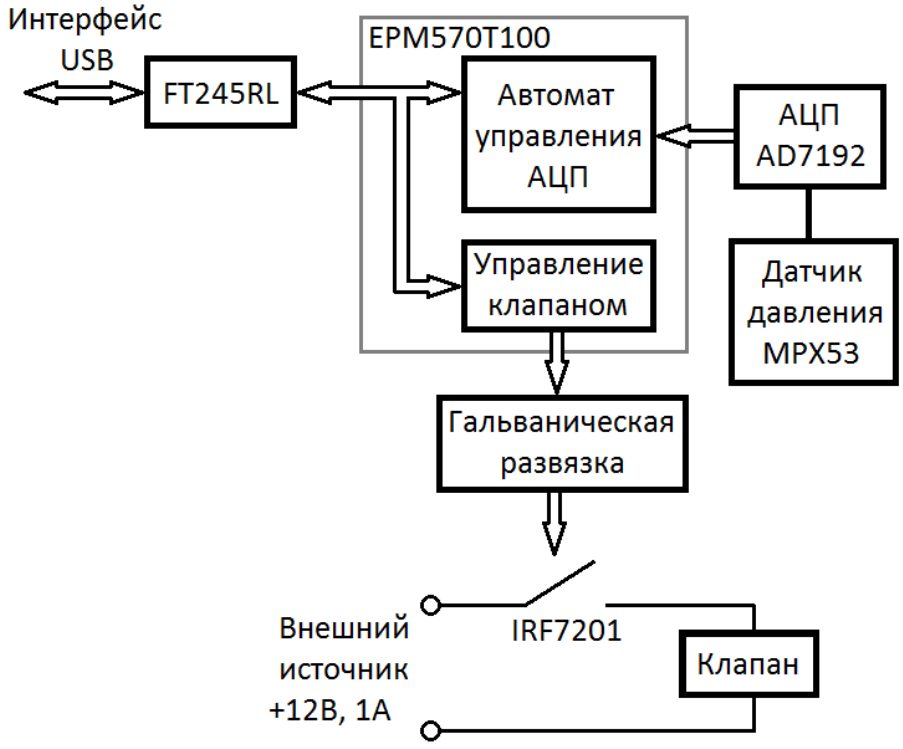


Рис. 1. Блок схема устройства MD245.

Устройство MD245 осуществляет снятие показаний с датчика давления MPX53GP (Freescale Semiconductor), встроенного в прибор для медико-физиологических исследований дыхания, состоящий из загубника, клапанной коробки с инспираторным и экспираторным клапанами, а также дополнительного электромагнитного клапана на входе инспираторного воздуховода (Рис. 2). Измерение давления в дыхательном тракте осуществляется с помощью сигма-дельта АЦП AD7192 (Analog Devices) с последующей выдачей цифрового результата по интерфейсу USB в компьютер.

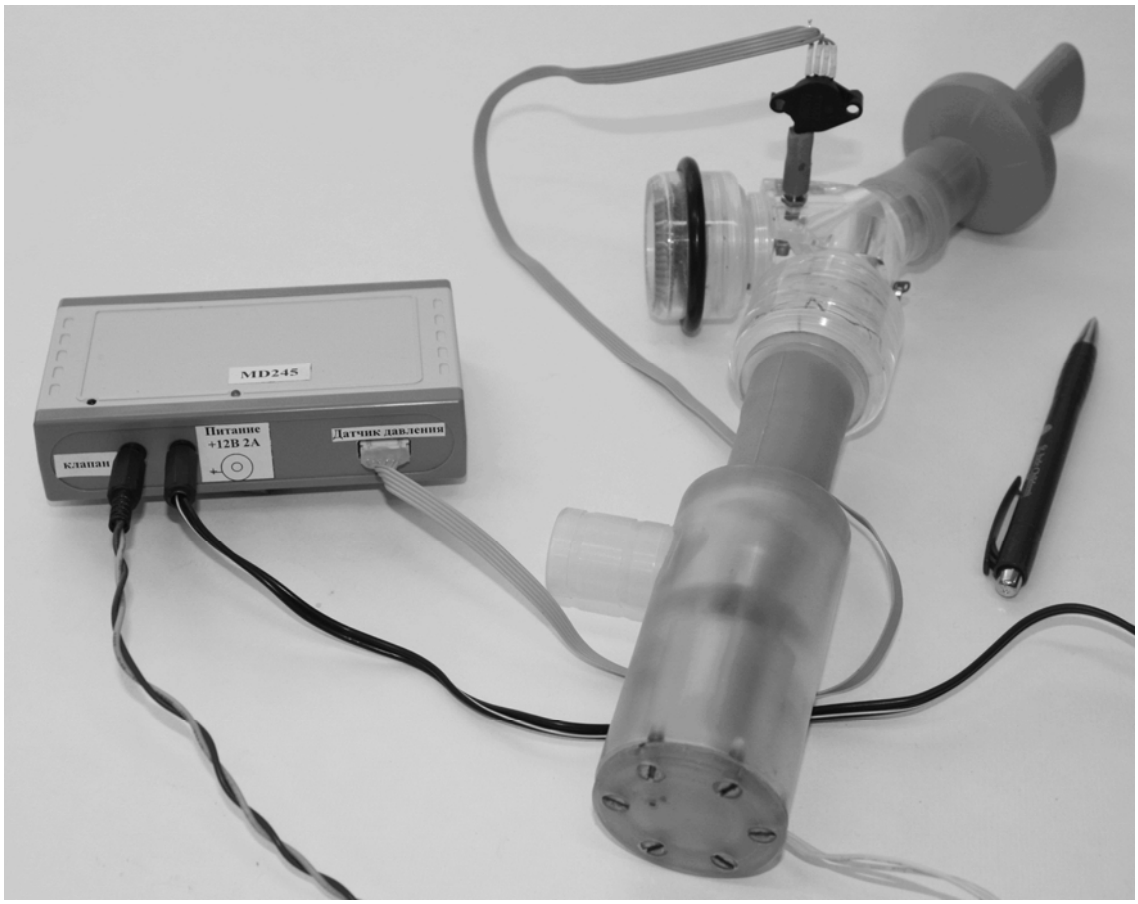


Рис.2. Внешний вид прибора для исследования дыхания с устройством MD245

Основным управляющим узлом устройства MD245 является программируемая логическая интегральная схема – CPLD EPM570T100 серии MAX II (Altera). Обмен данными с компьютером через интерфейс USB выполняют преобразователь USB↔FIFO, реализованный на микросхеме FT245RL (FTDI), и блок, преобразующий данные из буфера FIFO во внутренние команды, а также осуществляющий запись данных в буфер FIFO из устройства. Управление дополнительным электромагнитным клапанным механизмом перекрытия дыхательного тракта производится с помощью транзистора IRF7201 и гальванически развязано с остальной частью схемы.

Управление устройством MD245 осуществляется с помощью компьютера с интерфейсом USB 2.0 Full-Speed, для программирования необходим свободно распространяемый драйвер, например, (http://www.ftdichip.com/FTDrivers.htm).

