Министерство образования и науки Российской Федерации
Государственное образовательное учреждение
Высшего профессионального образования
Алтайский государственный технический университет
им. И.И.Ползунова

НАУКА И МОЛОДЕЖЬ – 2011

VIII Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых

СЕКЦИЯ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

подсекция

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Барнаул – 2011

УДК 004

VIII Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь – 2011". Секция «Информационные технологии». Подсекция «Вычислительные системы и информационная безопасность». / Алт. гос. техн. ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2011. – 61 с.

В сборнике представлены работы научно-технической конференции студентов, аспирантов и молодых ученых, проходившей 29 апреля 2011 г.

СОДЕРЖАНИЕ

ПРИМЕНЕНИЕ УЧЕБНЫХ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ПРАКТИЧЕСКОЙ НАПРАВЛЕННОСТИ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ПО НАПРАВЛЕНИЮ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Волков М.М. – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет (г. Барнаул)

В связи с переходом на двухуровневую систему образования – бакалавриат и магистратуру, меняется подход к образовательному процессу, в частности он является компетентностно - ориентированным и для бакалавриата характерна практическая направленность образовательного процесса. Выпускник по окончанию университета должен обладать общекультурными и профессиональными компетенциями. Профессиональные компетенции выпускника по направлению «Информационная безопасность» формируются в значительной части в ходе выполнения практических и лабораторных работ.

Однако специфика формирования профессиональных компетенций по данному направлению заключается в необходимости наличия объектов защиты информации с различными условиями обработки конфиденциальной информации, с помощью которых можно было бы формировать компетенции. Проблема допуска студентов к конфиденциальной или секретной информации предприятий г. Барнаула не позволяет в полной мере осуществлять формирование профессиональных компетенций на реальных объектах защиты информации.

Отчасти эта проблема решается за счет производственной и преддипломной практики студентов, но при проведении практических и лабораторных занятий возникают трудности обеспечения практической направленности образовательного процесса.

Согласно основной образовательной программы университета выпускник направления «Информационная безопасность» должен обладать профессиональными компетенциями и быть способным:

- формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.
- организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации.
- организовывать и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов.
- определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.
- участвовать в разработке подсистемы управления информационной безопасностью.

К проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.

- собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.
- проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов

Данные способности формируются в рамках лабораторных практикумов и практических занятий по дисциплинам: информационная безопасность предприятия (организации),

информационно-аналитическая деятельность по обеспечению комплексной безопасности, информационная безопасность автоматизированных систем, проверка информационной защищенности на соответствие нормативным документам, управление информационной безопасностью.

Одним из способов решения проблемы наличия реальных предприятий может быть их имитация – разработка учебных объектов защиты информации.

Объекты защиты информации представляют собой информацию, носители информации, информационные процессы. Кроме того в различных стандартах и нормативных документах под объектами защиты информации понимаются объекты информатизации, включающие автоматизированные системы различного уровня и назначения, сети и системы связи, средства отображения и размножения информации, помещения в которых происходит обработка информации и помещения для ведения конфиденциальных переговоров [1,2].

Данные объекты представлены в структуре виртуальных предприятий. Типовыми предприятиями являются предприятия, в информационных системах которых обрабатывается государственная, коммерческая тайна, персональные данные.

Для разработки учебных объектов защиты информации на основе факторов влияющих на организацию комплексной системы защиты информации были определены характеристики информационной безопасности необходимые для описания «макета» учебного объекта защиты информации [3]:

- форма собственности предприятия;
- организационная структура предприятия;
- характер основной деятельности предприятия;
- состав, объекты и степень конфиденциальности защищаемой информации;
- структура и территориальное расположение предприятия;
- степень автоматизации основных процедур обработки защищаемой информации.

Более детализированные характеристики учебных объектов защиты информации определяются на основе анализа требований законодательства РФ в области защиты той или иной тайны. Например, при защите персональных данных такими характеристиками являются:

- категории субъектов персональных данных;
- действия с персональными данными;
- способ обработки персональных данных;
- категория персональных данных;
- структура информационной системы и др.

Таким образом, в результате анализа характеристик учебного объекта защиты информации структура «макета» виртуального предприятия будет иметь вид, представленный на рисунке 1.

Указанные характеристики отражают всю необходимую информацию о предприятии с точки зрения проектирования (модернизации) системы защиты информации, они позволяют рассчитывать угрозы и риски информационной безопасности, оценивать уровень защищенности предприятия и определять требования по защите информации, то есть формировать профессиональные компетенции.

Комплекс разработанных учебных объектов защиты информации должен способствовать развитию профессиональных компетенций по направлению «Информационная безопасность» и планируется к внедрению на кафедре «Вычислительных систем и информационный безопасности» факультета «Информационных технологий» по

направлению подготовки «Информационная безопасность», а так же по специальности «Комплексная защита объектов информатизации».

Рисунок 1 – Структура виртуального предприятия

Список литературы

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. [электронный ресурс]. – http://www.fstec.ru/_razd/_isp0o.htm
2. ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [электронный ресурс]. – http://www.fstec.ru/_razd/_isp0o.htm
3. Комплексная система защиты информации на предприятии: учебник для студ. высш. учеб. заведений./ В.Г. Грибунин, В.В. Чудовский.- М.: Издательский центр «Академия», 2008.-320с.

РАЗРАБОТКА МЕТОДИКИ И ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ РЕЗУЛЬТАТОВ ПРОГРАММНОЙ РЕАЛИЗАЦИИ ВНЕДРЕНИЯ ЗАШИФРОВАННОЙ ИНФОРМАЦИИ В ГРАФИЧЕСКИЕ ОБЪЕКТЫ

Жаркова А.А. – студент, Ленюк С.В. – к.ф.-м.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Круг задач, решаемых в области защиты информации, постоянно расширяется. Растут требования к качеству их решения. Среди всего спектра методов обеспечения защиты информации в информационных системах особое место занимают криптографические методы защиты информации. В современных условиях методы традиционной криптографии в целом ряде задач становятся недостаточными, поскольку не позволяют сохранить в тайне сам факт передачи и/или хранения информации, ее объем и источник. С созданием глобальных телекоммуникационных сетей и образованием цифровой информационной среды подобные проблемы стало возможным решать методами компьютерной стеганографии, позволяющими скрытно внедрять дополнительную информацию в компьютерные данные, представляющие собой различные файлы, программы, пакеты протоколов.

Компьютерная стеганография – активно развивающееся направление в области информационной безопасности. Для решения стеганографических задач, среди которых сокрытие самого факта передачи и/или хранения конфиденциальной информации, применяются известные и разрабатываются новые методы. Задача сокрытия конфиденциальной информации с применением стеганографических методов сводится к разработке стеганографической системы, устойчивой к атакам. Как правило, профессионально разработанная стеганографическая система обеспечивает трехуровневую модель защиты информации, решающую две основные задачи [1]:

– скрытие самого факта наличия защищаемой информации (первый уровень защиты);

– блокирование несанкционированного доступа к информации, осуществляемое путем избрания соответствующего метода скрытия информации (второй уровень защиты).

Предварительное криптографическое преобразование позволяет обеспечить третий (дополнительный) уровень защиты. Для эффективного обеспечения защиты конфиденциальной информации криптостеганографическая система должна быть разработана на основе совокупности стойких алгоритмов шифрования и стойких методов внедрения информации. Совокупность криптографических алгоритмов образует криптографический модуль системы, совокупность методов внедрения (используемый метод) – стеганографический модуль.

В данной работе рассматривается криптостеганографическая система, созданная на основе современных стойких алгоритмов шифрования и стеганографического метода, разработанного автором.

Криптографическое преобразование информации применяется с целью исключить доступ к данной информации посторонних пользователей, а также с целью обеспечения целостности информации.

В качестве алгоритмов шифрования в криптографическом модуле используются:

– алгоритм Rijndael;

– алгоритм ГОСТ 28147-89 (режим Простой замены);

– алгоритм BlowFish.

Данные шифры относятся к алгоритмам блочного шифрования и имеют вполне сопоставимые параметры. Все эти криптографические алгоритмы соответствуют требованиям стойкости и надежности, предъявляемым к современным алгоритмом шифрования.

В качестве метода внедрения в стеганографическом модуле используется разработанный автором метод «Пиксельная карта». Данный метод относится к методам

сокрытия данных в пространственной области. Преимущество алгоритмов замены в пространственной области заключается в том, что для встраивания (внедрения) данных не нужно вычислительно сложные и длительные преобразования изображения. В качестве контейнеров для информации используются растровые изображения, представленные в формате либо без компрессии, либо с неискажающей компрессией: BMP, PNG или GIF.

Цветное изображение *C* представляется через дискретную функцию, которая определяет вектор цвета *c(x,y)* для каждого пикселя изображения *(x,y)*, где значение цвета задает трехкомпонентный вектор в цветовом пространстве. Цвет пикселя задается тремя составляющими: красной, зеленой, синей – RGB. Каждой из них соответствует свое значение интенсивности, которое может изменяться от 0 до 255. Таким образом, за каждый из цветовых каналов отвечает 8 битов (1 байт), а цветовая глубина изображения в целом - 24 бита (3 байта).

Принцип метода состоит в следующем: для внедрения одного бита сообщения используется один бит изображения-контейнера, совпадающий по значению со встраиваемым. Т.е. для внедрения бита «1» подойдет любой из битов байта контейнера, значение которого «1». Соответственно, для встраивания «0» может быть использован любой бит, равный «0». Подобный подход позволяет не изменять характеристик изображения: вся секретная информация (разряд бита, координаты байта/ пикселя) заносится в ключ, биты контейнера не меняются – носитель-результат аналогичен пустому контейнеру. Поэтому для встраивания сообщения можно использовать все подходящие биты контейнера: как биты одного байта пикселя, так и всех трех байтов.

В общем случае, возможно внедрить такое количество битов сообщения, чтобы соблюдалось равенство:

$$N_{z,b} \geq N_{z,m}, \quad N_{u,b} \geq N_{u,m} \tag{1}$$

Т.е нельзя внедрить большее количество нулевых битов сообщения $N_{z,m}$, чем в контейнере $N_{z,b}$. Аналогично число битов-единиц сообщения $N_{u,b}$ не может превышать числа битов-единиц изображения $N_{u,m}$. При этом можно для встраивания сообщения использовать как биты одного цветового канала (например, в большинстве методов замены в пространственной области используется канал синего цвета), так и биты всех трех каналов.

Количество бит, пригодных для встраивания в них, определяется емкостями байта/ пикселя E_z и E_u – количеством нулей и количеством единиц в байте/ пикселе. В случае использования всех цветовых каналов емкость пикселя определяется емкостями каждого канала.

Данный стеганографический метод может иметь следующие варианты реализации:

1) «Первый из группы». Для внедрения одного бита сообщения используется либо первая единица в байте, либо первый ноль. Пропускная способность контейнера в этой вариации, при условии использования полноцветного изображения (в каждый байт/ пиксель носителя можно внедрить по крайней мере 1 бит информации, т.е $E_z \geq 1$ либо $E_u \geq 1$), приблизительно равна 1/8 размера контейнера.

2) «Случайный бит». Бит контейнера для встраивания информации выбирается из группы с помощью генератора случайных чисел, при этом каждый выбранный бит используется только один раз. Из байта выбирается только один бит. Пропускная способность контейнера такая же, как и в предыдущей вариации.

3) «Плотное заполнение». Для внедрения битов сообщения используются все подходящие биты контейнера. Заполнение может производиться как последовательно, так и в случайном порядке. Пропускная способность носителя в данном случае складывается из двух компонент - нулевая емкость и единичная емкость контейнера. Емкость контейнера (нулевая или единичная) определяется как сумма емкостей (соответственно, E_z и E_u каждого байта) всех байтов/ пикселей изображения. При встраивании сообщения в три цветовых канала емкость контейнера складывается из емкостей по каждому каналу.

4) «Максимальное заполнение». В данном варианте снимается ограничение (1). Байты и биты контейнера выбираются с помощью генератора случайных чисел. Возможно повторное использование одних и тех же битов. Пропускная способность контейнера в таком случае стремится к бесконечности при условии:

$$N_{z,b} \geq 8, \quad N_{u,b} \geq 8 \tag{2}$$

Изображение должно содержать, по крайней мере, 8 единиц (8 нулей), чтобы закодировать 1 байт информации, имеющий значение 255 (0). Такой контейнер называется носителем бесконечной емкости.

Таким образом, в носитель можно внедрить сообщение практически любого размера.

В общем виде стеганографический алгоритм «Пиксельная карта» имеет следующий вид:

1) Предварительная подготовка контейнера. На этом этапе определяется множество всех (одного канала) байтов изображения и входящее в него подмножество всех битов. Для каждого из пикселей носителя вычисляются нулевая и единичная емкости, суммы всех нулевых и единичных емкостей пикселей определяют емкости контейнера.

2) Предварительная подготовка сообщения. На этом этапе сообщение (зашифрованное или оригинальное) подвергается аналогичной обработке: определяются множество байтов и входящее в него подмножество битов. При наличии ограничения (1) создаются множества флагов (меток использования) для всех байтов и для всех битов. Все метки изначально равны нулю. Также в этом случае вычисляется количество нулей $N_{z,m}$ и количество единиц в сообщении $N_{u,m}$. В случае «Максимального заполнения» осуществляется переход к этапу 4.

3) Проверка ограничения (1). В общем случае этот этап следует за подготовкой сообщения. В случае если выполняется (1), то осуществляется переход к этапу 4. Если ограничение (1) не выполняется, то в зависимости от реализации производится возврат на этап 1 (выбор другого изображения) либо на этап 2 (выбор другого сообщения).

4) Поиск подходящего бита в контейнере. Этот этап повторяется для каждого бита сообщения. Координаты бита (его разряд и порядковый номер байта) заносятся в стеганографический ключ, который необходим для извлечения информации. Таким образом, в ключ записывается своеобразная карта битов и пикселей, использованных для кодирования (внедрения) информации.

Данный метод внедрения информации обладает следующими достоинствами:

1) Высокая стойкость к статистическим атакам и сложность детектирования. При внедрении информации не осуществляется изменений каких-либо характеристик изображения. Даже если при совершении атаки на систему противнику известны детали ее реализации, единственным параметром, неизвестным ему, является стеганографический ключ. Без ключа, даже имея доступ к системе, противник не может получить информацию.

2) Максимизация пропускной способности контейнера. Неизменность характеристик контейнера позволяет внедрять информации во все три канала, используя все необходимые для этого биты. Это позволяет увеличить в несколько раз пропускную способность носителя, но и при использовании четвертой вариации метода с соблюдением минимального ограничения (2) внедрить практически любое количество информации.

3) Использование современного подхода. Так как информация встраивается в значительные области изображения (внедрение производится не только в младшие биты), то атака, направленная на разрушение сообщения, приведет к значительной деградации носителя.

Список литературы

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

РАЗРАБОТКА ТИПОВОЙ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ДЛЯ ОРГАНИЗАЦИИ МАЛОГО БИЗНЕСА

Занина О.А. – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Согласно российскому законодательству к субъектам малого и среднего бизнеса (СМБ) относятся организации, в которых среднесписочная численность сотрудников не превышает двухсот пятидесяти человек [6].

Все предприятия, действующие на территории Российской Федерации (РФ), должны выполнять требования нормативно-правовых актов РФ, в том числе и по информационной безопасности. Требования по защите персональных данных (ПДн) сотрудников появились в Трудовом кодексе (ТК) РФ, принятом в 2002 году. Фактически в ТК РФ определены права и обязанности работодателя и права работников. В 2006 году был принят Федеральный закон (ФЗ) «О персональных данных», в котором подробнее определены требования к обработке информации, относящейся к определенному или определяемому на основании такой информации физическому лицу. Окончательное вступление в силу этого закона неоднократно откладывалось по причине неготовности предприятий обеспечить безопасность информационных систем, обрабатывающих персональные данные (ИСПДн), в соответствии с требованиями законодательства. Трудности испытывают, в первую очередь, предприятия СМБ. Основными причинами этого являются:

– отсутствие квалифицированных сотрудников в области информационной безопасности на предприятиях СМБ;

– отсутствие методических рекомендаций, направленных на решение задач защиты ПДн, для предприятий СМБ;

– отсутствие финансовых возможностей субъектов СМБ для заказа разработки системы защиты ПДн специализированным фирмам.