Разработано программное обеспечение (программа Breathing), обеспечивающее на базе устройства MD245 регистрацию давления воздуха в дыхательном тракте, управление электромагнитным клапаном

перекрытия воздушного потока, графическое отображение регистрируемого давления во времени, определение различных временных параметров дыхательного цикла, а также вычисление индекса функционального состояния инспираторных мышц по формуле:

$$iTT = P_{0,1}/MIP \times T_i/T_t,$$

где $P_{0,1}$ - пиковая величина давления, развиваемого на фоне перекрытия дыхательного тракта в первые 100 мс после начала вдоха, MIP - максимальное инспираторное давление, T_i - продолжительность вдоха, T_t – общая продолжительность дыхательного цикла. Значения T_i и T_t определяются моментами пересечения текущего уровня измеряемого давления с заданным «нулевым» уровнем, задаваемым в интерактивном режиме экспериментатором.

На рис. 3 показан фрагмент графического поля экрана с общей картиной измерения инспираторного сигнала на всех этапах исследования.

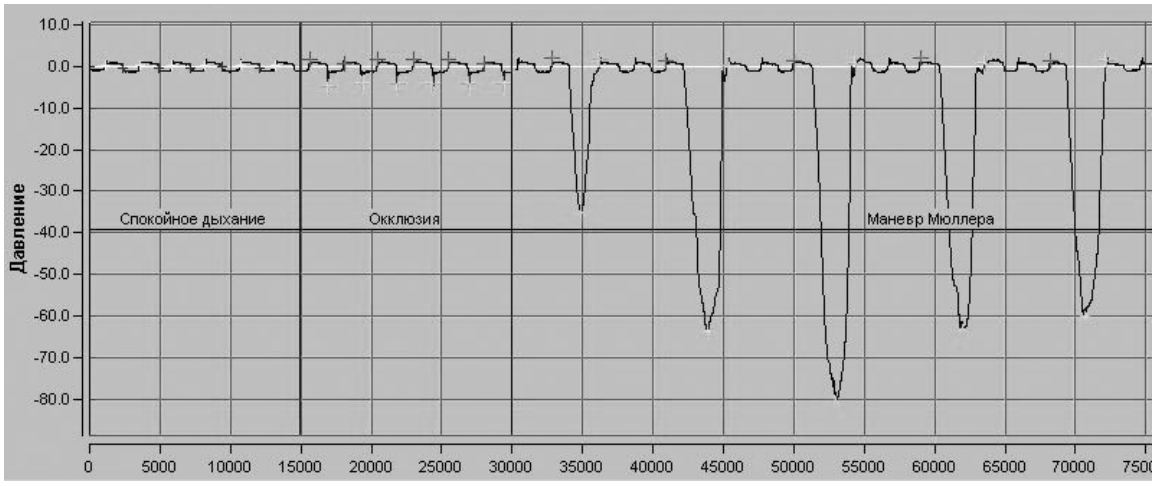


Рис.3 Фрагмент графического интерфейса программы

В графическом поле программы отображается входной инспираторный сигнал в соответствии с заданными этапами исследования дыхания - спокойное дыхание, дыхание с перекрытием. На этапе «дыхание с перекрытием» (окклюзия) программа выдает управляющие сигналы на клапанный механизм перекрытия инспираторного канала (через 50мс после начала выдоха клапан закрывается и через 100мс после начала вдоха клапан открывается). Во время так называемого маневра Мюллера клапан закрывается через 50 мс после начала выдоха, а открывается через 50 мс после достижения максимального давления в инспираторном канале. Затем проходят два дыхательных цикла (вдох - выдох) без перекрытия клапана и снова повторяется маневр Мюллера. На рисунке видны моменты закрытия и открытия клапана (крестики), перекрывающего инспираторный канал, моменты начала вдоха-выдоха, максимальное давление на вдохе во время маневра Мюллера. По общей картине изменения инспираторного сигнала экспериментатор определяет необходимость сохранения результатов измерения в базе данных для дальнейшей работы. Вместе с общей картиной измерения инспираторного сигнала целиком на всех этапах выводится таблица вычисляемых параметров.

Программное обеспечение для поддержки работы устройства разработано в среде Delphi v.6.0 с использованием библиотеки функций Windows API, графической библиотеки DirectX и компоненты SL Scope из свободно распространяемой библиотеки визуальных компонентов Mitov Software.

Проведенные испытания подтвердили возможность использования прибора в клинике для функциональной диагностики дыхания у больных с заболеваниями органов дыхания, а также для исследования дыхания у здоровых людей, занимающихся специфическими видами трудовой и спортивной деятельности.

Окрепилов М.В., Мешалкин М.А., Мешалкина М.Н.

КОМПЛЕКСНАЯ ОЦЕНКА ИЗМЕРЕНИЙ ФОРМАЛЬДЕГИДА В ВОЗДУХЕ ПОМЕЩЕНИЙ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

Здоровье, работоспособность и существование людей зависят от качества воздушной среды, в которой они проводят всю свою жизнь. Человек до 95% всего времени пребывает в закрытом помещении: место работы, транспорт, квартира, место отдыха или досуга. В настоящее время экологическая чистота и безопасность жилых и производственных помещений приобретает все более возрастающее значение в связи с широким использованием мало исследованных химических веществ для создания новых строительных и отделочных материалов. Качество воздушной среды определяется степенью ее загрязненности посторонними химическими веществами. Эти вещества поступают в воздушную среду в результате работы промышленных предприятий, транспорта и из других источников, а затем через вентиляционные системы зданий попадают внутрь жилых помещений. Здесь они смешиваются и вступают в реакции с веществами, образующимися в процессе жизнедеятельности организма человека, работы бытовых приборов, выделений из различных предметов, мебели, ковров. В итоге качество воздушной среды жилых помещений может оказаться значительно хуже, чем городского атмосферного воздуха. Эти проблемы можно перенести на любой замкнутый объем помещения.

Сравнительная оценка загрязнения воздуха вне и внутри помещений жилых и общественных зданий показала, что его уровень, как правило, в 2-4 раза выше в квартирах и офисах, чем на улице [1]. В лаборатории эколого-гигиенической оценки жилых и общественных зданий выявлено, что в атмосфере внутри домов могут одновременно присутствовать более 100 летучих химических веществ – формальдегид, фенол, бензол, оксиды азота и др.

Причины экологического неблагополучия внутри помещений известны – «химизация» строительства и бесконтрольное использование добавок в строительные материалы различных смесей вредных веществ. Губительное воздействие таких добавок проявляется не сразу – иногда через несколько лет. Они постепенно выделяют высокотоксичные и, в том числе, канцерогенные вещества.

Потенциально до 500 летучих органических соединений могут находится в воздухе помещений. Это в основном токсичные

органические соединения, выделяющиеся в воздух из синтетических покрытий, облицовок, обоев, ковров, клеев, мастик, лаков для мебели и полов.

Особые требования по качеству воздуха должны предъявляться к помещениям детских садов, школ, университетов и больниц. Однако в настоящее время не выработаны нормы по допустимым концентрациям для внутренних жилых помещений в зданиях. Поэтому ориентироваться приходится предельно допустимые концентрации (ПДК) загрязняющих веществ, установленных для атмосферного воздуха населенных мест.

1) Существует список летучих химических веществ, подлежащих обязательному контролю при проведении оценки санитарно-химического состояния воздуха закрытых помещений (Таблица 1) **[**2**]**.

Таблица 1

Некоторые химические вещества, подлежащие обязательному контролю

Химическое вещество	Допустимый уровень содержания в воздухе закрытых помещений, мг/м^3
Аммиак	0,04
Бутилацетат	0,1
Винилацетат	0,15
Дибутилфталат	0,05
Диоктилфталат	0,05
Метанол	0,5
Стирол	0,002
Формальдегид	0,035
Фенол	0,003
Этилацетат	0,1

Наиболее опасными для здоровья человека являются фенол, формальдегид, аммиак и метанол. На первом месте по использованию в различных материалах стоит формальдегид. Это вещество используется при изготовлении древесно-стружечных и древесно-волокнистых плит, мастик, пластификаторов, шпаклевки, смазок для бетонных форм и т.д. Измерению формальдегида в учебных помещениях Санкт-Петербургского политехнического университета посвящена данная работа. Исследовался на содержание в нем формальдегида не только воздух помещений, в которых проходят занятия, но и материалы, из которых изготовлена мебель, находящаяся в этих помещениях.

Формальдегид имеет формулу CH_2O, это бесцветный газ с резким раздражающим запахом, легко полимеризуется. Обладает общей токсичностью, раздражающе действует на слизистые оболочки верхних

дыхательных путей, глаз и кожных покровов. ПДК в атмосферном воздухе населенных мест: среднесуточная – 0,003 мг/м^3, максимально разовая – 0,035 мг/м^3, в воздушной среде рабочей зоны - 0,5 мг/м^3 относится ко 2-му классу опасности. Для воздушной среды помещений рекомендуется норматив в 0,01 мг/м^3[3]. Внесен в список канцерогенных веществ, обладает хронической токсичностью, негативно воздействует на генетический материал, репродуктивные органы, дыхательные пути, глаза, кожный покров. Оказывает сильное действие на центральную нервную систему.

Формальдегид в помещения поступает в основном из мебели, которая изготавливается на основе древесно-стружечных плит с добавлением формальдегидных смол.

Полимерные материалы, из которых изготавливается мебель, должны подвергаться санитарно-химической оценке, и должны удовлетворять следующими требованиями:

1. полимерные материалы не должны создавать в помещении специфического запаха;

2. полимерные материалы не должны выделять в окружающую среду летучие вещества в таких количествах, которое может оказывать прямое или косвенное неблагоприятное воздействие на организм человека.

В случае установления факта выделения вредных веществ из полимерных материалов в концентрациях, превышающих допустимые уровни, этот материал бракуется на стадии предупредительного санитарного надзора.

Целью санитарно-химических исследований полимерных материалов является качественное и количественное определение вредных летучих веществ, выделяющихся из них в воздух. Эти исследования проводят в моделируемых (лабораторных) и натурных условиях [4].

Для исследования используются специальные климатические камеры с регулированием температуры. В камеру помещается исследуемый образец мебели из расчета 1м^2 образца на 1м^3 камеры, края образцов, не закрытые полимерным материалом, заклеиваются алюминиевой фольгой силиконовым клеем. Образец выдерживается в камере в течение 3-х суток при температуре 40 ^{o}C. Затем из камеры отбираются пробы и анализируется на содержание формальдегида. Методы измерения содержания формальдегида – хроматографический, инфракрасный и фотометрический.

Из этих методов наиболее простым в реализации является фотометрический метод с ацетилацетоновым реактивом. На него существует стандартизованная методика [5]. В лабораториях СПбГПУ

есть спектрофотометр, на котором можно производить измерения, посуда и химические реактивы, а так же термостат и эксикатор, которые можно использовать как климатическую камеру.

Главной целью работы является измерение содержания формальдегида в воздухе учебных помещений, а также испытание образцов мебели на экологическую безопасность материалов, из которых они изготовлены.

Для достижения этой цели необходимо были решить следующие задачи:

- провести процедуру проверки фотометрической шкалы спектрофотометра по контрольным светофильтрам;
- построить градуировочную характеристику зависимости концентрации формальдегида от оптической плотности для спектрофотометра с помощью стандартных образцов состава формальдегида;
- собрать лабораторную установку для отбора проб воздуха из помещений и из камеры с образцами мебели;
- провести пробоотбор воздуха из помещений и сравнить полученные результаты с нормативами;
- произвести испытание образцов мебельных материалов в климатической камере, что позволит провести комплексную оценку безопасности газовыделений формальдегида в воздух помещений.

Проверка правильности показаний спектрофотометра проходила при выполнении всех пунктов методики его поверки с применением светофильтров, измеренные параметры не выходили за пределы заданных параметров.

Градуировочная характеристика проводилась с помощью стандартных образцов содержания формальдегида различных концентраций.

Для отбора проб была собрана установка на основе термостатируемого шкафа, герметичного эксикатора и поглотителей Полежаева, изображенная на рис. 1.

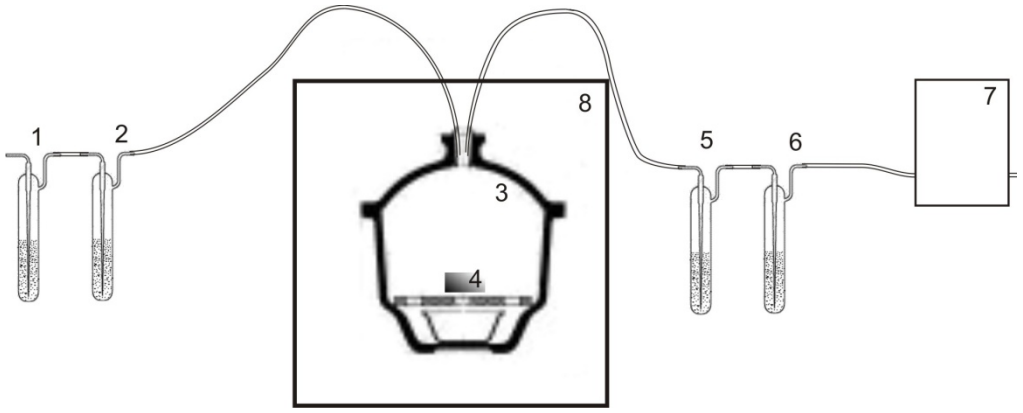


Рис.1 Установка для отбора проб:1, 2, 5, 6 – поглотители Рихтера; 3 – эксикатор, 4 – исследуемый образец; 8 – термостат; 7 – аспиратор

Подготовленный образец помещался в испытательную камеру таким образом, чтобы площадь образца соответствовала объему камеры в соотношении $1м^2/1м^3$. Образец при статических условиях находился в герметически закрытой камере в течение 3-х суток при температуре 40 ^oC. Затем отбирался десятикратный объем воздуха из камеры с помощью аспиратора в поглотители Полежаева (5 и 6 на рис.1), заполненные поглотительным раствором. В процессе подготовки пробы образуется нелетучее производное формальдегида. Одновременно отбиралась контрольная проба воздуха, подаваемого в климатическую камеру в поглотители Полежаева 1и 2 на рис.1. Отобранные пробы помещались в кюветы и проводились измерения оптической плотности на спектрофотометре при длине волны 412 нм. Измерение содержания формальдегида в пробе проводили с использованием градуировочной характеристики на спектрофотометре. Нижний предел обнаружения формальдегида при применении данного метода составляет 0,001 $мг/1м^3$, погрешность определения ±10%.

Результаты измерений формальдегида при испытании одних и тех же образцов мебельных материалов в статическом режиме менялись в разных опытах от 0,016 до 0,035 $мг/м^3$, что можно объяснить неравномерным распределением формальдегидной смолы по плите мебельного материла. Результаты измерений газовыделений формальдегида в испытанных образцах мебели, не превысили санитарные нормативы.