Начиная с 2008 года, разрабатываются рекомендации по обеспечению защиты ПДн для банков, рекомендации для операторов связи, негосударственных пенсионных фондов, организаций здравоохранения, профессиональных участников рынка ценных бумаг, кадровых агентств. Вопросы защиты ПДн сотрудников организации освещены в настоящее время только с точки зрения кадрового делопроизводства, решения были разработаны до принятия ФЗ «О персональных данных». Комплексного решения, охватывающего организационные и технические меры защиты ПДн и ИСПДн, с учетом требований действующего законодательства для предприятий СМБ не существует.

Вышеизложенное определяет необходимость разработки рекомендаций для защиты ПДн сотрудников предприятий СМБ, в основу которых может быть положена типовая система защиты ПДн и этапы её разработки.

Этапы разработки системы защиты ПДн, должны включать [3]:

– обследование организации – анализ «бумажного» документооборота и бизнес процессов организации;

– определение требований к системе в зависимости от установленного класса ИСПДн и модели угроз безопасности;

– проектирование системы защиты – определение состава средств защиты, предполагаемых к использованию, требований к настройке и эксплуатации средств, параметры их взаимодействия, организационные меры защиты и их описание, перечень и состав организационно-распорядительных документов и др.;

– внедрение системы защиты – заключается в установке и настройке выбранных средств защиты, реализации организационных мер, разработке организационно-распорядительных документов;

– обучение сотрудников по вопросам эксплуатации средств защиты ПДн, обеспечения безопасности ПДн;

– сопровождение системы защиты – контроль эффективности системы защиты, ее модернизация.

В результате выполнения первого этапа были определены особенности предприятий СМБ и выделены объекты защиты.

В наиболее общем случае предприятия обрабатывают данные кадрового учета, базы данных клиентов – физических лиц, базы данных партнеров и контрагентов, содержащие данные о физических лицах. В связи с многообразием сфер деятельности предприятий СМБ возможно определить категорию и объем ПДн только сотрудников организаций, так как принципы кадрового учета и расчета с сотрудниками не зависят от области деятельности предприятия.

В ходе изучения деятельности предприятий СМБ было выявлено, что кадровым учетом персонала чаще всего занимается либо отдельный сотрудник, либо сотрудник, выполняющий такие обязанности по совместительству (например, секретарь), вопросами оплаты труда и других выплат занимается бухгалтер (один или два) с использованием ИС, чаще всего «1С Зарплата» и, реже «1С Зарплата и Управление кадрами». Количество субъектов ПДн в базе по количеству сотрудников, режим обработки – однопользовательский либо многопользовательский с равными правами. Организации с численностью свыше 50 человек в обязательном порядке предоставляют отчетность в фискальные органы и внебюджетные государственные фонды в электронном виде, для чего используют сеть Internet.

ПДн сотрудников существуют в двух формах: на бумажных носителях и в электронном виде. Формы ПДн определили объекты защиты, которые более подробно приведены на рисунке 1.

Рисунок 1 – Объекты защиты ПДн сотрудников

В ходе анализа угроз ПДн сотрудников в соответствии с [5] были выявлены следующие группы актуальных угроз:

– утечки видовой информации;

– угрозы НСД;

– угрозы внедрения вредоносных программ;

– угрозы «анализа сетевого трафика» с перехватом информации, передаваемой по локальной сети, а также во внешние сети и принимаемой из внешних сетей.

В 2007 году по результатам ежегодного опроса американского Института компьютерной безопасности первое место среди угроз заняли умышленно и неумышленно совершенные противоправные действия внутренних пользователей (инсайдеров). На третьем месте оказалась угроза потери носителей с конфиденциальными данными [4]. Больше всего инсайдеров привлекают персональные данные (68%) [1]. Для предприятий СМБ характерны неумышленные действия сотрудников, приводящие к нарушению целостности, доступности, конфиденциальности ПДн. Риск подобных нарушений можно снизить, реализовав меры

организационной защиты. Для обеспечения комплексной защиты ПДн организационных мер недостаточно.

В соответствии с Положением «О методах и способах защиты информации в информационных системах персональных данных» была определена следующая типовая структура системы защиты ПДн (рисунок 2):

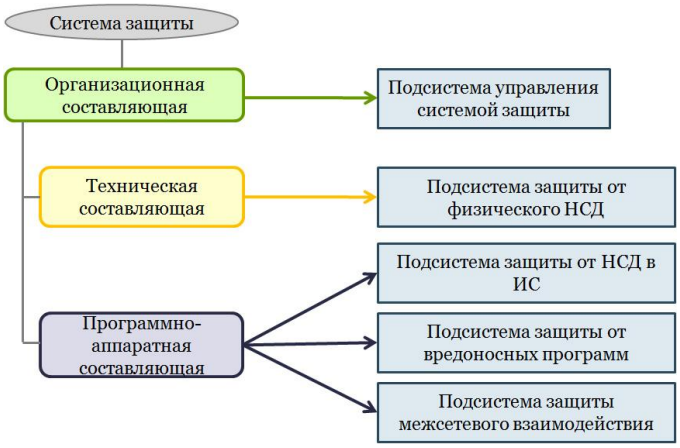


Рисунок 2 – Структура системы защиты ПДн сотрудников

Кроме того была определена структура подсистем защиты, а также перечни программно-аппаратных средств, требования к их настройке, организационные меры защиты, состав пакета документов, необходимых для обеспечения безопасности ПДн.

В результате проведенной работы разработаны методические рекомендации по построению системы защиты ПДн сотрудников организаций СМБ. Рекомендации включают:

– введение;
– рекомендации по определению объектов защиты;
– рекомендации по составлению частной модели угроз ПДн;
– рекомендации по определению структуры и состава системы защиты;
– перечень средств защиты, позволяющих реализовать компоненты программно-аппаратной составляющей системы защиты;
– состав нормативно-методического обеспечения;
– приложения (типовые формы документов нормативно-методического обеспечения).

Список литературы

1. Инсайдерство в России: диагноз – безнаказанность и латентность [Электронный ресурс] – Режим доступа: http://www.anti-malware.ru/node/1026., свободный. – Загл. с экрана.
2. Информационная безопасность [Электронный ресурс]: Защита персональных данных предприятиями малого и среднего бизнеса – Режим доступа: http://www.itsec.ru/articles2/Oborandteh/zashita-personalnih-dannih-predpriyatiyami-malogo-i-srednego-biznesa, свободный. – Загл. с экрана.
3. Комплексная система защиты информации на предприятии: учеб. пособие/ В.Г. Грибунин, В.В. Чудовский. – М. : Издательский центр «Академия», 2009. – 416 с.
4. Кто такие инсайдеры [Электронный ресурс] – Режим доступа: http://netler.ru/pc/insider.htm, свободный. – Загл. с экрана.
5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.) [Электронный ресурс] – Режим доступа: http : //www.fstec.ru/_spravs/metodika.doc, свободный. – Загл. с экрана.
6. Федеральный закон «О развитии малого и среднего предпринимательства в Российской Федерации» от 24 июля 2007 года № 209-ФЗ. – М.: Изд-во стандартов,2007. – 19 с.

ЭЛЕКТРОННОЕ УЧЕБНОЕ ПОСОБИЕ ПО СРЕДСТВАМ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Масалова К.В. – студент, Шарлаев Е.В. – к.т.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Сейчас невероятно тяжело найти человека, который никогда не слышал о персональных компьютерах или никогда их не видел. Для работы мало видеть компьютер, нужно знать и его устройство. Для технических специальностей требования к знанию компьютеров более жесткие, поскольку они должны быть более углубленными.

Студенты не всегда честно выполняют свою главную обязанность – добросовестно учиться - заказывают лабораторные, списывают на экзаменах и контрольных, прогуливают занятия. Поэтому традиционные методы контроля знаний не всегда эффективны. Отсюда вытекает необходимость разработать метод, который бы мог объективно оценить знания студента. Таким требованиям соответствует система тестирования – студент не может знать заранее, какие вопросы ему попадутся, а, следовательно, для получения положительной оценки, он должен разбираться во всей теме целиком.

Данная проблема порождает следующую цель:
Разработать приложения, которые помогут преподавателю развить интерес к своему предмету, а также позволят контролировать знания предмета с максимальной объективностью и достоверностью.

Для достижения цели, необходимо решить следующие задачи:

- Снабдить студентов наглядным пособием по информатике, которое поможет расширить и углубить знания по теме «Устройство ПК»;
- Разработать программу-тестер;
- Разработать тестовую базу по материалу курса «Информатика».

Этапы решения поставленных задач отражены в основной части.

При подборе теоретического материала учитывалась не только актуальность (например, [1]) и достоверность (например, [2]) информации, но и доступная форма изложения. Так же выбиралсить наиболее интересные факты из состава и принципа работы устройства. Приведенные в учебниках схемы анимированы.

Среда разработки также выбрана не случайно – Flash позволяет компилировать .fla файлы не только в .swf, но и в полноценное видео (.mov), а также в приложения Windows (.exe), MacOS (.hqx) [4]. Flash-приложения также легко интегрируются в сайты, как и Java-апплеты и, при этом, не позволяют копировать приложение на использующий его ПК, что является подспорьем для защиты авторских прав.

Наглядное пособие представляет собой .exe –файл, без каких либо дополнений.

Тестер состоит из двух частей: первая – основная программа-тестер; вторая – база вопросов.

Наглядное пособие:

Наглядное пособие представляет собой скомпилированный .exe файл с теоретическим материалом и множеством вложенных анимаций (они разрабатывались при помощи [3]). Например, работа сканера представляется наглядно: студент видит схему, на которой отображаются основные части сканера во время сканирования. Это позволяет упростить понимание материала.

Тестер:

Тестер представляет собой .exe написанный в среде Flash с применением скрипотового языка ActionScript.

.fla файл состоит из четырех фреймов.

Первый фрейм – фрейм регистрации (Рисунок 1). Он предлагает пользователю ввести свои данные и количество вопросов, на которые необходимо дать ответ. Возможность

выбора количества вопросов легко обосновывается: преподаватель может предложить студенту выбрать такое количество вопросов, которое подтвердит его успеваемость.

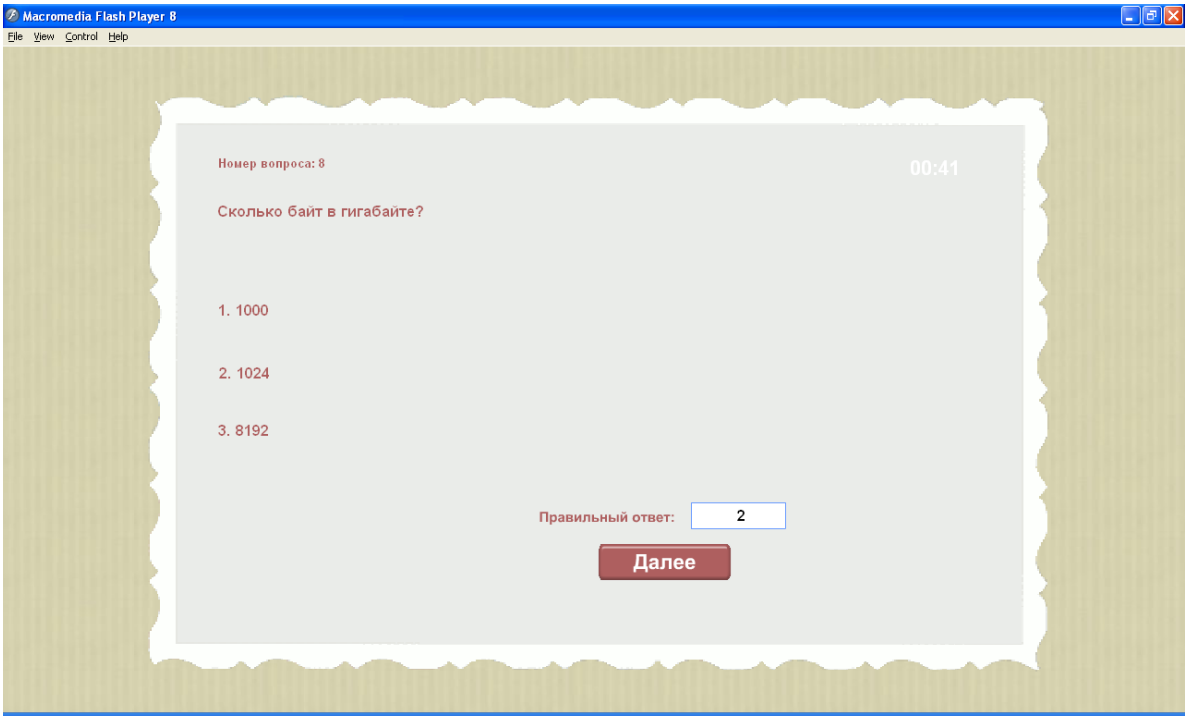


Рисунок 1 – Фрейм регистрации

Второй фрейм – динамическая форма. На ней автоматически выводится вопрос, варианты ответа, поле ввода правильного варианта, а так же независимые поля: поле таймера и номера текущего вопроса (Рисунок 2). В данном фрейме все рассчитывается и выводится автоматически из базы вопросов, которые хранятся в подкаталоге.

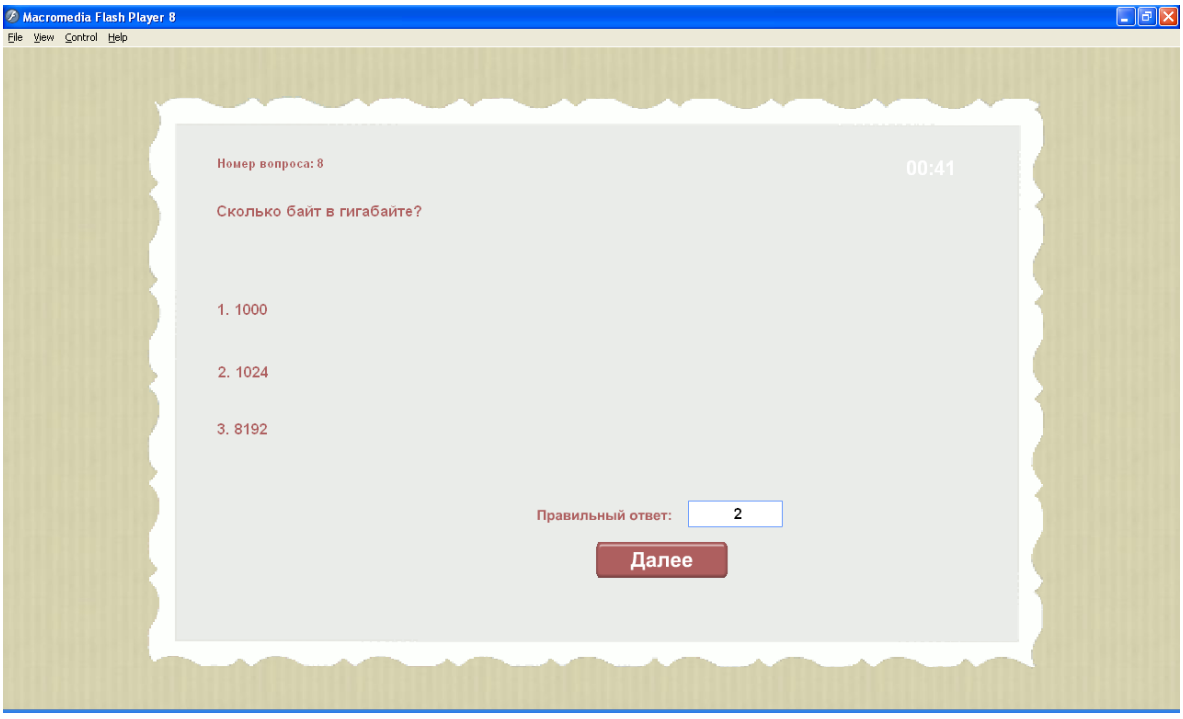


Рисунок 2 – Динамическая форма

Третий фрейм – результаты теста. На данном фрейме выводится ФИО, количество предложенных вопросов, количество правильных ответов и время, за которое был выполнен тест. Эти данные сохраняются в КЭШе, и выводятся при следующем обращении в четвертом фрейме. Это необходимо для исключения возможности подтасовки результатов тестирования студентами.