В учебной лаборатории университета, в которой была новая мебель, образцы которой испытывались, проводились регулярные измерения концентрации формальдегида в разное время. Концентрация формальдегида менялась от минимальной 0,002 $мг/м^3$ в проветренном помещении до максимальной 0,043 $мг/м^3$ в летний период в жаркую

погоду в закрытом помещении после длительного летнего отпуска. Насыщенность мебелью в данном помещении составила максимальное значение – примерно 1 $м^2/м^3$: при объеме помещения 168,7 $м^3$ площадь мебельных поверхностей составила 175,6 $м^2$.

Кроме измерений на содержание формальдегида в помещениях университета, авторами были проведены аналогичные исследования в помещениях детских садов Санкт-Петербурга, данные измерений приведены в Таблице 2.

Таблица 2

Результаты измерений формальдегида в помещениях детских садов

Место измерения	Концентрация формальдегида, $мг/м^3$
Детский сад №29 Выборгского района	0,008
Детский сад №32 Василеостровского района	0,004
Детский сад N26 Василеостровского района	0,008
Детский сад N20 Петроградского района	0,016
Детский сад N20 Адмиралтейского района	0,009

В помещениях детских садов, где находилось небольшое количество мебели, купленной давно, содержание формальдегида в воздухе значительно ниже норматива.

Проведенные исследования показали, что закупленная для университетских помещений новая мебель с точки зрения санитарно-химических требований является удовлетворительной по газовыделению формальдегида в воздух. При правильной эксплуатации вентиляционных систем и соблюдению норм по не превышению насыщенностью помещений мебели в соотношении 1 $м^2$ поверхности мебельных поверхностей на 1 $м^3$ объема помещений, содержание формальдегида в воздухе таких помещений является безопасным для здоровья.

Литература

1. Майоров В.А. Запахи. Их восприятие, воздействие, устранение. М.: Мир, 2006, 365 с.

2. ГН 2.1.6.1338-03. Предельно допустимые концентрации загрязняющих веществ в атмосферном воздухе. М., ИПК Издательство стандартов, 2001.
3. Другов Ю.С., Конопелько Л.А., Попов О.Г. Контроль загрязнения воздуха жилых помещений, офисов, административных и общественных зданий. – СПб: Наука, 2013-302 с.
4. ГОСТ 16371-93. Мебель. Общие технические условия. М., ИПК Издательство стандартов, 2003.
5. ГОСТ 30255-95. Мебель. Древесные и полимерные материалы. Метод определения выделения формальдегида и других вредных летучих химических веществ в климатических камерах. М., ИПК Издательство стандартов, 2001.

Полонский Ю.З., . Холявин А.И.

ЗАЩИТА ОТ ОШИБОК ИЗМЕРЕНИЙ ПРИ РАСЧЕТАХ И ФАНТОМНОМ МОДЕЛИРОВАНИИ В СТЕРЕОТАКСИЧЕСКИХ ОПЕРАЦИЯХ С ПОМОЩЬЮ МАНИПУЛЯТОРОВ КЛАССА ОРЕОЛ

Институт мозга человека им. Н.П. Бехтеревой РАН, С.-Петербург

Стереотаксис - наукоемкая медицинская технология, обеспечивающая малотравматичные нейрохирургические доступы к глубоким образованиям головного мозга человека с целью диагностики, лечения и изучения сложных заболеваний центральной нервной системы. В стереотаксических методиках погружение стереотаксического инструмента в мозг оперируемого больного производится (по предварительным расчетам) через отверстие малого диаметра с помощью специальных (стереотаксических) аппаратов или манипуляторов. Показаниями к стереотаксическим вмешательствам являются самые разнообразные патологические процессы: паркинсонизм, опухоли мозга, внутримозговые кисты и абсцессы, эпилепсия, двигательные нарушения в виде гиперкинезов и т.д.

Обязательным и во многом определяющим этапом стереотаксической процедуры является расчетная нейровизуализация (интраскопия), роль которой заключается в определении положения (локализации) целевых зон мозга и получении пространственной информации, необходимой для наведения стереотаксического инструмента на эти зоны. В настоящее время для предоперационной визуализации внутримозговых мишеней применяются, как правило,

различные виды томографии (МРТ, МСКТ, ПЭТ/КТ - см. доклад Холявин А.И., Полонский Ю.З.).

Очевидно, что цена ошибки при операциях на глубоких образованиях мозга очень высока и что стереотаксические методики должны включать в себя надежную систему защиты от грубых ошибок. Эти ошибки могут быть самой различной природы. Так, например, существуют ошибки, одинаковые для всех видов интраскопии, связанные с неверным съемом данных или с их неверным переносом с одного носителя информации на другой; ошибки, порождаемые ложным распознаванием и, соответственно, ложной локализацией внутримозговых ориентиров и мишеней на томограммах мозга. Существуют ошибки, специфичные для каждого вида интраскопии. Например, ошибки, вызванные неверной маркировкой лицевой стороны рентгеновской пленки, или ошибки, возникающие в результате непроизвольных движений головы пациента во время расчетного МРТ-исследования.

«Классический» рамный стереотаксис предполагает использование на всех этапах процедуры стереотаксической рамы (основания) манипулятора, жестко фиксируемой к голове пациента посредством острых винтовых упоров. При этом рама стереотаксического аппарата является основой для построения трехмерной (чаще всего прямоугольной) системы координат, в которой определяют положение целевых точек мозга. Отличительной особенностью манипуляторов класса ОРЕОЛ является способ наведения стереотаксического инструмента на целевые точки мозга, основанный на использовании съемных стереотаксических локализаторов, и программное обеспечение, переводящее координаты целевых точек и внутримозговых ориентиров из внутренней системы координат томографа в системы координат, построенные по меткам локализаторов «Ореола» [1]. Локализаторы - легкие съемные устройства, воспроизводимо фиксируемые относительно черепа оперируемого пациента с помощью оттиска его зубов.

Каждый из разработанных методов расчетной интраскопии в своей расчетной составляющей содержит блок контрольных вычислений, который, по нашему мнению, является обязательной компонентой любой системы стереотаксических расчетов. Назначение блока – защита от возможных грубых ошибок.

Проводимые заблаговременно до операции контрольные вычисления при расчетной томографии: а) по томографическим координатам вычисляются расстояния между метками МРТ (КТ) локализатора и выводятся в отдельном контрольном окне на экран монитора. Оцениваются отклонения вычисленных расстояний от измеренных; б) в последние модели универсального локализатора

введена дополнительная контрольная метка, координаты которой в системе координат локализатора известны и могут быть заново вычислены по томографическим измерениям; в) вычисляются координаты целевых точек в комиссуральной системе координат мозга пациента. Их примерное расположение нам известно из стереотаксических атласов; г) вычисляется и оценивается межкомиссуральное расстояние (диапазон допустимых расстояний известен).

Непосредственное наведение стереотаксического инструмента происходит при помощи так называемого фантомного моделирования [2]. На черепе больного с помощью жестких винтовых упоров крепится основание манипулятора. Больной прикусывает зубной оттиск с закрепленным на нем «рентгеновским» локализатором (зубной пластиной). По расчетам на (фантомной плите манипулятора) создается физическая (механическая) модель внутримозгового пространства, содержащая: имитатор основания стереотаксического манипулятора, закрепленного на голове пациента, точки, имитирующие метки локализатора, фиксированного на зубах пациента, и точку (перекрестие), имитирующую целевую. Взаимное расположение основания манипулятора и меток локализатора определяется механически с помощью специального устройства. Направляющее устройство манипулятора (выполненное в виде изоцентрической дуги) устанавливается на имитатор основания, после чего, используя поступательные степени свободы направляющего устройства, конец стереотаксического инструмента подводят к имитатору целевой точки и фиксируют в этом положении. Таким образом, изоцентр дуги направляющего устройства совпадает с перекрестием на фантоме, имитирующим целевую точку. После этого направляющее устройство переносится на основание манипулятора на голове пациента. Стереотаксический инструмент через фрезевое отверстие погружается в мозг до достижения изоцентра дуги, соответствующего положению целевой точки.

Ошибки на этапе моделирования, как правило, связаны с неправильным выставлением имитаторов на базовой плите фантома в соответствии с расчетными координатами. При обязательном механическом контроле расстояния между имитаторами меток рентгеновского локализатора сверяются с реальными расстояниями между метками. С помощью специального механического устройства периодически проверяется целостность механической сборки фантома.

Своеобразной комплексной защитой от непредвиденных ошибок является возможность использования внутримозговой системы координат пациента во время фантомного моделирования на операции.

Защитой служит «наглядность», заключающаяся в возможности визуального сопоставления построенной на фантомной плите модели внутримозгового пространства, содержащей имитаторы основания аппарата и имитаторы меток локализатора, и головы оперируемого.

И, наконец, сама конструкция манипулятора и применяемый способ наведения стереотаксического инструмента защищают нейрохирурга от измерительных ошибок в момент погружения инструмента в мозг. Направляющие стереотаксического манипулятора не имеют шкал, а во время (финального) погружения стереотаксического инструмента в целевую зону мозга отсутствуют какие либо измерительные манипуляции. Благодаря использованию изоцентрической дуги, независимо от расположения целевой точки, инструмент погружается в мозг до упора (с помощью ограничителя глубины).

Литература:

1 Полонский, Ю.З. Безрамная расчетная магнитно-резонансная томография со стереотаксическими манипуляторами класса «Ореол» / Ю.З. Полонский, А.И.Холявин, Б.В. Мартынов, В.Е. Парфенов, Г.Е. Труфанов // Вестник Российской Военно-медицинской академии. – 2009. – № 4(28). – С.71-78.

2 Патент РФ № 2130759, МКИ А61 в 6/00. Способ наведения стереотаксического инструмента на целевую точку // Авт. изобрет. Аничков А.Д., Полонский Ю.З., Низковолос В.Б., Трофимова Т.Н. - Опубл. – 27.05.1999, Бюл. 25.

[1]Прошкин В.Н., [1]Прошин И.А., [2]Прошкина Л.А.

МАГНИТОСТРИКЦИОННЫЙ ПРЕОБРАЗОВАТЕЛЬ УГЛОВЫХ ПЕРЕМЕЩЕНИЙ НА КРУТИЛЬНЫХ МАГНИТОУПРУГИХ ВОЛНАХ
MAGNETOSTRICTIVE TRANSDUCER ANGULAR DISPLACEMENT ON THE TWISTING MAGNETOELASTIC WAVES

[1]Пенза, ФГБОУ ВПО «Пензенский государственный технологический университет»
[2]Пенза, ФГБОУ ВПО «Пензенский государственный университет»

Проведен анализ современных магнитострикционных преобразователей угловых перемещений. Выявлены недостатки и предложены пути их устранений.

The analysis of modern magnetostrictive transducers angular movements. Identified weaknesses and suggests ways to address them.

Существенный интерес многих инженеров-разработчиков и производителей различных систем контроля и управления, сконцентрирован на магнитострикционных преобразователях угловых перемещений [1].

Мировым лидером в области разработки и производства новейших конструкций магнитострикционных измерительных преобразователей (ИП) параметров движений является фирма MTS Sensors, выпускаемых под брендом Temposonics [1, 2]. Актуальность таких преобразователей в системах управления во многом обусловлена не только возможностью работать в жестких условиях (вибрация, тряска, агрессивные среды, перепады температур и т.д.), но и их физической природой, конструктивными и функциональными особенностями, являющимися следствием базового измерительного принципа. Фирма MTS Sensors наладила выпуск преобразователей угловых перемещений, выполненных в различных конструктивных модификациях на основе спиралеобразных, U-образных, C-образных и O-образных волноводов [1].

Рассмотренные технические решения имеют существенный недостаток, который необходимо учитывать при разработке, изготовлении и эксплуатации выпускаемых изделий. Измерительный диапазон, длина паразитной «мертвой» зоны, наблюдаемая в районе узла считывания и характеристика нелинейности зависят от вида размещения волновода в корпусе ИП [2]. Для компенсации внутренних напряжений в волноводе и исключения образования в его рабочем пространстве интерферирующих магнитоупругих волн, волновод устанавливается с определенными продольным и радиальным механическими напряжениями. Величина напряжений выбирается исходя из диаметра, длины и материала волновода. Для уменьшения провиса волновода дополнительно вводят систему внутренних и внешних канальных опор. Только при соблюдении этих условий можно добиться высоких метрологических и эксплуатационных характеристик изделия. Поэтому известные преобразователи способны эффективно работать только при больших радиусах кривизны сенсорного волновода.

Для устранения указанных выше недостатков предлагается иное решение данной проблемы. Так как ИП определяет большую часть метрологических и эксплуатационных характеристик, предлагается измерительную систему выполнять линейной, а магнитную систему позиционирования криволинейной, например, в виде геликоиды.

В работе [3, 4] приведен один из вариантов геликоидальной магнитной системы позиционирования и технология его изготовления. Там же показан принцип формирования магнитоупругих волн в линейном акустическом осцилляторе.

Проведенный анализ и экспериментальные исследования разработанного способа и магнитострикционного преобразователя угловых перемещений показали, что, в сравнении с другими методами угловых измерений, он обладает следующими преимуществами: технологичность, малые габаритные размеры, высокая точность, линейность, надежность.

Список литературы

1.Сысоева С.С. Автомобильные датчики положения. Современные технологии и новые перспективы. Часть 13. Магнитострикционные преобразователи – актуальные измерители линейных и нелинейных перемещений и детекторы крутящего момента. Компоненты и технологии № 6 (№ 59). 2006. С. 92-103.

2.Прошкин В.Н. Конструкторско-технологические способы совершенствования магнитострикционных преобразователей линейных перемещений для специальных условий эксплуатации: дис…канд. техн. наук. – Астрахань, 2007. – 173 с.

3.Патент RU 2343645 МПК: H04R 15/00, G01B 17/00. Магнитострикционный датчик перемещений /А.Н. Дигузов, А.Н. Шеркутов, В.Н. Прошкин// Опубл. 10.01.2009. – Бюл. № 1.

4. Прошкин В.Н., Прошин И.А., Прошкина Л.А. Способ детектирования угловых перемещений на магнитострикционных эффектах с геликоидальной магнитной системой позиционирования. //Естественные и технические науки. 2013. № 6 (68). С. 342-347.

Ткачева Т.А.