Достоинства:

- Тестирование — это более мягкий инструмент, они ставят всех учащихся в равные условия, используя единую процедуру и единые критерии оценки, что приводит к снижению нервных напряжений
- Кроссплатформенность. ActionScript сам по себе кроссплатформенный интерпретируемый язык, а Flash является кросс-компилятором.

Недостатки:

- Данные, получаемые преподавателем в результате тестирования, хотя и включают в себя информацию о пробелах в знаниях по конкретным разделам, но не позволяют судить о причинах этих пробелов.
- Тест не позволяет проверять и оценивать высокие, продуктивные уровни знаний, связанные с творчеством, то есть вероятностные, абстрактные и методологические знания.

Особая актуальность изучения темы «Устройство ПК» дисциплины «Информатика» связана с тем, что именно недостаточное знание азов работы составных частей компьютера зачастую является главной причиной трудностей, возникающих при изучении дисциплин смежной направленности. Поэтому особое внимание уделялось качеству контроля знаний и развитию интереса к предмету.

Приложения, которые были разработаны, соответствовали этой цели. Наглядное пособие выдается студентам на дом для самостоятельного изучения. Тестер используется преподавателем в лабораторных условиях для контроля знаний

В будущем предполагается расширить базу вопросов и увеличить количество тем, охватываемых наглядным пособием.

Список литературы

1. Угринович Н.Д., Информатика и ИКТ : Учебник для 11 класса / Н.Д. Угринович. – 4-е изд. – М.: БИНОМ. Лаборатория знаний, 2010. – 187 с.:ил.
2. Фигурнов В.Э., IBM PC для пользователя. Краткий курс. / В.Э.Фигурнов. – 7-е изд, перераб. и доп. – М.:ИНФРА-М, 1997. – 640 с.:ил.
3. Переверзев С. И., Анимация в Macromedia Flash MX / С. И. Переверзев. 2-е изд. — М.: БИНОМ. Лаборатория знаний, 2009. – 374 с.: ил. — (Практикум)
4. Гурский Д.А., Flash 8 и ActionScript / Д.А.Гурский, Ю.А.Гурский - СПб.: Питер, 2007. – 528 с.

РАЗРАБОТКА ДИДАКТИЧЕСКИХ СРЕДСТВ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ В ОБЛАСТИ ПРАВОВОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Митина О.С. – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Острота проблем информационной безопасности будет только увеличиваться по мере дальнейшего увеличения масштабов внедрения современных информационных и коммуникационных технологий, являющихся технологической основой процессов глобализации, во все сферы жизнедеятельности современного общества, развития электронных систем для защиты персональных данных, коммерческой, служебной и

профессиональной тайн. Это выдвигает в качестве одной из актуальных задач более качественную подготовку специалистов и в частности по вопросам правой защиты конфиденциальной информации.

Для решения в системе высшего профессионального образования педагогических проблем, связанных с обучением основам информационной безопасности и правовой защиты конфиденциальной информации как инвариантной составляющей подготовки в области комплексного обеспечения информационной безопасности объектов информатизации, требуется системный подход, реализующий методологические, организационные, содержательные, дидактические и технологические аспекты. Правовая защита конфиденциальной информации представляет собой комплекс правовых методов базирующихся на законодательстве РФ и включающий: определение информации конфиденциального характера, установление режимов защиты, определение мер правовой ответственности за нарушение этих режимов в отношении коммерческой, служебной, профессиональной тайны, персональных данных.

В рамках подготовки специалистов по защите информации в АлтГТУ, по специальности «Комплексная защита объектов информатизации» на изучение вопросов правовой защиты конфиденциальной информации отводится 20 часов учебного времени (Модуль №4) в курсе «Правовое обеспечение информационной безопасности», из них 8 часов - лекции, 4 часа - семинаров, 8 часов - СРС. При изучении этих вопросов по программе подготовки бакалавров по направлению «Информационная безопасность», которая будет реализовываться с 2011 года, предусматривается такой же лимит времени на лекции, семинары и СРС, и дополнительно планируется 4 часа практических занятий [1].

Наиболее часто в педагогической практике, для развития у обучающихся творческого мышления, индивидуального подхода, моделирования ситуаций, используются дидактические материалы. Эти психолого-педагогические составляющие дидактического материала направлены на привлечение внимания учащегося, поддержание познавательного интереса, активизацию его мышления, на формирование оценок описываемого, создание побудительных мотивов к углубленному изучению того или иного вопроса.

Память человека имеет избирательный характер: чем важнее, интереснее и разнообразнее материал, тем прочнее он закрепляется и дольше сохраняется, поэтому практическое использование полученных знаний и умений, является эффективным способом продолжения их усвоения, в условиях моделирующей среды [2].

На выходе, согласно образовательному стандарту учебной дисциплины «Правовое обеспечение информационной безопасности», специалист по защите информации должен освоить следующие профессиональные компетенции в области правовой защиты конфиденциальной информации:

Студенты должны ***обладать знаниями:***

– об институтах правовой защиты служебной, коммерческой, банковской, профессиональной тайны и правовой защиты информации персонального характера;

Студенты должны ***уметь использовать:***

– нормативно-правовые акты в области обеспечения информационной безопасности;

– нормы законодательства РФ, регулирующие правовые отношения в сфере информационного обмена и обработки информации, в том числе для информационных систем РФ, подключаемых к сети Интернет;

– законодательство РФ в области защиты государственной тайны и конфиденциальной информации.

Федеральным законом Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» конфиденциальными следует считать такие сведения, которые законом отнесены к какой-либо тайне, доступ к

которым ограничен в силу закона или которые имеют признаки, определенные законом, за исключением государственной тайны. Комплексный анализ законодательства Российской Федерации в области правового регулирования защиты конфиденциальной информации и информационного права, позволяет представить все виды конфиденциальной информации в рамках четырёх институтов права (рисунок 1).

Рисунок 1 − Виды конфиденциальной информации в рамках четырёх институтов права

С целью повышения эффективности процесса обучения студентов и развития навыков применения полученных знаний на практике, предлагается использовать следующие дидактические материалы, которые были разработаны в соответствии с требованиями стандартов АлтГТУ к стандартам дисциплин [2], к практическим занятиям [3], к фонду квалификационных заданий и тестов [4]:

- тесты, закрытого и открытого типа;
- проблемные задачи, условия которых максимально приближены к реальным.
- типовые ситуационные задачи.

Примером теста закрытого типа являются следующие разработанные материалы:

1. Определите категорию персональных данных: ФИО, сведения о политических взглядах, сведения о состоянии здоровья
   1) 3 категория;
   2) 1 категория;
   3) 2 категория;
   4) 4 категория;
   5) 5 категория;

   Ответ: 2.
2. Перечень информации, составляющую тайну организации утверждается и вводится в действие:
   1) приказом руководителя организации;
   2) с согласия правообладателя;
   3) работниками на основании трудовых договоров;
   4) распоряжением представителя организации, разработавшей систему защиты информации в организации;
   5) руководителем подразделения защиты информации.

   Ответ: 1.

Однако тестирование не позволяет проверять и оценивать продуктивный уровень знаний, связанный с творчеством, то есть вероятностные, абстрактные и методологические знания, а ограниченность времени и широта всех аспектов темы не даёт времени для глубокого анализа темы [2]. С целью решения этой проблемы разработаны проблемные (ситуационные) задачи, две из которых приводятся ниже.

На предприятии действует информационная система заказа пропусков, куда вносятся Ф.И.О посетителя и данные документа, удостоверяющего его личность (серия-номер

паспорта, номер водительского удостоверения и т.д.). Правомерны ли действия руководства предприятия по ведению такой базы данных?

Ответ:

Действия руководства правомерны на основании п.1 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

Согласно Православию любой прихожанин может покаяться в любой день страстной седмицы. В один из дней седмицы 13-летний мальчик Кирилл решил покаяться, на исповеди он признался батюшке, что из-за трудной жизненной ситуации он не раз сбегал из семьи, совершал мелкие кражи и путался с плохой компанией. Через 3 дня к батюшке по поводу этого мальчика пришел социальный работник и работник детской комнаты милиции с целью розыска и сбора сведений о Кирилле. Под нажимом того, что государство предоставит мальчику более достойную жизнь и образование батюшка рассказал о жизненных трудностях и проступках мальчика.

1. Как можно рассудить действия батюшки?
2. Мог ли батюшка отказаться от дачи показаний?

Ответ:

Если следовать строго букве закона, то действия батюшки можно рассудить следующим образом:

1. Согласно Конституции РФ ст. 28, каждому человеку гарантирована свобода совести, свобода вероисповедания, тайна исповеди, право свободно выбирать, иметь, распространять религиозные убеждения и действовать в соответствии с ними. В соответствии с этим батюшка нарушил профессиональную тайну, но поступил исходя из благих намерений.

2. Духовное лицо не подлежит ответственности за недонесение о преступлении, ставшем ему известным из исповеди. Уголовное дело не может быть возбуждено, а возбужденное подлежит прекращению в отношении священнослужителя за отказ от дачи показаний по обстоятельствам, известным ему из исповеди (п.11 ст.5 УПК).

В результате выполнения работы разработан дидактический комплекс, включающий 75 практических задач и 100 тестовых заданий и реализующий систему подготовки специалистов по защите информации в рассматриваемой области на основе креативного подхода к изучаемым темам.

Список литературы

1. СТП 16.222-2010 Образовательный стандарту учебной дисциплины «Правовое обеспечение информационной безопасности». АлтГТУ, Барнаул: 2010. - 48 с.
2. Габай.Т.В. «Дидактические основы комплексного использования средств обучения в учебно-воспитательном процессе» – М.: 1991.
3. СТО 12 701-2009 Образовательный стандарт высшего профессионального образования АлтГТУ. Практические и семинарские занятия. Общие требования к организации, содержанию и проведению. АлтГТУ, Барнаул: 2009. – 36 с.
4. СТП 12 100-02 Образовательный стандарт высшего профессионального образования АлтГТУ. Требования к фонду квалификационных заданий и тестов. АлтГТУ, Барнаул: 2002. – 18 с.

РАЗРАБОТКА СТРУКТУРЫ ЗАЩИЩЕННОГО ХРАНИЛИЩА ИНФОРМАЦИИ НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОГО СРЕДСТВА ДЛЯ ДОСТУПА К ДАННЫМ

Моторинский Д.А. – студент, Ленюк С.В. – к.ф.-м.н., доцент
Алтайский государственный технический университет (г. Барнаул)

В системах многопользовательской обработки конфиденциальной информации одной из важнейших является задача обеспечения конфиденциальности информации. Для решения этой задачи возможно использование методов криптографической защиты. Однако криптографическая защита сама по себе не является достаточной для обеспечения секретности информации, поскольку зашифрованная информация может быть перехвачена (украдена с носителя или при передаче по сетям связи) и расшифрована при помощи подбора пароля при помощи грубой силы или при помощи украденного/перехваченного пароля.

Появляется необходимость не только зашифровать информацию, но и ограничить доступ к ней посторонних лиц и возможность распространения информации вне организации, для чего можно было бы использовать криптографические методы не только для шифрования, но и для аутентификации доступа и блокирования информации при переносе на любой другой персональный компьютер.

Таким образом, для обеспечения эффективной защиты информации с помощью криптографических методов должна быть разработана система, основанная на структуре защищенного хранилища данных.

Методика, описанная в данной работе, предполагает создание защищенных хранилищ конфиденциальных документов, необходимых каждому из сотрудников, работающих за одним персональным компьютером. В результате мы имеем защищенное хранилище информации, имеющее жесткую привязку к конкретному персональному компьютеру, доступ к которому имеет только один сотрудник, защищенный двумя уровнями шифрования.

В данной работе рассматривается криптографический комплекс, общая стойкость которого выше, чем стойкость входящих в него компонентов. Состав комплекса можно условно разделить на несколько модулей:

- криптографический модуль;
- модуль аутентификации;
- модуль привязки к рабочей машине (персональному компьютеру).

Большую роль в повышении стойкости занимает правильное согласование использованных компонентов. Данный комплекс обеспечивает определенный уровень комплексности подхода к обеспечению секретности информации.

Криптографический модуль обеспечивает безопасность информации путем двух уровневого шифрования хранилища информации, один из которых привязывает контейнер с информацией к одной определенной вычислительной машине, а второй обеспечивает аутентификацию доступа к информации. Для каждого из уровней может быть выбран один из трех алгоритмов шифрования с различными длинами ключей.

В ходе работы был проведен анализ современных симметричных криптографических алгоритмов, что позволило принять оптимальное решение по выбору алгоритмов шифрования [1]. В данной системе используются следующие алгоритмы:

- AES(Rijndael);
- ГОСТ 28147-89;
- Blowfish.

Модель криптографической системы основана на разработанной структуре защищенного хранилища информации (рисунок 1).

Краткий алгоритм работы криптографической системы (рисунок 1) состоит из следующих этапов:

1) получение или выборка исходной информации (текста);

2) шифрование информации с помощью выбранного заранее алгоритма шифрования и ключа;

3) передача полученного шифротекста по каналу связи;

4) расшифровка шифротекста;

5) получение информации конечным пользователем.

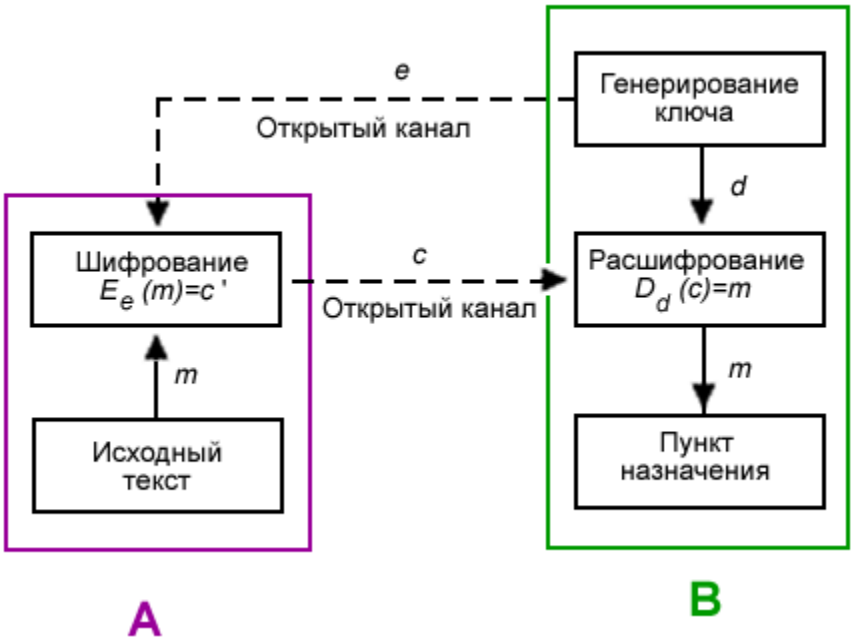


Рисунок 1 – Модель криптографического средства

Структурно защищенное хранилище состоит из двух независимых модулей:

- модуль хранения и адресации созданных хранилищ;
- модуль шифрования информации и создания и учета ключей доступа.