ПРОЦЕССНОЕ ИССЛЕДОВАНИЕ НАПРАВЛЕНИЙ РАСШИРЕНИЯ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ И ПОВЫШЕНИЯ ТОЧНОСТИ МОСТОВЫХ RC-ПРЕОБРАЗОВАТЕЛЕЙ ШИРОКОГО НАЗНАЧЕНИЯ (БОРТОВЫХ АВТОТРАНСПОРТНЫХ ЭЛЕКТРОННЫХ СИСТЕМ)

Московский государственный машиностроительный университет (МАМИ)

В настоящее время в различных электронных устройствах информационных бортовых системах на автотранспорте промышленного назначения (ИБС АПН) как отечественных, так и зарубежных широко используется частотные сигналы. Т.е. мы имеем массовое применение мостовых RC-преобразователей различной мощности в измерительных, управляющих и силовых цепях АПН, эксплуатируемых на 55-65% в ненормированных режимах. Это и определяет повышенные требования к их надёжности, метрологическим и эксплуатационным показателям и характеристикам в современных условиях.

Обзор научно-технических и литературных источников и технических результатов промышленных экспериментов показал перспективность применения мостового RC-преобразования, обладающего рядом важных свойств (сочетанием прецизионной точности, высокой чувствительности и надёжности); а для задач контроля, наблюдений и измерений расширенными возможностями согласованного включения любых новых датчиков физических величин.

Разработанные в МАМИ и используемые новые: схемно-технические решения по мостовым экспоненциальным RC-преобразователям, включающие различные по качеству нуль-органы (например, прецизионные операционные усилители (ПОУ) в модифицированных схемах, дополнительные обратные связи с элементами стабилизации и др.); способы их использования для управления устройствами; аналитические и статистические методы оценки фактических и предельных параметров мостовых схем – в целом дают возможность снизить основную погрешность мостового RC-преобра-зования в несколько раз за счёт учёта и коррекции влияния дестабилизирующих факторов, всегда сопровождающих эксплуатацию ИБС АПН. Кроме того, для повышения эффективности мостового RC-преобразования предложена новая методика точного нормирования, в которой используют свободные аналитический и статистический

алгоритмы обработки данных по показателям эксплуатации мостовых RC-преобразователей в различных динамических режимах.

Фрагмент схемной реализации мостового RC-преобразования представлен на рис. 1.

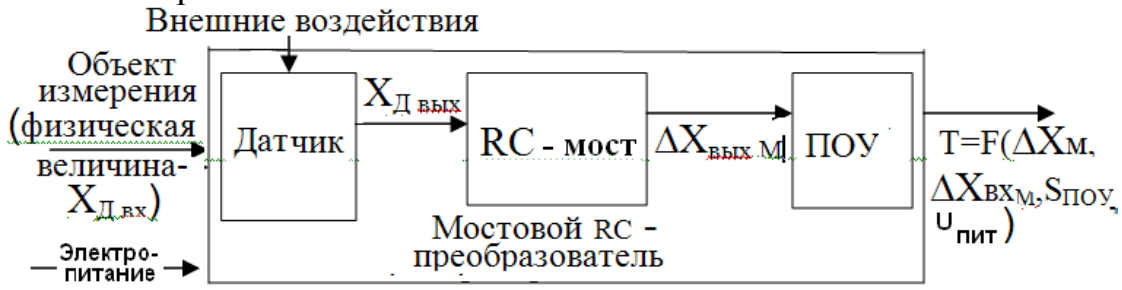
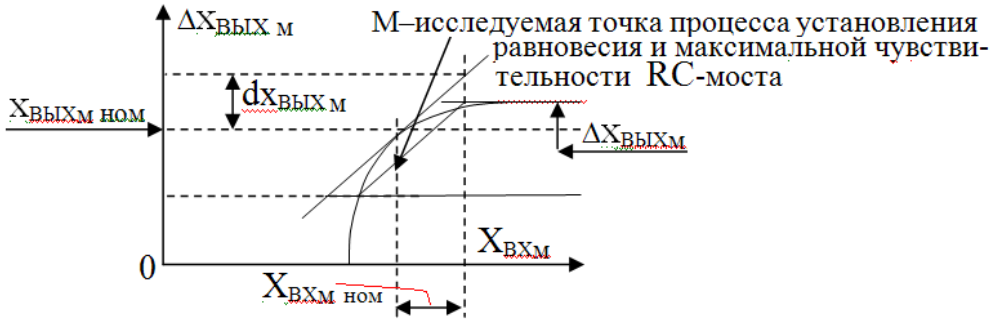


Рис. 1. Обобщённая схема мостового RC-преобразования

Получаемые на выходе периоды следования импульсов T есть сложные функции мостового RC - преобразования и изменчивости характеристик схемы включения, свойств и работы ОУ. Любые изменения в режимах работы RC-моста и ОУ приводят к смещению исследуемой точки равновесия (рис. 2). Поэтому необходима их коррекция и стабилизация. Прямая зависимость справедлива только на некотором интервале, вблизи точки М, где устанавливается равновесие.



где $X_{вхм\ ном}$ – номинальное значение $X_{вхм}$; $\Delta x_{выхм}$ – оценка абсолютного отклонения $\Delta x_{выхм}$; $dx_{вых\,м}$ – оценка полной погрешности выходного сигнала RC – моста.

Рис. 2. Графическое исследование установления равновесия RC – моста

Чувствительность мостового RC - преобразования для обобщённой схемы, представленной на рис. 1 определяется как

по дифференциалу $S_d = dX_{вых\,м} / dX_{д\,вх}$, (1)

по приращению $S_\Delta = \Delta X_{вых\,м} / \Delta X_{д\,вх}$, (2)

При этом важно отметить, что увеличение чувствительности моста происходит тогда, когда $\Delta X_{д\ вх}$ стремится к бесконечно малой величине. Параметры системы «Д - RC-мост – ПОУ» и режимы работы метрологически строго согласованы по чувствительности, возникающим погрешностям и т.д.

В настоящее время определение чувствительности и точности изменчи-вости сложных функций многих переменных, что характерно для мостового RC - преобразования, составляющих основу свободной алгоритмизации и программирования прецизионных процессов функционирования данного вида преобразования измеряемых величин, ведётся на основе методов, использующих математический аппарат частных производных, подробно разработанных С.В. Ковалевской. Для такого вида МИС, функционально представляемые сложными функциями многих переменных, при решении удобно переходить от дифференциалов к приращениям (1-2), а значить иметь возможность точнее рассчитывать погрешности и чувствительность бесконечно малых отклонений при измерении требуемых для ИБС АПН физических величин. В новый аналитический алгоритм включены уточненные модели всех возникающих типов погрешностей мостовых схем, которые реализуют косвенный метод измерения и предложены режимы работы, улучшающие их метрологические характеристики [1,2].

Кроме того, в работе используется свободное программное обеспечение для статистических исследований. А, именно, разработанный статистический алгоритм включает: расчёты полной совокупности статистических параметров мостового RC-преобразования (например, периода следования и длительности и формы импульсов, амплитуды и др.) и исследование закономерностей их распределения (так, изменчивость ΔT распределяется по N-закону, с минимальной дисперсией $D(\Delta T) \rightarrow \min$ и некоторой асимметрией). Но заметим, что всё же статистические методы не дают значительного повышения точности, т.к. в них обработка ведётся данных ограниченной точности, определяемой метрологическими возможностями всех составляющих.

Всё указанное выше определяет новое развитие методологии совместного применения аналитических и статистических исследований и перспективы применения современного мостового RC-преобразования, погрешность которого по результатам экспериментальных исследований, проведенных на информационных бортовых системах на автотранспорте промышленного назначения за последние годы составила менее 0,005%. Итак, мостовые экспоненциальные RC-преобразователи могут служить и высокоточным временным или частотным сигналом, который может быть широко использован в системах управления широкого назначения в

различных отраслях промышленности (автопрома, машиностроении, приборостроении, энергетике, горной отрасли, металлургии и др.) [2].

Список использованной литературы

1. Ткачева Т.А. Методология прецизионности оценки метрологических показателей ЦИИС наноразмерного диапазона, обеспечивающих надёжность АИМ. МК и выставка «ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ И ЕЕ ПРИМЕНЕНИЕ». Март 2009. г. Москва. Труды НТО РЭС им. А.С.Попова. Выпуск: IX-2. - 2009. С. 550-553.

2.МИ 1730-87 Государственная система обеспечения единства измерений. Погрешности косвенных измерений характеристик процессов. Методика расчёта.

Холявин А.И., Полонский Ю.З.

ПРЕИМУЩЕСТВА ИЗМЕРЕНИЙ НА СОВМЕЩЕННЫХ ИЗОБРАЖЕНИЯХ ГОЛОВНОГО МОЗГА ПРИ ПРЕДОПЕРАЦИОННОМ СТЕРЕОТАКСИЧЕСКОМ ПЛАНИРОВАНИИ

Институт мозга человека им. Н.П. Бехтеревой РАН, С.-Петербург

Послойные изображения головного мозга пациентов, получаемые при помощи томографов (сканеров), во многих случаях позволяют получить ценную диагностическую информацию о патологических изменениях структуры и функций мозга и тем самым дают возможность определить тактику дальнейшего лечения. Наиболее часто в диагностике используют рентгеновскую компьютерную (КТ), магнитно-резонансную (МРТ) и позитронно-эмиссионную томографию головного мозга (ПЭТ).

В то же время, диагностические возможности перечисленных видов томографии существенно отличаются друг от друга. При этом, как правило, невозможно выбрать из разных видов диагностики один, наиболее информативный: каждый из них отражает лишь какую-то часть патологических изменений, и лишь комплексный анализ нескольких видов изображений мозга различных модальностей дает возможность составить полноценное представление о состоянии мозга пациента.

В этой ситуации, повысить информативность исследования позволяет совмещение («fusion») изображений, представляющее собой способ постпроцессинговой обработки томографических срезов мозга. Во многих случаях совмещение срезов на одном изображении выявляет как морфологические, так и функциональные изменения в организме пациента. Кроме того, совмещение томограмм головного мозга, полученных при нескольких видах исследований, может использоваться

при подготовке малотравматичных стереотаксических вмешательств на мозге.

Стереотаксические операции выполняются с использованием специальной аппаратуры – стереотаксических манипуляторов, и позволяют прицельно выполнять хирургические воздействия в глубинных зонах мозга, недоступных при обычных нейрохирургических операциях. Стереотаксический метод может использоваться для биопсии или многопозиционной деструкции опухолей мозга, а также для лечения некоторых других заболеваний центральной нервной системы. Точное попадание в целевые зоны мозга достигается благодаря измерениям, проводимым на дооперационных томограммах головного мозга пациента. В качестве реперных элементов для проведения измерений на томограммах используются точечные объекты - метки стереотаксического локализатора, закрепленного на голове пациента во время проведения томографии.

Наиболее часто используется совмещение изображений ПЭТ и КТ. ПЭТ, являясь чувствительным методом выявления метаболических изменений, не обладает высокой разрешающей способностью и не позволяет с достаточной точностью локализовать анатомические структуры. Эти недостатки компенсируются высокой анатомической точностью КТ. В некоторых случаях используется совмещение и других видов медицинских изображений – например, ПЭТ и МРТ, структурной и функциональной МРТ. Как правило, применяются специальные программы, использующие различные алгоритмы совмещения. В большинстве случаев используется совмещение объемных реконструкций мозга пациента с возможностью их «сечения» в различных направлениях и получения таким образом срезов, представляющих собой совмещенные изображения.

Например, ПЭТ, проводимая в предоперационном периоде, позволяет локализовать целевые зоны внутримозговой опухоли, избирательно накапливающие туморотропный радиофармпрепарат. Эти зоны характеризуются максимальной клеточной пролиферацией (скоростью деления клеток) и определяют рост новообразования. Прицельное взятие биоптата из этих зон позволяет более точно осуществить гистологическую диагностику, а их избирательное разрушение (например, криодеструкция) дает возможность остановить или замедлить рост опухоли и тем самым повысить показатели выживаемости пациентов.

В то же время, стереотаксическое планирование деструкций в глубинных и функционально значимых зонах мозга требует четкой анатомической визуализации церебральных структур, прилежащих к опухоли, чего не может обеспечить ПЭТ. Кроме того, необходимо

решать задачу планирования безопасных траекторий интраоперационного прохождения стереотаксической канюли через вещество мозга к целевым точкам опухоли. Для этой цели лучше всего подходит МРТ головного мозга. Наиболее точные результаты измерений положения реперных элементов локализатора, необходимых для прицеливания инструмента на выбранные структуры мозга во время операции, обеспечивает КТ.

При подготовке операций в клинике Института мозга совмещение МРТ, КТ и ПЭТ проводили на рабочей станции Philips с использованием программного пакета Philips IntelliSpace Portal (применяли опции Multimodality Viewer и Automatic registration). Такая методика позволила у всех пациентов успешно осуществить стереотаксическую деструкцию пролиферативно-активных зон опухоли без нарастания очаговой неврологической симптоматики, несмотря на локализацию новообразований в глубинных и функционально значимых зонах головного мозга.

Чащегоров П.С.

АЛГОРИТМ ЛОКАЛИЗАЦИИ ПОМЕХ В ЭЛЕКТРИЧЕСКИХ ЦЕПЯХ С ПРОИЗВОЛЬНЫМ КОЛИЧЕСТВОМ КОНТРОЛЬНЫХ УЗЛОВ

Санкт-Петербургский государственный политехнический университет

Воздействие помех на электрические цепи систем автоматического контроля и управления технологическими процессами может привести к нарушению их работы и к негативным последствиям для объекта управления [1,2]. При обнаружении воздействия помехи необходимо вывести управляемый объект в заведомо безопасное состояние и локализовать помеху.

Электрические цепи хорошо описываются математическими моделями (например, системами уравнений контурных токов и узловых напряжений, или графами), которые могут быть использованы для автоматизированного обнаружения места приложения помехи или неисправности. Задача локализации тем самым может быть сведена к поиску узла на модели цепи, к которому был подключен источник помехи.

Состояние систем управления технологическими процессами отслеживается по показаниям измерительной аппаратуры, подключенной в контрольных узлах схемы. Количество таких узлов и характер

получаемой измерительной информации от задачи к задаче разнятся [4]. Поскольку для повышения достоверности результата локализации помехи желательно использовать всю имеющуюся в наличии информацию, возникает вопрос о правилах и способах ее учета.

В работе [3] приведен алгоритм локализации помехи в электрической цепи по результатам измерений, выполненным в двух контрольных узлах, сводящий задачу локализации к задаче оптимизации.

В настоящей работе представлено обобщение данного алгоритма на случай большего числа контрольных узлов. Представлено обоснование вида целевого функционала, минимизацией которого достигается определение узла приложения помехи. Моделирование работы предложенного алгоритма выполнено в пакете Matlab на примере электрических цепей, чьи модели представлены в работах [5, 6]. Сделаны количественные выводы о достоверности результатов локализации помехи.