Модуль хранения и адресации предоставляет доступ к созданным хранилищам и позволяет управлять ими. В качестве хранилища предполагается использование зашифрованного архива, внутри которого информация хранится в зашифрованном виде. Доступ к информации хранящейся в хранилище может получить только пользователь, имеющий ключевой файл и пользователь, создавший хранилище. Доступ к списку файлов имеют любые пользователи, работающие на данной локальной машине, так как для доступа к списку используется системный ключевой файл. Перенос хранилища на любой другой локальный ПК делает невозможным доступ к хранилищу, так как в качестве системного ключа используются хеш – суммы уникальных параметров системы. Это дает возможность ограничить распространение информации и блокирует канал утечки через копирование хранилища.

При создании пользовательского ключа также используется набор редко повторяющихся параметров:

- хеш – сумма фамилии и инициалов пользователя;
- хеш – сумма пароля, введенного пользователем для создания ключа.

Доступ к информации, находящейся в хранилище ограничивается требованием предъявления криптографическому средству доступа одновременно двух ключей.

При не соответствии одного из ключей оригинальной записи доступ к хранилищу блокируется на заданное администратором время (от 1 часа до 24 часов), что резко понижает шансы подбор ключа методом грубой силы.

Для хеширования, используемого при создании ключей, применяется алгоритм MD5, для которого в данный момент не существует способа подбора ключевой информации, кроме как при помощи радужных таблиц. Но и этот способ крайне дорогостоящий и требует достаточно больших временных затрат.

Список литературы

1. Авдошин С.М., Савельева А.А. Криптографические методы защиты информационных систем// Бизнес-информатика, 2006. - С.91-99.

ПРИМЕНЕНИЕ ЭКСПЕРТНЫХ ОЦЕНОК В КОГНИТИВНОМ МОДЕЛИРОВАНИИ

Пойманов К.И. – студент, Пивкин Е.Н. – к.т.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Важнейшим этапом в процессе осуществления информационной безопасности является оценка информационных рисков организации. Сложность этой задачи обусловлена наличием большого количества неопределенных, неполных и нечетких характеристик организации. В связи с этим оценку информационных рисков осуществляют с применением технологий когнитивного моделирования (когнитивных карт).

При построении когнитивных карт и оценке информационных рисков целесообразно использовать методы экспертных оценок. Экспертов привлекают на всех этапах построения когнитивных карт, включая:

1) определение списка концептов;
2) установление причинно-следственных связей между концептами;
3) установление силы (веса) связей между концептами.

К достоинствам экспертных методов относят: быстрота получения результатов без наличия нормативной базы, возможность оценивания того или иного объекта при невозможности измерить его характеристики количественными объективными методами. К недостаткам экспертных методов относят: определенную субъективность и соответствующие этому возможные погрешности результатов опроса [2].

Число экспертов в экспертной группе зависит от множества факторов и условий, в частности от важности решаемой проблемы, наличия возможностей и т.п. Минимально необходимое количество экспертов определяют по формуле [2]:

$$Н_{эмин} = 0{,}5 \times \left(\frac{3}{ж} + 5\right),$$

где *ж* – возможная ошибка результатов экспертизы (0 <*ж* < 1).

При ошибке результатов экспертизы 0,15 количество участвующих экспертов – 13.

При осуществлении когнитивного моделирования экспертов привлекают для определения весов когнитивной карты, характеризующих степень (силу) влияния факторов друг на друга (рисунок 1).

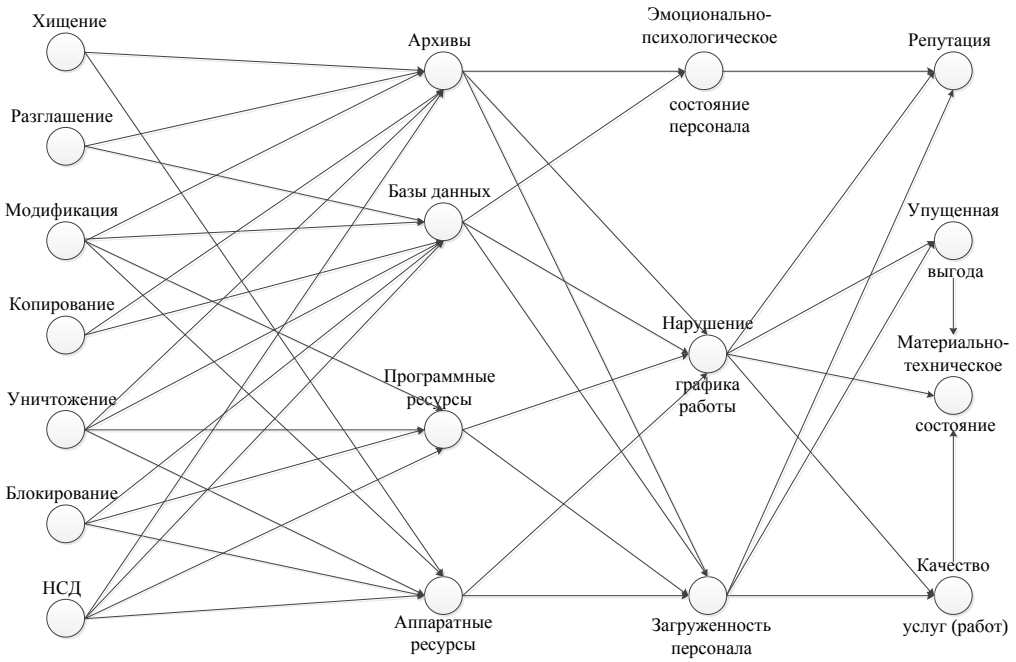


Рисунок 1 – Когнитивная карта для оценки рисков информационным ресурсам

Для установления силы (веса) связей между концептами используют числовые значения в диапазоне от 0 до 10 в соответствии со шкалой (рисунок 2).

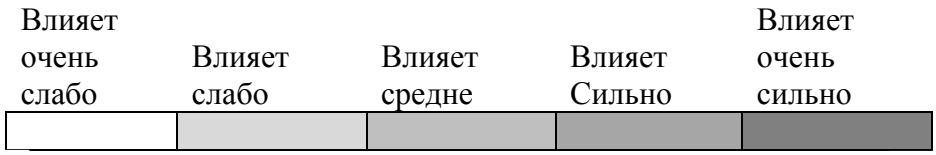


Рисунок 2 – Шкала для экспертной оценки взаимовлияния концептов

Для подсчета весов, характеризующих степень (силу) влияния факторов друг на друга, применяют формулу:

$$\omega_j = n/\left(\frac{1}{n-1}\sum_{i=1}^{n}\left(A_{ji}-\overline{A}_j\right)^2\right),$$

где ω_j – вес j-ой связи между концептами, n – количество экспертов, A_i – оценка i-го эксперта, $\overline{A}_j$ – среднее значение оценок экспертов.

При этом следует учитывать, что мнения экспертов часто совпадают неполностью, поэтому необходимо количественно оценивать меру согласованности мнений экспертов и установить причину несовпадения суждений. Для оценки меры согласованности мнений экспертов используются, как правило, коэффициенты конкордации.

Мера согласованности определяется на основе статистических данных всей группы экспертов. Так, согласованность мнений экспертов при определении весов (силы) взаимодействия концептов друг на друга рассчитывается с помощью коэффициента конкордации по формуле:

$$W = 12 \times \frac{C}{(K^2 \times (H^3 - H))}, \quad (1)$$

где C – сумма квадратов отклонений сумм весов по каждой связи от суммы весов по всем, т.е.:

$$C = \sum_{i=1}^{h}\left[\sum_{j=1}^{k} A_{ij} - K \times \left(\frac{H+1}{2}\right)\right]^2,$$

где $K \times \left(\frac{H+1}{2}\right)$ – средняя сумма весов, *K* – количество экспертов, *H*– количество связей между концептами.

Коэффициент конкордации может быть в диапазоне 1 >W> 0. При W=0 согласованность мнений экспертов отсутствует, а при W = 1 согласованность полная. Согласованность вполне достаточна, если W ≥ 0,5.

Рассчитанные таким образом веса связей между концептами формируют матрицу смежности весов для когнитивных карт, на основании которой производят оценку информационных рисков. Анализ информационных рисков позволяет, в свою очередь, выявить наиболее слабые места в системе защиты информации, оценить влияние потенциально существующих угроз, определить возможный ущерб от действия этих угроз и, в конечном итоге, минимизировать этот ущерб путем введения соответствующих контрмер.

Список литературы

1. Васильев, В. И., Савина, И. А., Шарипова, И.И. Построение нечетких когнитивных карт для анализа и управления информационными рисками вуза – Вестник УГАТУ, №2 (27), 2008 г.
2. Шаров Ф.Л. Исследование систем управления:Учеб. пособие / Под ред. Ф.Л. Шарова. – М.: МИЭП, 2007. – 136 с.

ПОДХОД К ОЦЕНКЕ ИНФОРМАЦИОННЫХ РИСКОВ С ИСПОЛЬЗОВАНИЕМ КОГНИТИВНЫХ КАРТ

Пойманов К.И. – студент, Пивкин Е.Н. – к.т.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Оценку информационных рисков информационной безопасности в организациях осуществляют с применением технологий когнитивного моделирования (когнитивных карт), в связи с большим количеством неопределенных и нечетких параметров в деятельности любой организации.

Рассмотрим задачу оценки информационных рисков с помощью когнитивных карт для информационных ресурсов организации. В таблице 1 приведены основные дестабилизирующие факторы для информационных ресурсов объекта информатизации организации. На основании этой таблицы формируют связи дестабилизирующих факторов и информационных ресурсов.

Таблица 1 – Дестабилизирующие факторы информационным ресурсам

Информационные ресурсы	Дестабилизирующие факторы
Архивы	Хищение, разглашение, модификация, копирование, уничтожение, НСД
Базы данных	Разглашение, модификация, копирование, уничтожение, блокирование, НСД
Программные ресурсы	Копирование, уничтожение, блокирование, НСД
Аппаратные ресурсы	Хищение, модификация, уничтожение, блокирование, НСД

Анализ основных бизнес-процессов, дестабилизирующих факторов и информационных ресурсов позволил определить перечень концептов когнитивной карты и сформировать карту (рисунок 1). Веса связей задавались экспертами в виде чисел из интервала [0,10].

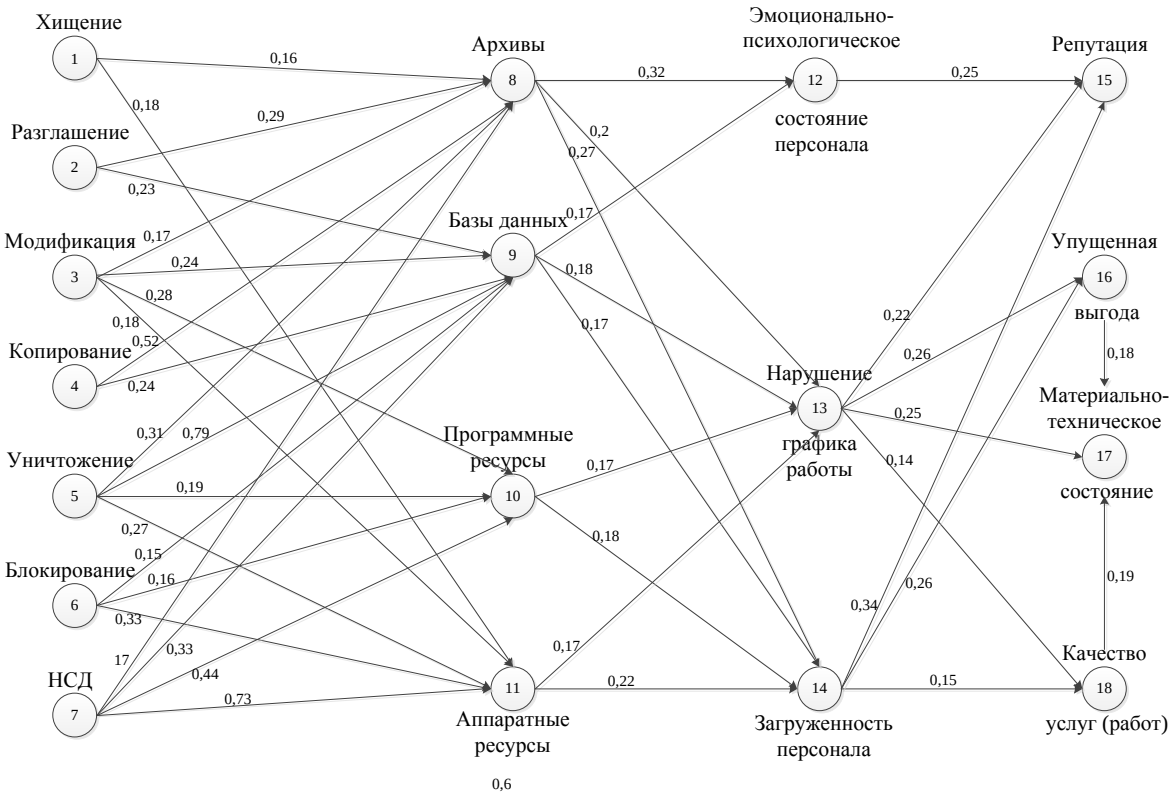


Рисунок 1 - Когнитивная карта для оценки рисков информационным ресурсам

Для определения общего эффекта от действия концепта (дестабилизирующего фактора) на концепт (фактор определяющий состояние бизнес-процесса организации) находят матрицу достижимости:

$$T = \sum_{i=1}^{n-1} W^i,$$

где $W^i = \| W_{ij} \|$ – матрица смежности когнитивной карты; W_{ij} – вес связи между i-м и j-м концептами когнитивной карты; n – число концептов когнитивной карты.

Матрица достижимости T когнитивной карты, приведенной на рисунке 1, имеет вид:

0	0	0	0	0	0	0	0,16	0	0	0,18	0,05	0,06	0,08	0,05	0,04	0,03	0,02
0	0	0	0	0	0	0	0,29	0,23	0	0	0,13	0,1	0,12	0,09	0,06	0,04	0,03
0	0	0	0	0	0	0	0,17	0,24	0,28	0,19	0,1	0,16	0,18	0,12	0,08	0,06	0,05
0	0	0	0	0	0	0	0,52	0,24	0	0	0,21	0,15	0,18	0,14	0,08	0,06	0,05
0	0	0	0	0	0	0	0,31	0,79	0,2	0,27	0,23	0,28	0,31	0,22	0,15	0,11	0,09
0	0	0	0	0	0	0	0,15	0,16	0,33	0	0,08	0,11	0,12	0,09	0,06	0,05	0,03
0	0	0	0	0	0	0	0,17	0,33	0,44	0,74	0,11	0,29	0,34	0,21	0,16	0,12	0,09
0	0	0	0	0	0	0	0	0	0	0	0,32	0,2	0,27	0,21	0,12	0,08	0,07
0	0	0	0	0	0	0	0	0	0	0	0,17	0,18	0,17	0,14	0,09	0,07	0,05
0	0	0	0	0	0	0	0	0	0	0	0	0,17	0,17	0,1	0,09	0,07	0,05
0	0	0	0	0	0	0	0	0	0	0	0	0,17	0,22	0,11	0,1	0,07	0,06
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,24	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,22	0,26	0,32	,014
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,34	0,25	0,07	0,15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,18	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,19	0

Анализ матрицы достижимости позволяет определить дестабилизирующие факторы, которые оказывают наиболее существенное влияние на бизнес-процессы организации.