ЛИТЕРАТУРА

1. Khalid, S. Power quality issues, problems, standards & their effects in industry with corrective means / S. Khalid, B. Dwiveldi // International Journal of Advances in Engineering & Technology. – 2011. – N 2. – Pp. 1-11
2. Schipman, K. The importance of good power quality / K. Schipman. – ABB Power Quality Products, 2010. – 20 p.
3. Лысенко, Г. С. Локализация источников помех / Диссертация на соискание ученой степени кандидата техн. наук. — СПб: 2013, 100 с.
4. РД 153-34.0-15.502-2002. Методические указания по контролю и анализу качества электрической энергии в системах энергоснабжения общего назначения. Часть 2. Анализ качества электрической энергии.
5. Shin, Y.-J. Signal processing-based direction finder for transient capacitor switching disturbances / Y.-J. Shin, E. J. Powers, W. Mack Grady, A. Arapostathis // IEEE transactions on power delivery. – 2008. – N 4 – Pp. 2555- 2562.
6. Зернов, Н. В. Теория радиотехнических цепей / Н. В. Зернов, В. Г. Карпов / издание 2-ое, перераб. и дополн. – Л.: Энергия, 1972 – 816 с.

Богданов С.С., Козлов В.Н., Окрепилов М.В., Кимков В.Н.

БАЗОВАЯ КАФЕДРА КАК ПУТЬ РАЗВИТИЯ НАУЧНО-ПРОИЗВОДСТВЕННОГО ПОТЕНЦИАЛА ПРЕДПРИЯТИЯ

Санкт-Петербургский государственный политехнический университет

Впервые в Ленинградской области Институт информационных технологий СПбГПУ и ОАО «Завод Кризо», как представитель ВПК России создали базовую кафедру. Положившая начало сотрудничеству кафедра « Системный анализ и управление» (Зав. Кафедрой д.т.н., профессор В.Н.Козлов) с 2009 года сотрудничала с заводом «Кризо». На предприятии проходили производственная и учебная практика студентов, велись студенческие НИР, сотрудники завода активно поддерживали обучающихся в выполнении курсовых и дипломных работ по направлениям деятельности предприятия.

Теперь, согласно распоряжениям и договоренностям базовая кафедра является выпускающей и отвечает за подготовку дипломированных специалистов для предприятия и оказывает научно – методическую поддержку для осуществления подготовки и переподготовки по рабочим специальностям. Кафедра обеспечивает подготовку инженеров и других специалистов по специальностям, перечень которых устанавливается ежегодно совместным решением университета и предприятия. Кафедра, является основой для организации научно - образовательного Регионального ресурсного кадрового центра на базе Предприятия и призвана к организационному расширению и укреплению всесторонних связей университета с предприятием. В своей деятельности базовая кафедра руководствуется законами Российской Федерации «Об образовании», «О высшем и послевузовском профессиональном образовании», «Типовым положением о высшем учебном заведении», Уставом СПбГПУ, Уставом предприятия и Соглашением о сотрудничестве между Университетом и Предприятием. Все виды учебной работы Базовая кафедра проводит помещениях Университета и в учебно - лабораторных помещениях, выделенных Предприятием.

Кафедра «Управление безопасностью технических объектов» видит свою задачу в проведении всех видов учебных занятий по дисциплинам, закрепленным за нею учебными планами, руководство самостоятельными занятиями студентов, проведение текущего контроля знаний, курсовых экзаменов и зачетов, в том числе (см. схему 1):

Кафедра «Управление безопасностью технических объектов»

организация и проведение производственной и учебной практики студентов на заводе с использованием технологических возможностей предприятия;	руководство курсовым и дипломным проектированием;
руководство курсовым и дипломным проектированием;	обеспечение условий для проведение циклов лабораторных работ с использованием технологических возможностей предприятия;
чтение отдельных курсов по общеинженерной и экономической подготовке студентов соответствующих специальностей;	чтение специальных курсов, обеспечивающих конструкторско-технологическую подготовку и специализацию по профилю отрасли и предприятия.
Разработка программ целевой подготовки специалистов для предприятия по согласованным основным и дополнительным обязательным учебным программам, формируемым рабочей группой, состоящей из ведущих специалистов предприятия и преподавателей университета.	Оснащение учебных и совместных научно-учебных лабораторий по профилю предприятия для выполнения научных исследований, обеспечение учебного процесса и привлечения к научной работе студентов.
Организация работы по профориентации в средних общеобразовательных учебных заведениях с целью подбора талантливых и профессионально пригодных абитуриентов способных, в дальнейшем, работать на предприятии.	Организация подготовительных курсов для абитуриентов желающих поступать учиться в ИИТУ по целевому направлению предприятия, подтвержденному муниципальными органами.

Кроме того, работники кафедры предполагают свое непосредственное участие в разработке учебных планов подготовки специалистов, бакалавров и магистров по соответствующим направлениям, осуществлять своё влияние на подготовку и внесение изменений в учебные планы, разработанные на основе государственных образовательных стандартов.

Одной из учебно-методических задач видится подготовка учебников, учебных и методических пособий по дисциплинам кафедры, апробация и внедрение новых технологий обучения.

Повышение научно-производственного потенциала невозможно без постоянной работы с кадрами, поэтому:

1. переподготовка и повышение квалификации работников предприятия, переподготовка и повышение квалификации научно-педагогических кадров для нужд кафедры;
2. привлечение специалистов предприятия к преподавательской деятельности для разработки и чтения новых курсов;
3. поддержка и развитие научно-педагогических школ по профилю кафедры;
4. оказание научно – методической поддержки для осуществления предприятием подготовки и переподготовки по рабочим специальностям;
5. проведение научно-исследовательских и опытно конструкторских работ по заказам предприятия;
6. создание творческих коллективов для реализации совместных научно-исследовательских проектов вплоть до создания студенческих научных лабораторий;
7. содействие научно-исследовательской деятельности Университета путем привлечения экспериментальной и производственной базы предприятия для выполнения экспериментальной части научно-исследовательских работ;
8. обеспечение доступа к технологическому оборудованию предприятия преподавателей и научных сотрудников вуза, в том числе предоставлением его во временное пользование;
9. подготовка и тиражирование учебно-методической литературы с использованием издательской базы предприятия и университета;
10. проведение совместных научно-технических мероприятий (семинаров, конференций) по приоритетным научно-техническим направлениям. Организация совместных

научных и научно-методических публикаций;

11. сотрудничество с родственными кафедрами Института информационных технологий, Университета, других вузов, с профильными научными и образовательными учреждениями, организациями и предприятиями по всем видам деятельности кафедры;

12. проведение системной профессионально ориентационной работы в средних и средних специальных учебных заведениях с целью формирования будущего контингента студентов Института информационных технологий и кафедр, работающих по тематике близкой к направлениям деятельности предприятия;

13. проведение агитационной работы на Предприятии и родственных предприятиях отрасли с целью формирования контингента студентов и слушателей вечернего факультета и подготовительных отделений;

14. проведение мероприятий по обеспечению безопасности жизнедеятельности в соответствии с факультетскими и университетскими планами.

Это задачи, которые предстоит решать совместно администрации предприятия и работникам кафедры в самое ближайшее время.

СОДЕРЖАНИЕ

СЕКЦИЯ 1
АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

СЕКЦИЯ 2
МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

СЕКЦИЯ 3
ИЗМЕРИТЕЛЬНЫЕ ТЕХНОЛОГИИ