Так, для выбранных факторов: «Репутация» (концепт 15), «Упущенная выгода» (концепт 16), «Материально-техническое состояние» (концепт 17) и «Качество услуг» (концепт 18) полный эффект от воздействия угроз составляет:

$W_{1\text{-}15} = 0{,}05;$	$W_{1\text{-}16} = 0{,}04;$	$W_{1\text{-}17} = 0{,}03;$	$W_{1\text{-}18} = 0{,}02;$
$W_{2\text{-}15} = 0{,}09;$	$W_{1\text{-}16} = 0{,}06;$	$W_{2\text{-}17} = 0{,}04;$	$W_{2\text{-}17} = 0{,}03;$
$W_{3\text{-}15} = 0{,}12;$	$W_{1\text{-}16} = 0{,}08;$	$W_{3\text{-}17} = 0{,}06;$	$W_{3\text{-}17} = 0{,}05;$
$W_{4\text{-}15} = 0{,}14;$	$W_{1\text{-}16} = 0{,}08;$	$W_{4\text{-}17} = 0{,}06;$	$W_{4\text{-}17} = 0{,}05;$
$W_{5\text{-}15} = 0{,}22;$	$W_{1\text{-}16} = 0{,}15;$	$W_{5\text{-}17} = 0{,}11;$	$W_{5\text{-}17} = 0{,}09;$
$W_{6\text{-}15} = 0{,}09;$	$W_{1\text{-}16} = 0{,}06;$	$W_{6\text{-}17} = 0{,}05;$	$W_{6\text{-}17} = 0{,}03;$
$W_{7\text{-}15} = 0{,}21;$	$W_{1\text{-}16} = 0{,}16;$	$W_{7\text{-}17} = 0{,}12;$	$W_{7\text{-}17} = 0{,}09.$

Риск j-го фактора по отношению к i-ому дестабилизирующему фактору ( ) определяют по формуле:

$$R_{ij} = T \times r_j, \qquad (1)$$

где r_j – ценность j-го ресурса; T – полный эффект воздействия одного фактора на другой.

Для оценки риска необходимо задать ценность каждого целевого фактора. Так, если ценность факторов определять в условных единицах (баллах), например, «Репутация» – 100, «Упущенная выгода» – 150, «Материально-техническое состояние» – 250 и «Качество услуг» – 200, то информационные риски рассчитанные по формуле (1) составят:

$R_{1\text{-}15} = 5{,}42;$	$R_{1\text{-}16} = 5{,}55;$	$R_{1\text{-}17} = 6{,}58;$	$R_{1\text{-}18} = 4{,}24;$
$R_{2\text{-}15} = 9{,}34;$	$R_{1\text{-}16} = 8{,}28;$	$R_{2\text{-}17} = 10{,}19;$	$R_{2\text{-}17} = 6{,}31;$
$R_{3\text{-}15} = 11{,}73;$	$R_{1\text{-}16} = 12{,}73;$	$R_{3\text{-}17} = 15{,}94;$	$R_{3\text{-}17} = 9{,}68;$
$R_{4\text{-}15} = 14{,}37;$	$R_{1\text{-}16} = 12{,}54;$	$R_{4\text{-}17} = 15{,}23;$	$R_{4\text{-}17} = 9{,}56;$
$R_{5\text{-}15} = 22{,}44;$	$R_{1\text{-}16} = 22{,}76;$	$R_{5\text{-}17} = 28{,}69;$	$R_{5\text{-}17} = 17{,}3;$
$R_{6\text{-}15} = 8{,}54;$	$R_{1\text{-}16} = 9{,}12;$	$R_{6\text{-}17} = 11{,}56;$	$R_{6\text{-}17} = 6{,}93;$
$R_{7\text{-}15} = 20{,}67;$	$R_{1\text{-}16} = 24{,}2;$	$R_{7\text{-}17} = 30{,}01;$	$R_{7\text{-}17} = 18{,}42.$

Общий риск R по отношению к учитываемому множеству дестабилизирующих факторов рассчитывают по формуле:

$$R = \sum_{i=1}^{m} \sum_{j=1}^{n} \nu_i \times R_{ij}$$

где m – число учитываемых дестабилизирующих факторов; k – число факторов; – значимость j-го фактора.

Тогда общий риск с учетом значимости факторов (например, $\nu_{15} = 0{,}3$; $\nu_{16} = 0{,}25$;$\nu_{17} = 0{,}3$;$\nu_{18} = 0{,}15$;) составит R = 97,88, что составляет примерно 14% от общей ценности.

Таким образом, когнитивные карты для типового объекта информатизации организации позволяют анализировать и прогнозировать состояние информационной безопасности организации в условиях действия различных дестабилизирующих факторов. Анализ информационных рисков позволяет, в свою очередь, выявить наиболее слабые места в системе защиты информации, оценить влияние потенциально существующих угроз, определить возможный ущерб от действия этих угроз и, в конечном итоге, минимизировать этот ущерб путем введения соответствующих контрмер.

Список литературы

1. Куканова, Н. Современные методы и средства анализа и управления рисками информационных систем компаний [Электронный ресурс]/Н. Куканова. Режим доступа: http://www.dsec.ru/about/articles/ar_compare/.
2. Борисов В.В., Круглов В.В., Федулов, А.С. Нечеткие модели и сети. – М.: Горячая линия – Телеком, 2007. – 284 с.
3. Васильев, В. И., Савина, И. А., Шарипова, И.И. Построение нечетких когнитивных карт для анализа и управления информационными рисками вуза – Вестник УГАТУ, №2 (27), 2008 г.

К ВОПРОСУ О РЕАЛИЗАЦИИ ИМИТАЦИОННОЙ МОДЕЛИ ЗЛОУМЫШЛЕННИКА

Петухов С.С. – студент, Пивкин Е.Н. – к.т.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Трудность исследования вопросов осуществления информационной безопасности в организациях усугубляет большая неопределенность условий функционирования объектов информатизации.

Решение этой задачи связано с высокой трудоемкостью процедур анализа и зависимостью конечного результата от субъективных факторов. Для чего необходимо разработать модель злоумышленника с учетом различных его характеристик: поведения, намерений присущих для различных типов злоумышленников. Успешное решение этих задач позволит учесть мотив, воздействующие факторы внешней среды для адекватной оценки защищенности объекта информатизации.

Существующие модели злоумышленников обладают следующими недостатками: не рассматривают мотивы злоумышленников, трудно реализуемы на ЭВМ [1]. Плохая формализация моделей злоумышленников и условий внешней среды приводит к невозможности автоматизации процесса их компьютерного представления, которое в значительной мере повысило бы качество систем анализа систем обеспечения безопасности.

В качестве инструмента для построения имитационной модели были выбраны средства имитационного моделирования (программный комплекс AnyLogic) [2-3].

В ходе анализа были выделены следующие основные характеристики нарушителя:

– тип нарушителя (ориентирован на успех \ ориентирован на избежание неудачи);

– задача нарушителя (угрозы реализуемые нарушителем);

– цель нарушителя (месть, нажива и т.д.);

– уровень подготовки нарушителя (Специалист \ Любитель \ Дилетант \ Сотрудник);

– уровень технической оснащенности нарушителя (Специалист \ Любитель \ Дилетант \ Сотрудник);

– вид нарушителя (внешний \ внутренний).

Логическая схема действий злоумышленника состоит из следующих основных блоков в системе имитационного моделирования AnyLogic (рисунок 1):

- pedSource1 – блок генерирующий поток внешних злоумышленников;
- pedSource5 – блок моделирующий появление внутренних злоумышленников;
- pedSource12 – блок моделирующий проникновение в помещение;
- pedCmdWait1 – блок моделирующий проведение атаки;
- pedSelectOutput6 – блок выбора дальнейший действий:
  - выход 1 – задержание злоумышленника;

- выход 2 – выход злоумышленника;
- выход 5 – выбор нового объекта для атаки;

– pedGoTo6-pedGoTo8 – модули моделирующие движение злоумышленника к выходам (главный либо пожарные);
– pedWait3 – блок моделирующий задержание злоумышленника;
– pedSink4 – блок уничтожающий модели злоумышленников созданные блоком pedSource1.

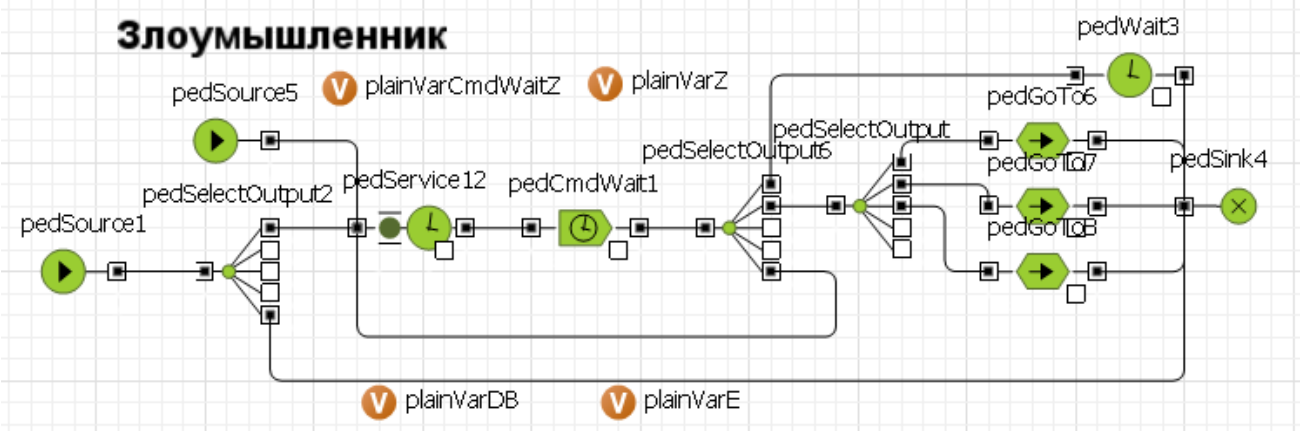


Рисунок 1 – логическая схема действий злоумышленника.

В «мониторе злоумышленников» отображены параметры реализации угроз злоумышленника:

– уровень подготовки злоумышленника;
– цель злоумышленника (номер помещения);
– наименование текущей атаки;
– минимальный уровень злоумышленника необходимый для проведения данной атаки;
– минимальное время необходимое на совершение атаки;
– минимальное время необходимое на устранение последствий атаки;
– ущерб, который будет нанесен объекту защиты (организации) при совершении атаки.

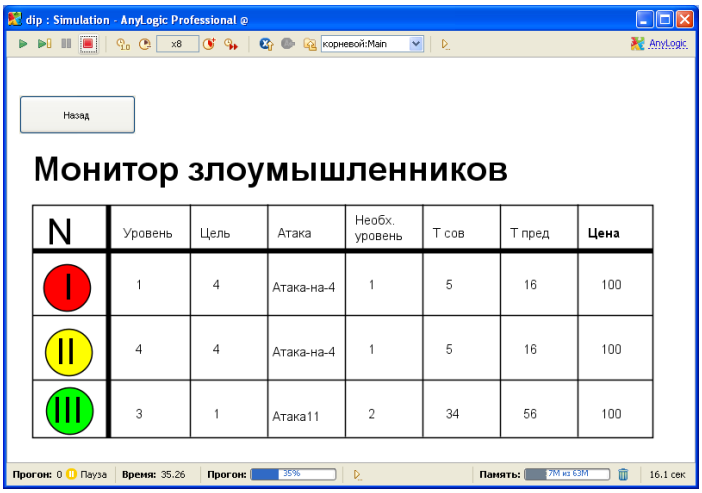


Рисунок 2 – Внешний вид «монитора злоумышленников»

В имитационной модели нарушителя сотрудник организации рассматривается как потенциальный внутренний нарушитель при наступлении определенных условий.

Логическая схема поведения сотрудника организации представлена на рисунке 3. Характеристики сотрудников организации:

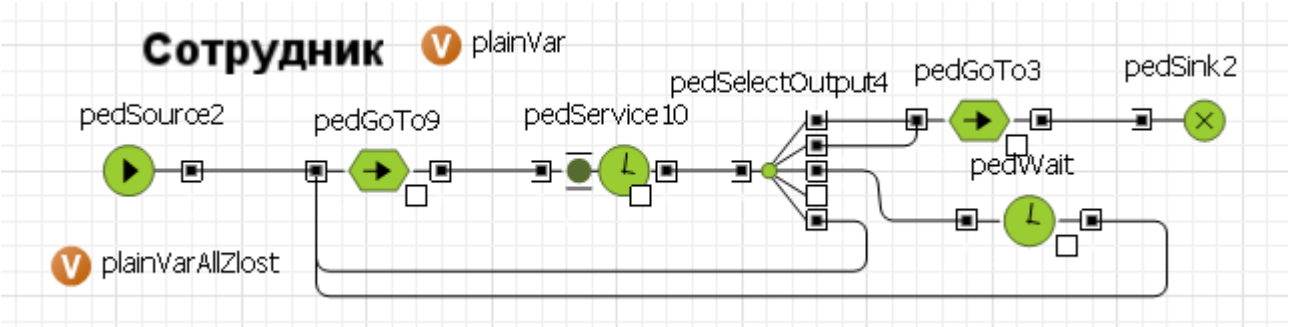


Рисунок 3 – Логическая схема поведения сотрудника организации

Схема сотрудника состоит из следующих основных блоков:

- pedSource2 – блок генерирующий поток сотрудников;
- pedGoTo9 – прохождение до выбранного помещения;
- pedService10 – блок моделирующий выполнение задания;
- pedSelectOutput4 – блок выбора дальнейшего события:
  - ветвь 1 – окончание рабочего дня (модельное время);
  - ветвь 2 – сотрудник стал внутренним злоумышленником;
  - ветвь 3 – обеденный перерыв;
  - ветвь 5 – переход к очередному заданию;
- pedGoTo3 – прохождение к выходу;
- pedWait – блок моделирующий обеденный перерыв;
- pedSink2 – блок уничтожающий сотрудников созданных в pedSource2.

По завершению модельного времени подсчитывают нанесенный и предотвращенный ущербы, количество срабатываний средств и систем защиты информации на попытки реализации угроз, распределение совершенных атак по уровню подготовки и техническому обеспечению злоумышленника, количество совершенных и предотвращенных атак, динамику изменения уровня защищенности объекта информатизации от атак злоумышленников.

Разработанная имитационная модель злоумышленника позволит проводить более эффективно осуществлять оценку уровня защищенности объекта информатизации, оценивать влияние дестабилизирующих факторов, что позволит анализировать информационные риски, выявлять слабые места объекта информатизации.

Список литературы

1. Саляхов А.Ф., Кардаш Д.И. Модель целенаправленного поведения злоумышленника. «Вопросы защиты информации» №1(76). 2007. – с. 8-10.
2. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. – СПб.: БХВ-Петербург, 2006. – 400 с.
3. Датьев И.О., Маслобоев А.В. Имитационное моделирование развития региональных информационно-коммуникационных систем. «Инфокоммуникационные технологии», Том 8, №2, 2010. – с. 51-56.

РАЗРАБОТКА ПРОГРАММНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЛАБОРАТОРНОЙ РАБОТЫ «БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ ZIGBEE» ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ СИСТЕМЫ»

Банщиков А.С. – студент
Алтайский государственный технический университет (г. Барнаул)

В современном мире уже никого не удивишь устройством беспроводной передачи данных. В нашу жизнь давно проникли технологии мобильной связи, интернета, систем спутниковой навигации. Однако лишь относительно недавно беспроводные сетевые технологии начали применяться в сферах коммунального хозяйства и промышленности. Причем, если в сфере коммунального хозяйства уже множество задач коммуникации решается с помощью беспроводных технологий (сбор показаний счетчиков воды/электроэнергии, управление освещением, сбор информации с разнообразных датчиков, построение системы «умный дом»), то в сфере промышленности аналогичные работы только начинаются. При этом эффективность от внедрения таких систем в промышленности очень высока, так как именно здесь насчитывается множество объектов автоматизации различной сложности, связь между которыми удобно осуществлять через беспроводные каналы. А в случае расположения части системы на движущихся объектах, как это может быть в автоматизированных складах, применение беспроводных сетей оказывается единственно возможным решением. До последнего времени внедрение этих технологий в промышленность сдерживалось из-за проблем, связанных с надежностью каналов связи в жестких условиях эксплуатации при большом уровне промышленных помех, а также с защитой беспроводных промышленных сетей от несанкционированного доступа. Сейчас ситуация кардинально меняется, и из области «экзотики» беспроводные промышленные сети переходят в область целесообразных технических решений.

Среди наиболее известных беспроводных технологий можно выделить: Wi-Fi, Wi-Max, Bluetooth, Wireless USB и относительно новую технологию - ZigBee, которая изначально разрабатывалась с ориентацией на промышленное применение. На рисунке 1 изображена зависимость скорости передачи данных с помощью определённой технологии от расстояния.

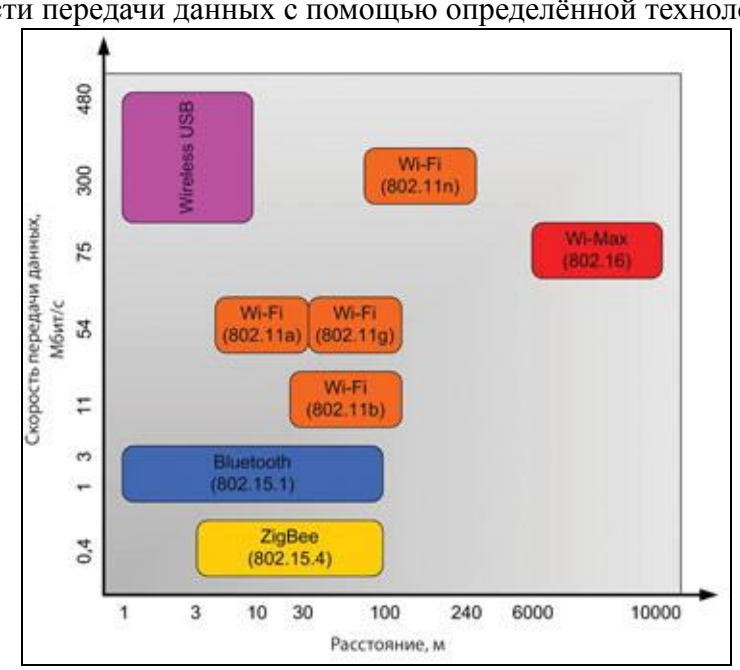


Рисунок 1

Каждая из этих технологий имеет свои уникальные характеристики, которые определяют

соответствующие области применения. Высокоскоростные технологии Wi-Fi, Wi-Max, Bluetooth, Wireless USB предназначены в первую очередь для обслуживания компьютерной периферии и устройств мультимедиа. Они оптимизированы для передачи больших объемов информации на высоких скоростях, работают в основном по топологии «точка-точка» или «звезда» и мало пригодны для реализации сложных разветвленных промышленных сетей с большим количеством узлов. Напротив, технология ZigBee имеет достаточно скромные показатели скорости передачи данных и расстояния между узлами, но обладает следующими важными, с точки зрения применения в промышленности, преимуществами:

1. Она ориентирована на преимущественное использование в системах распределенного мульти-микропроцессорного управления со сбором информации с интеллектуальных датчиков, где вопросы минимизации энергопотребления и процессорных ресурсов являются определяющими.
2. Предоставляет возможность организации самоконфигурируемых сетей со сложной топологией, в которых маршрут сообщения автоматически определяется не только числом исправных или включенных/выключенных на текущий момент устройств (узлов), но и качеством связи между ними, которое автоматически определяется на аппаратном уровне.
3. Обеспечивает масштабируемость - автоматический ввод в работу узла или группы узлов сразу после подачи питания на узел.
4. Гарантирует высокую надежность сети за счет выбора альтернативного маршрута передачи сообщений при отключениях/сбоях в отдельных узлах.
5. Поддерживает встроенные аппаратные механизмы шифрации сообщений AES-128, исключая возможность несанкционированного доступа в сеть. [1]

На данный момент на русском языке очень мало материалов, связанных с технологией ZigBee. Фактически существует всего порядка десяти оригинальных русских статей по этой технологии, основная масса информации по-прежнему находится в иноязычных источниках. Целью данной работы является разработка программно-технического обеспечения, которое поможет студентам в изучении основ построения ZigBee сетей на примере использования стартового набора AVR RZ RAVEN. Стартовый набор включает в себя два ZigBee-модуля, фактически являющиеся приёмопередатчиками с дополнительным функционалом (например, LCD-дисплеем, на который можно выводить необходимую информацию), а также в набор входит приемопередатчик RZUSBSTICK, но его можно подсоединить к персональному компьютеру через USB порт. Будут разработаны методические указания для проведения лабораторной работы; в них войдет полноценное описание беспроводной технологии ZigBee, построения ZigBee-сетей с использованием BitCloud-стека от компании Atmel, программирования ZigBee-модулей, а также порядок проведения работы. Всё это позволит студентам освоить навыки:

1. Использования отладочного комплекта STK-600 и интегрированной среды разработки AVR Studio для программирования микроконтроллеров.
2. Написания программ для любых ZigBee устройств фирмы Atmel, т.к. BitCloud стек является общим для всех линеек.
3. Построения простейшей ZigBee-сети для передачи данных между устройствами и персональным компьютером.

Список литературы

1. Незнамов Ю., Козаченко В. Перспективы использования беспроводных ZigBee – интерфейсов в электроприводе / Электронные компоненты. - 2008, №11

РАЗРАБОТКА WEB-ПРИЛОЖЕНИЯ ДЛЯ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОГО УЧЁТА

Казаков П.П. – студент
Алтайский государственный технический университет (г. Барнаул)

Информационный век немыслим без точного анализа и учёта ценностей, а ограниченность ресурсов привёла к тому, что человек просто обязан рационально относиться к имеющимся ценностям. Мы всё больше должны контролировать процессы учёта, быть ответственными и принимать решения, относящиеся к тем или иным процессам.

Проблемой является локализированный учёт материально-технических ценностей. Бухгалтерский учёт ценностей не может дать точных данных о ценностях, которые после своего поступления формально списываются и не присутствуют ни в каких документах. Руководителю для того, чтобы оценить свои ресурсы подразделения или организации на текущий момент, требуется полная и точная информация обо всех имеющихся ценностях, которые присутствуют и отсутствуют, чтобы принять верное решение о необходимости приобретения для проведения соответствующих работ.

На сегодняшний день существуют в области материально-технического и складского учёта , которые могут применяться в данном сегменте. Однако они не подходят для решения вышеупомянутых задач, так как не учитывают всех особенностей предметной области и требований для многопользовательского режима доступа к данным.

Подобные продукты на рынке выпускаются под заказ, но стоят они довольно дорого и обслуживание системы требует специализированного обучения.

Предлагаемое решение по созданию информационной системы материально-технического учёта просто в администрировании и интуитивно понятно обычному пользователю. Сочетание в ней бесплатных продуктов программного обеспечения(MySQL) и детального моделирования процессов позволило создать мощное и гибкое приложение. Данное решение поддерживает технологию клиент-сервер для удобного и распределённого доступа к базе данных материально-технического учёта.

Архитектура клиент-сервер имеет следующие достоинства:

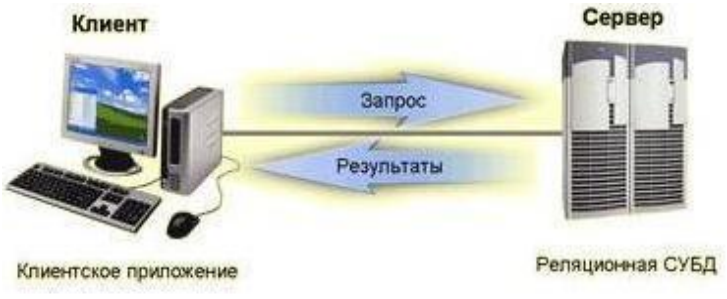


Рисунок 1. Архитектура клиент-сервер

1. Большинство вычислительных процессов происходит на сервере; таким образом, снижаются требования к вычислительным мощностям компьютера клиента;
2. Снижается сетевой трафик за счет посылки сервером клиенту только тех данных, которые он запрашивал;
3. Упрощается наращивание вычислительных мощностей в условиях развития программного обеспечения и возрастания объемов обрабатываемых данных
4. БД на сервере представляет собой, как правило, единый файл, в котором содержатся таблицы БД, ограничения целостности и другие компоненты БД. Взломать такую БД, даже при наличии умысла, тяжело;
5. Сервер реализует управление транзакциями и предотвращает попытки одновременного изменения одних и тех же данных;

На данный момент для разрабатываемой информационной системы материально-технического учёта создана концептуальная модель базы данных представленная на рисунке 2.

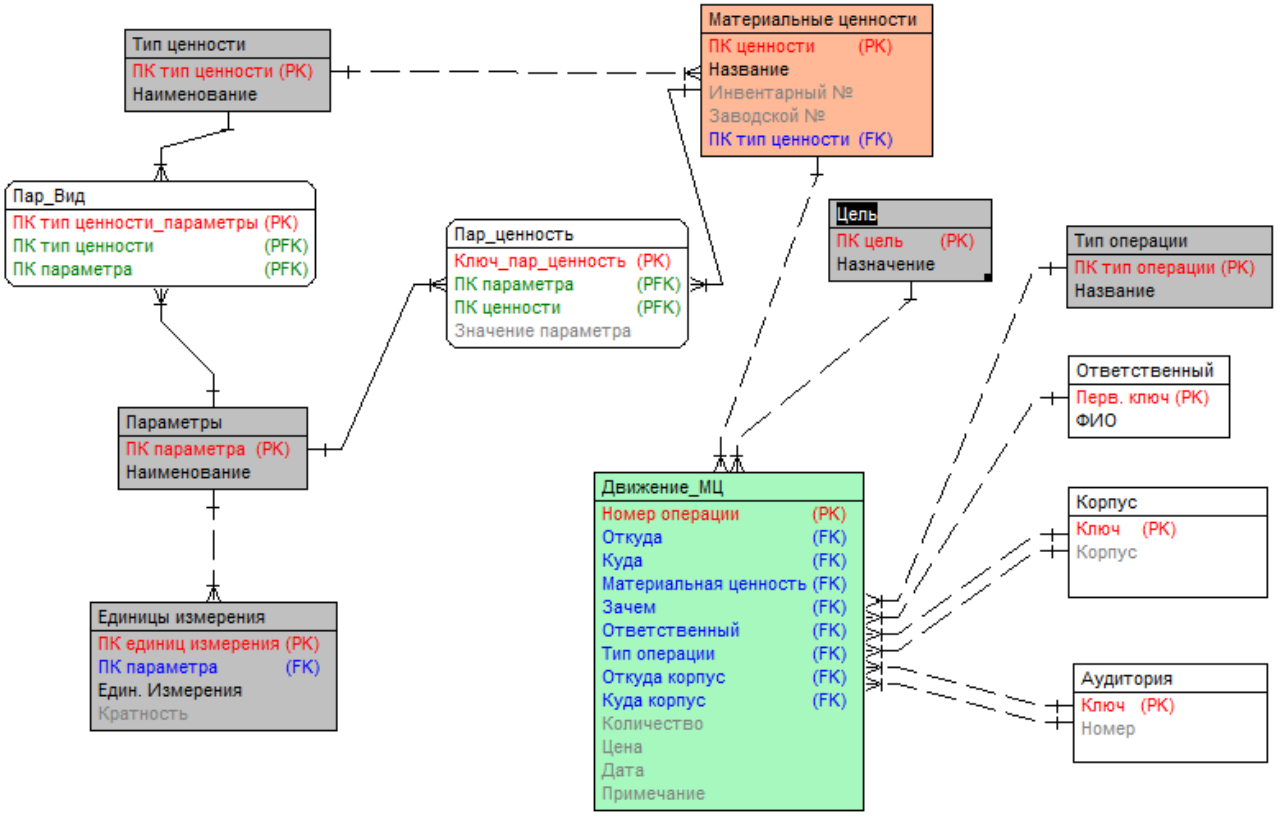


Рисунок 2 − Концептуальная модель

Каждое действие, совершенное над предметом, должно фиксироваться в информационной системе. Это способствует улучшению анализа ценностей и уменьшает вероятность того, что какие бы то ни было материальные ценности пропадут бесследно. Данная информационная система разрабатывается для организации материально-технического учёта на кафедре ВСИБ АлтГТУ.
Проведя некоторые изменения в данной модели, её можно легко адаптировать для материально-технического учёта на других предприятиях.

Список литературы

1. Маклаков С.В. Разработка и внедрение информационных систем [Электронный ресурс] / С.В. Маклаков, Е.Н. Павловская // Режим доступа: http://www.betec.ru/process

ВЫБОР КОМПОНЕНЕНТНОЙ БАЗЫ ДЛЯ АВТОМАТИЗИРОВАННОГО ЭЛЕКТРОКАРДИОГРАФА

Кайгородов А.В. – студент, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Современная функциональная диагностика обладает обилием средств, которые позволяют находить различные заболевания на разных стадиях. Самым распространённым способом диагностики является электрография, в том числе и электрокардиография.

С точки зрения электротехнической составляющей мы сталкиваемся с проблемой усиления слабого сигнала. Дело в том, что наше сердце в разные моменты времени и в зависимости от того, в какой фазе сокращения мышц оно находится, вырабатывает

электрические импульсы, которые и необходимо детектировать. Основной проблемой здесь является усиление слабого уровня сигнала, который для сердечных импульсов составляет порядка 5 мВ. Кроме того своё влияние сказывает постоянная составляющая ±300 мВ, которая возникает в результате кожно-гальванической реакции. Чтобы получить достаточный уровень для оцифровывания нам необходимо усилить сигнал в 500 – 1000 раз. Это означает, что при наличии шума на входе этот шум будет также усилен в 500-1000 раз, что по очевидным причинам не должно быть допустимо, ибо может сказать своё влияние и осложнить последующий анализ. Это означает, что нам необходимо отфильтровать сигнал на входе и после прохождения всех фильтров должны получить наиболее чистый сигнал. Однако если уровень шумов будет не много меньше, чем полезный сигнал, то в таком случае мы можем прибегнуть к реализации алгоритмов фильтрации на компьютере и последующей выдаче результатов на экран.

Ранее на кафедре ВСиБ существовала разработка кардиографа ЕФКР-4 1992 года. Однако, учитывая современные тенденции развития техники, и концепции приборостроения, эта разработка мрально и физически устарела. В связи с этим было принято решение о создании электрокардиографа на современной элементной базе. Очевидными критериями являются: пониженное энергопотребление прибора, высокое быстродействие, простота обслуживания, малые габариты, возможность подключения к компьютеру посредством интерфейса USB.

Наиболее простым и распространённым способом построения приборов, усиливающих слабый сигнал, является построение приборов на инструментальном усилителе. Как правило, для кардиологии достаточно таких инструментальных усилителей, как AD620, AD623, INA114. Типовая схема усиления кардиосигнала состоит из инструментального усилителя, и прецизионного быстродействующего усилителя. Операционный усилитель, получает на вход сигнал и контролирует коэффициент усиления с помощью резистора, параллельно которому подключена точка среднего потенциала, которая через фильтр ведёт на быстродействующий операционный усилитель. Быстродействующий ОУ необходим для подавления синфазной составляющей.

В ходе проведения практических исследований была обнаружена проблема наводок и шумов, которые попадают на вход инструментального усилителя. Т.к. полезный сигнал (кардиосигнал) лежит в диапазоне до 200 Гц, то на вход было решено поставить RC-фильтр второго порядка, который бы выделил из всего сигнала, поступающего на вход, только необходимый, полезный сигнал. Кроме того, во избежание биений, поставлены сглаживающие конденсаторы, на 0.1 мкФ. А также, чтобы не допустить появление паразитных емкостей между контактами во время построения тестовой платы между ними была проведена земля. Кроме того, если сделать землю замкнутой, то в таком случае мы получаем контур, в котором согласно закону электромагнитной индукции начинает возникать ЭДС самоиндукции, которая, естественно сказывает своё влияние на сигнал.

Фактически прибор получается разделённым на 2 структурные части: аналоговую, которая занимается усилением сигнала и цифровую, которая занимается оцифровкой аналоговых данных и последующей их передачей в компьютер. В цифровой части есть несколько способов реализации. Одним из известных и наиболее распространённых в применении способов является использование Сигма-дельта АЦП, однако это довольно дорогой способ. Вторым способом, который был положен в основу работаты тестовой установки кардиографа, является использование АЦП, встроенного в микроконтроллеры серии AtmegaX, скажем Atmega8. Этот способ позволяет добиться приемлемых результатов при меньших затратах. Десятибитного АЦП, встроенного в микроконтроллер вполне достаточно, чтобы перекрыть полный диапазон усиливаемого сигнала.

Для указанного контроллера была разработана программа, реализующая работу с АЦП и непосредственную передачу данных в компьютер для последующего анализа и вывода информации в графическом виде. Суть протокола передачи данных следующий: компьютер передаёт микроконтроллеру номер канала, с которого хочет получить данные, микроконтроллер снимает данные с АЦП и отправляет их на компьютер в виде 3х байт. В

первых двух байтах хранятся непосредственно оцифрованные данные, а третий несёт на себе информационную нагрузку. В нем хранится CRC и номер канала, с которого пришли данные. Это не окончательная версия алгоритма работы с АЦП. В ближайшем будущем планируется сократить количество отправляемых байтов и переделать логику взаимодействия компьютера с кардиографом. Компьютер будет инициализировать соединение с устройством, которое получит 1 байт информации, в котором будет храниться битовая маска с указанием каналов, с которых будет сниматься сигнал. Устройство будет пересылать данные с указанных каналов до тех пор, пока не получит команду останова.

Полученные данные можно пропустить через ряд адаптивных фильтров, на ПО, работающем на компьютере, тем самым сняв необходимость просчёта каких либо результатов на микроконтроллере и переложив эту задачу непосредственно на ПК. За счёт этого мы можем получить компактный недорогой кардиограф.

РАЗРАБОТКА СИСТЕМЫ ОХРАННОЙ СИГНАЛИЗАЦИИ С ЖУРНАЛИЗАЦИЕЙ СОБЫТИЙ

Клейменов В.В. – студент, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Система контроля доступа (СКУД) - совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также оперативный контроль перемещения персонала и времени его нахождения на территории объекта. Действительно, СКД это не только аппаратура и программное обеспечение, это продуманная система управления движением персонала. Но не стоит забывать, что эффективность использования любых технических средств зависит от применяемой технологии контроля доступа и квалификации оперативно-технического персонала. Роль человеческого фактора в конечном итоге может привести к неэффективному использованию самых передовых технических решений. Поэтому особого внимания заслуживает степень автоматизации процессов управления доступом, контроля действий персонала объекта и прогнозирования нештатных ситуаций. Следует констатировать, что возможность проведения аналитической работы с использованием современных программно-аппаратных платформ является необходимой качественной характеристикой СКУД.

Основными целями создания такой системы являются:

- защита законных интересов предприятия, поддержание порядка внутреннего управления;
- защита собственности предприятия, ее рациональное и эффективное использование;
- внутренняя и внешняя стабильность предприятия;
- защита коммерческих секретов и прав на интеллектуальную собственность.

Обобщенная структурная схема данной системы представлена на рисунке 1.

Рисунок 1 − общая схема устройства

В качестве идентификаторов будут выступать цифровые пароли и ключи iButton что позволит достигнуть таких целей как :

- добавление в базу данных ключей уже имеющихся у сотрудников, что позволит сократить риск утери данного ключа,
- выдача цифровых паролей сотрудникам, которым разрешён вход только один раз либо в течении определённого промежутка времени.

Важным моментом является роль персонального компьютера в данной системе. Все события в системе заносятся в журнал, хранящийся в памяти контроллера. При возникновении такой необходимости оператор осуществляет обмен информацией между ПК и контроллером, при этом ПК получает данные из журнала событий а также базу данных идентификаторов пользователей. Получив эту информация оператор может осуществлять различные манипуляции с системой:

- добавление новых цифровых паролей, так же редактирование и удаление уже имеющихся в базе,
- просмотр, обработку и анализ данных из журнала событий, что позволяет осуществлять необходимые действия в случае нештатных ситуаций, а так же получать необходимые статистические данные.

Роль исполнительного устройства выполняет электромеханический замок. Использование именно этого устройства позволяет в случае возникновения необходимости осуществить открытие/закрытие с помощью обычного ключа от замка.

Из всего выше сказанного следует что данная модель системы охранной сигнализации сочетает в себе функции автономных систем и некоторые функции сетевых систем, что является выгодным при необходимости СКУД малых размеров.

Список литературы

1. Тексты документов ГОСТ Р 51241-2008 и ГОСТ Р 51558-2008.
2. Ворона В.А., В.А. Тихонов. Системы контроля и управления доступом. Москва: Изд-во Горячая линия-Телеком, 2010 г. - 270 с.
3. Уокер Ф. Электронные системы охраны. Пер. с англ. М.: «За и против», 2009, 288 с.

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОГО МОДУЛЯ УПРАВЛЕНИЯ ОСВЕЩЕНИЕМ В УЧЕБНОЙ АУДИТОРИИ

Николенко Е.Ю. – студент, Сучкова Л. И. – к.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

В современном мире освещение общественных зданий представляет собой одно из наиболее перспективных направлений светотехники. Эта область предоставляет возможности для применения новейших осветительных технологий с современными средствами дизайна. В условиях ограниченности и исчерпаемости энергоресурсов, а также при ухудшении экологической обстановки за счет загрязнения атмосферы и водного бассейна отходами электростанций проблема рационального использования вырабатываемой электроэнергии приобретает особую актуальность.

Система автоматического управления освещением на основе микроконтроллера позволяет значительно снизить энергозатраты, а также автоматизировать процесс включения и выключения осветительных приборов без участия человека, что позволяет повысить удобство пользования данной системой.

Структурная схема автоматизированной системы управления освещением представлена на рисунке 1.

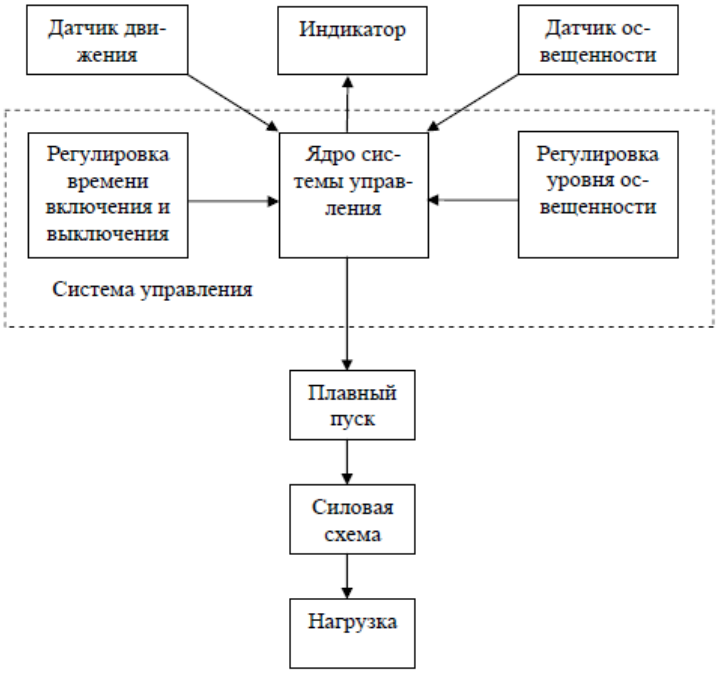


Рисунок 1 – структурная схема устройства

Данная система предусматривает работу осветительных устройств в зависимости от состояния окружающей среды.

Разрабатываемое устройство состоит из датчиков движения и освещенности, схемы управления и силовой схемы, к которой подключается загрузка. В схеме реализована возможность регулирования времени включения и выключения, а также уровня освещенности.

Сигналы с датчиков движения и освещенности поступают в схему управления. В ней происходит обработка полученной информации и вырабатывается управляющее воздействие. Оно подается на силовую схему и подключенные к ней нагрузки в виде устройств освещения. Регулировка времени задержки на включение необходима для избегания ложного срабатывания устройства и срабатывания при кратковременном появлении объекта в зоне определения датчика.

Задержка на выключение нужна для обеспечения работы нагрузки в случае временного исчезновения объекта из рабочей области ИК-датчика. Регулировка уровня освещенности служит для настройки устройства на заданный уровень освещенности при монтаже в аудитории и его использовании. С помощью индикатора осуществляется визуальный контроль процесса настройки устройства, а также индикации его включения в сеть.

Устройство плавного пуска используется только совместно с лампами накаливания, что позволяет предотвратить резкие скачки напряжения и увеличить их срок службы.

Список литературы

1. Системы автоматического управления освещением зданий [Электронный ресурс] / Режим доступа: http://www.nppsaturn.ru/suncheek.htm
2. ИнтернетДом – создание и проектирование систем «Умный дом» [Электронный ресурс] / Режим доступа: http://www.i-dom.ru/
3. Умный дом своими руками [Электронный ресурс] / Режим доступа: http://www.ixbt.com

СИСТЕМА ФАСЕТНОЙ КЛАССИФИКАЦИИ ДЛЯ СЕТЕВОЙ АРХИТЕКТУРЫ ХРАНЕНИЯ ДОКУМЕНТОВ

Петров А.С. – студент
Алтайский государственный технический университет (г. Барнаул)

На данный момент в любой организации стает проблема большого количества документов. Чем больше документов, тем сложнее в них ориентироваться и обмениваться ими. Общепринятые классификации не всегда подходят человеку, ведь проще ориентироваться в документах, классифицируя их, так как это удобно. Для решения этой проблемы существует большое количество программных продуктов, но все они обладают большим количеством минусов. Это может быть неудобный интерфейс, отсутствие возможности работы в локальной сети или отсутствие возможности разграничивать права доступа к данным.

Система фасетной классификации для сетевой архитектуры хранения документов лишена указанных недостатков. Данная система реализована на архитектуре «клиент - сервер», что дает возможность снижения нагрузки на сеть и сосредоточения данных на сервере.

Объектная модель базы данных данной системы представлена на рис. 1.

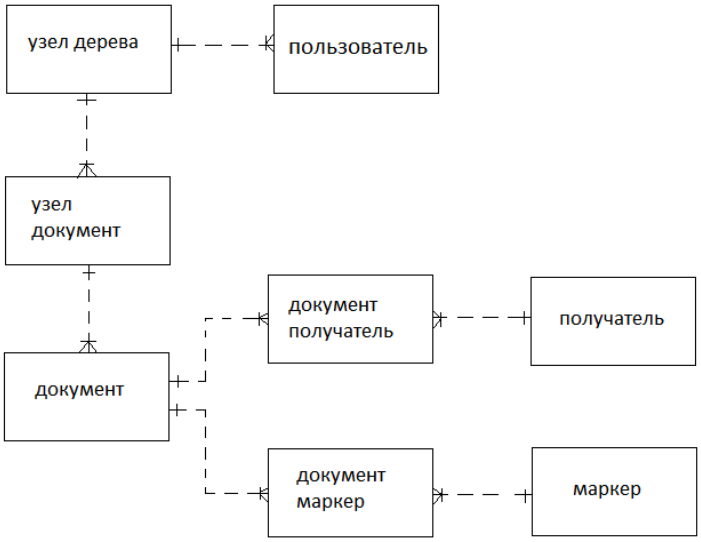


Рисунок 1 − Объектная модель базы данных

Система поддерживает два вида пользователей «администратор» и «гость». В связи с этим каждый пользователь входя в систему должен пройти авторизацию и аутентификацию. «Администраторы» имеют возможность редактировать древо принадлежности, добавлять и удалять документы из базы данных. У «гостей» эти возможности отсутствуют, они имеют собственный профиль классификации документов, который может изменить только «администратор».

В данном программном продукте присутствует система оповещения, то есть при добавлении в базу данных нового документа все пользователи оповещаются об этом и им предоставляется возможность выбрать узел дерева принадлежности, к которому будет привязан данный документ.

Система поддерживает тегирование документов. Любой документ можно пометить маркером либо добавить «получателя», которому необходимо отправить документ.

Благодаря этому программа имеет систему поиска документов. Документы можно искать по их названию, маркеру и получателю.

Система фасетной классификации для сетевой архитектуры хранения документов обладает многооконным интерфейсом, в котором используются только стандартные элементы управления. Это позволяет пользоваться программой пользователям любого уровня.

В процессе проектирования и реализации системы фасетной классификации были решены следующие задачи:

- реализована система фасетной классификации на архитектуре «клиент - сервер»
- спроектирована структуру базы данных;
- разработан эргономичный дизайн пользовательского интерфейса;
- реализовано деление пользователей на две группы («администраторы» и «гости»), их авторизация и аутентификация;
- реализован собственный профиль документов для группы «гости»;
- реализована фасетная классификация документов для группы «администраторы»;
- реализовано добавление, удаление, изменение документов;
- реализована система оповещения о добавлении нового документа;
- реализовано добавление и удаление тэгов документов («маркеры» и «получатели»);
- реализована систему поиска документов по названию, «маркеру» и «получателю».
- протестирована работа системы в локальной сети;

Список литературы

1. Организация архивного хранения электронных документов: проблемы [Электронный ресурс] / Режим доступа: http://www.alee-archive.ru/page.jsp?pk=node_100078
2. Классификация документов по различным признакам [Электронный ресурс] / Режим доступа: http://www.mybntu.com/general/delo/klassifikaciya-dokumentov-po-razlichnym-priznakam.html

МЕТОДЫ ИЗМЕРЕНИЯ СКОРОСТИ И НАПРАВЛЕНИЯ ВЕТРА

Плотников А.Д. – студент, Сучкова Л.И – к.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Проблема измерения скоростей воздушных потоков и определения направления их перемещения актуальна в промышленности, в медицине, в системах экологического мониторинга, в системах автоматического управления вентиляцией, в системах климат-контроля.

Существует несколько методов измерения скорости воздушных потоков, каждый из которых может быть применен в любой из сфер. Все методы можно разделить по физической идее на пять групп [1]:

а) методы, основанные на использовании энергии потока:
   1) методы, использующие переменный перепад давлений,
   2) методы, использующие измерение крутящего момента,
   3) методы, использующие явление обтекания.

б) тепловые методы:
   1) методы, использующие измерение температуры нагретого тела, помещаемого в поток (термоанемометры),

2) методы, использующие измерение температуры потока, нагреваемого нагревателем (теплокалориметры).

в) методы, основанные на введении в поток невесомой метки и измерении ее скорости:

1) методы, использующие впрыскивание порции иного состава, цвета,
2) методы, использующие намагничивание,
3) методы, использующие ионизацию,
4) методы, использующие подогрев,
5) акустические (условно).

г) корреляционные методы.

д) оптические методы.

Основными методами определения направления ветра являются флюгерный и акустический.

Наряду с крыльчатыми анемометрами и термоанемометрами большую популярность завоевывают ультразвуковые. Их преимуществами являются:

- отсутствие трущихся и движущихся деталей конструкции, что исключает износ;
- высокая точность измерения;
- высокая чувствительность;
- независимость от внешних факторов среды;

На базе акустического анемометра возможно создание прибора для определения направления воздушного потока. Такой прибор выгодно отличается от флюгера отсутствием механических вращающихся частей в конструкции.

В связи с перечисленными преимуществами акустических анемометров было принято решение по созданию прибора, работа которого основана именно на акустическом методе.

В качестве первичных преобразователей должны использоваться ультразвуковые датчики, работающие в диапазоне ультразвука низких частот 15-100 кГц, т.к. звуковые волны именно таких частот имеют наименьшее затухание при перемещении в воздушной среде [2]. Для применения анемометра в уличных условиях на открытом воздухе УЗ датчики должны иметь герметичную конструкцию. Под эти требования подходят УЗ датчики производителей Murata и Audiowell:

- датчик MA80A1 – производитель Murata, частота – 75 кГц, диапазон рабочих температур - -10…+60°C, время затухания – 1.2 мс, направленность - 40°;
- датчик MA40E7 – производитель Murata, частота – 40 кГц, диапазон рабочих температур - -30…+85°C, время затухания – 1.5 мс, направленность - 100°;
- датчик T/R40-18U – производитель Audiowell, частота – 40 кГц, диапазон рабочих температур - -40…+80°C, время затухания – 1.3 мс, направленность - 80°;
- датчик T/R40-16B – производитель Audiowell, частота – 40 кГц, диапазон рабочих температур - -40…+80°C, время затухания – 1.2 мс, направленность - 70°.

В разработанном приборе применялись датчики T/R40-18U. Выбор обосновывается сочетанием широкого диапазона рабочих температур и широкого угла направленности.

Разработанный прибор позволяет проводить измерение скорости воздушного потока в трех измерениях.

Список литературы

1. Шкундин С.З. Состояние и перспективы развития анемометрии в угольной промышленности. [Электронный ресурс] / С.З. Шкундин, О.А. Кремлёва, А.Л. Иванников // Режим доступа: http://www.sirsensor.ru/art_3.htm
2. Красильников В.А. Звуковые и ультразвуковые волны в воздухе, воде и твердых телах [Текст] // В.А. Красильников - М.: Государственное издательство физико-математической литературы, 1960. – 558 с.

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ПОРТАТИВНЫХ МЕТЕОСТАНЦИЙ

Попов А.Е. – студент
Алтайский государственный технический университет (г. Барнаул)

В настоящее время большую популярность получили домашние метеостанции. При невысокой цене они обеспечивают достаточно надежные данные.

Естественно, домашняя цифровая метеостанция не в состоянии подготовить прогноз погоды с такой вероятностью и надежностью, что Гидрометцентр. Прогноз погоды научных метеостанций основан на данных от всех станций, в том числе и заграничных, анализируются воздушные потоки, глобальные атмосферные явления и тому подобное и так далее, они оснащены дорогостоящим оборудованием. Но немало пользы могут принести и маленькие домашние метеостанции, помещающиеся на кухонном столе.

Портативная метеостанция состоит из двух основных компонентов: базы и метеодатчика. Погодная станция, которая является базой, находится в комнате на полке или в офисе на столе и информирует пользователя обо всех изменениях температуры в самом помещении. Питание базы погодной станции осуществляется от сети, либо от батареек в зависимости от модели. Можно устанавливать от одного до нескольких, каждый из них будет отдельно высылать свою сводку температурных режимов, влажности и других показателей. Чтобы вывести на экран нужную информацию достаточно просто выбрать один из датчиков. После установки погодных датчиков следует пропинговать их (дать метеостанции обнаружить связь с ними). Метеодатчику не страшны осадки, перепады температур и внешние атмосферные воздействия.

Метеостанции различаются не только по функционалу, но и по дизайну и внешнему виду. Порой трудно сделать правильный выбор домашней метеостанции. И чтобы метеостанция больше отвечала бытовым функциям и удобствам пользователя, зачастую ее совмещают с полезными бытовыми приборами. Портативные метеостанции Oregon отличаются ярким креативным дизайном, и помимо своих основных функций погодного информера, метеостанция становится элементом дизайна и украшением интерьера.

- Метеостанция часы-будильник. Почти все популярные метеостанции, помимо погодного информера совмещают в себе функцию часов с календарем и будильника. Некоторые модели делают записи погодных сводок по числам календаря, затем выявляют минимальные и максимальные отклонения температуры за определенный месяц и год.

- Метеостанция с проекционными часами. Проекция времени и погодных данных осуществляется направленным лазерным световым лучом на стену или любую ровную поверхность. Более четко и хорошо проекция просматривается ночью, но некоторые проекционные часы с метеостанцией имеют функцию дневного усиления проекции. Цвет проекции луча чаще всего красный, но бывают и другие цвета.

- Метеостанции с трехмерным изображением. Такие метестанции по функциональности ничем не отличаются от других погодных станций, но отображение времени, данных и погодных пиктограмм (солнце, облака, дождь, снег) происходит в специальной трехмерной прозрачной области. Такой способ информирования не так многофункционален, но оригинален и красив по дизайну.

- Fm-радиоприемник с метеостанцией. Бытовой прибор совмещающий метеостанцию и FM-радиоприемник для приема радиосинала fm частоты; удобен и полезен как в быту, так и на работе в офисе. Принцип работы тот же, просто в базу погодной станции с выносным метеодатчиком встроен еще и fm-приемник.

- Телефон со встроенной метеостанцией. Радиотелефон совмещающий бытовую метеостанцию - работает как обычный телефон от импульсного и тонального набора. При этом на большом жк экране отображаются данные с внешнего метеодатчика, расположенного за окном, и с датчика, встроенного в сам телефон.

Все погодные метеостанции имеют одну удобную функцию. Чтобы узнать погоду перед выходом на улицу, не надо тратить время на прослушивание прогноза погоды по радио или тв, заходить в интернет или выглядывать за окно и высовывая намоченный палец. Достаточно просто взглянуть в полную сводку на экране метеостанции, чтобы полностью быть готовым к погодным условиям улицы.

По поводу того, какое огромное значение люди придают прогнозу погоды, в одной книге иронизировал писатель Фазиль Искандер. Крик: «Потише! Погоду передают! » паренька с юга, прибывшего в 60-е в Москву, заставлял удивляться. Верно, к чему интересоваться прогнозом погоды на морском побережье? Она же всегда хорошая и замечательная. Впрочем, информация о завтрашней погоде для обитателей более жестких мест в климатическом плане имеет огромное значение. Выходя с утра на работу, редко когда человек не поинтересуется прогнозом погоды по телевидению или радио и не посмотрит на термометр. Гидрометцентр, от которого мы получаем прогноз погоды, располагается в Москве. Это государственная служба, ее метеостанции, располагающиеся по всей стране, собирают сведения о состоянии атмосферы, на основе которой и создается прогноз. Весьма популярны и обыкновенные уличные термометры, которые мы, как правило, крепим на раму окна с наружной стороны. Но сегодня развитие электроники сделало возможным делать - цифровые домашние метеостанции, устройства, которые в принципе способны получить прогноз погоды прямо у вас в квартире.

РАЗРАБОТКА АЛГОРИТМА ДЛЯ МОДЕЛИРОВАНИЯ И ИССЛЕДОВАНИЯ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ЭЛЕКТРОЭНЕРГИИ

Серебряков А.С. – студент, Сучкова Л.И. – к.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Среди многочисленных видов товаров, которыми мы пользуемся повседневно, есть и такой, как электроэнергия. Электроэнергия как товар обладает целым рядом специфических свойств. Она непосредственно используется при создании других видов продукции и оказывает существенное влияние на экономические показатели производства и качество выпускаемых изделий. Стандарты устанавливают допустимые уровни помех в электрической сети, которые характеризуют качество электроэнергии (КЭ) и называются показателями качества электроэнергии (ПКЭ). Существуют задачи мониторинга КЭ, требующие использования специальных приборов контроля качества.

Цель работы – разработка алгоритма расчета ПКЭ, а также создание программы, эмулирующей работу прибора, измеряющего ПКЭ.

Определение ПКЭ задача нетривиальная, так как большинство процессов, протекающих в электрических сетях – быстротекущие, все нормируемые ПКЭ не могут быть измерены напрямую – их необходимо рассчитывать, а окончательное заключение можно дать только по статистически обработанным результатам. Поэтому, для определения ПКЭ, необходимо

выполнить большой объём измерений с высокой скоростью и одновременной математической и статистической обработкой измеренных значений.

ПКЭ рассчитываются программно на основе мгновенных значений напряжения.

Описываемый программный продукт разработан в среде Microsoft Visual Studio 2008 Team System на языке C# с использованием технологии .NET. Для изображения графиков сигналов использована библиотека ZedGraph. Быстрое преобразование Фурье выполняется с помощью функций, описанных в библиотеке algLib.

Приложение представляет собой экранную форму с расположенными на ней элементами управления и меню (рисунок 1).

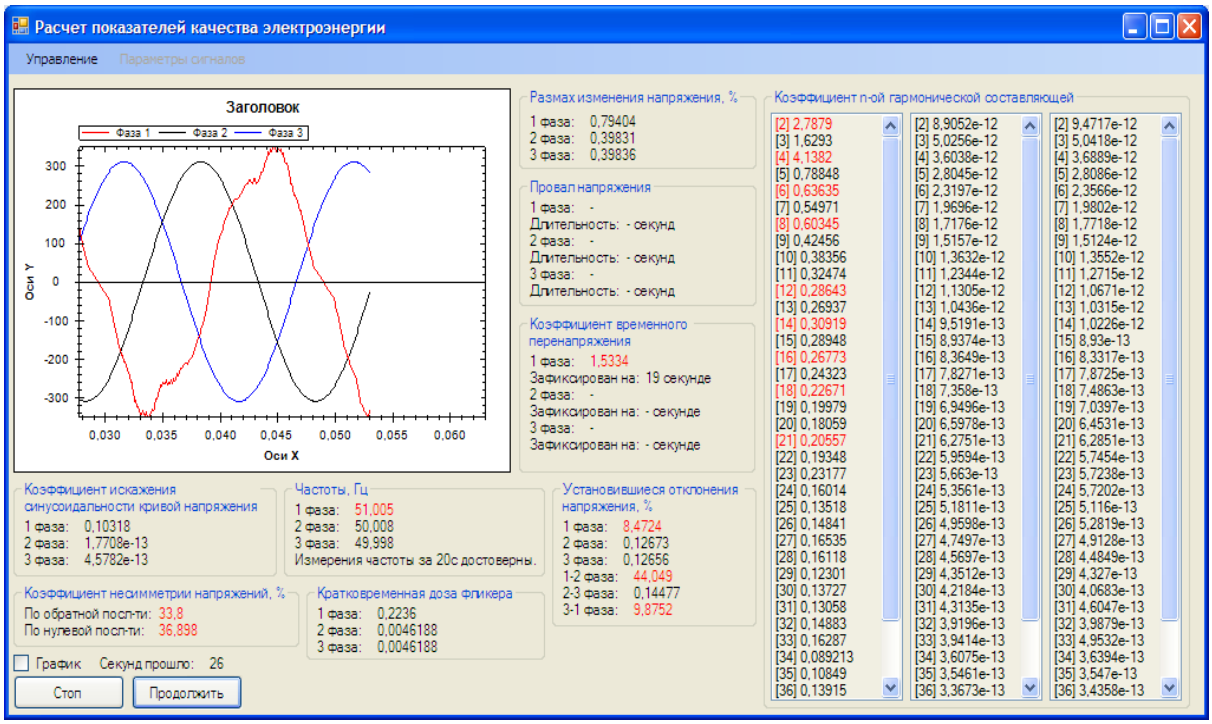


Рисунок 1 – Вид главной формы программы

Главная форма отображает ПКЭ, нормируемые ГОСТ 13109-97: коэффициент искажения синусоидальности кривой напряжения, частоту сигналов, коэффициент несимметрии напряжений по обратной и нулевой последовательностям, кратковременную дозу фликера, размах изменения напряжения, провал напряжения, коэффициент временного перенапряжения, установившееся отклонение напряжения, коэффициент n-ой гармонической составляющей. Если значение какой-либо величины превысило нормально допустимое значение, то это значение на форме выделятся красным шрифтом. Также отображаются графики сигналов, счетчик секунд и кнопки управления процессом расчета и элементом управления, служащим для разрешения и запрещения отрисовки графиков.

Меню служит для управления работой программы и для вызова окна настроек, изображенного на рисунке 2.

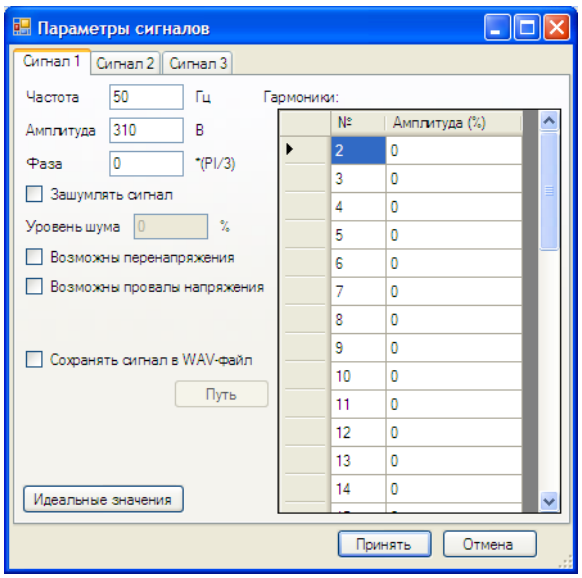


Рисунок 2 – Окно настроек программы

С помощью окна настроек есть возможность задавать параметры всех сигналов, такие как: частота, амплитуда, фаза, шумы, перенапряжения, провалы напряжения, а также амплитуды гармоник со второй по сороковую. Кроме того возможно восстановить значения по умолчанию, которые являются идеальными.

Может возникнуть необходимость в выводе генерируемых программой сигналов на звуковую карту компьютера, например, с целью тестирования аппаратно реализованного измерителя показателей качества электроэнергии. Для этого в программе предусмотрена запись сигналов в звуковой файл в формате WAV. При этом имеется возможность сохранять как все сигналы в один файл, так и каждый сигнал в отдельный файл.

Таким образом, в ходе работы была написана программа, эмулирующая работу прибора, рассчитывающего ПКЭ. К основным возможностям программы следует отнести: расчет ПКЭ в зависимости от параметров сигналов, которые можно изменять, сохранение сигналов в WAV-файл, вывод графиков сигналов.

Список литературы

1. Ефименко Ю.Г. Качество электроэнергии [Электронный ресурс] / Ю.Г. Ефименко. Режим доступа: http://home.onego.ru/~enadz/kachenerg.htm
2. ГОСТ 13109 – 97. Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения. – М. Изд-во стандартов, 1998.
3. Воронов И. Анализатор качества электроэнергии [Электронный ресурс] / И. Воронов. Режим доступа: http://powerdsp.narod.ru/analizatorkachestva/measpar.pdf
4. Павловская Т.А. C#. Программирование на языке высокого уровня. [Текст] / Т.А. Павловская. – СПб.: Изд-во Питер, 2009. – 432 с.
5. Гросс К. C# 2008 и платформа .NET 3.5 Framework: вводный курс. [Текст] / К. Гросс. – Изд-во Вильямс, 2009. – 480 с.

ПРОЕКТИРОВАНИЕ ОБЩЕГОРОДСКОЙ СЕТИ СБОРА И АНАЛИЗА ДАННЫХ УЧЁТА ТЕПЛОВОЙ И ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ

Синеев И.А. – студент, Сучкова Л.И. – к.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Проблема снятия показаний приборов учёта тепловой и электрической энергии актуальна для многих организаций, занимающихся обслуживанием этих приборов учёта. Особенно актуальна эта проблема стала после принятия федерального закона от 23.11.2009 №261 «Об энергосбережении…», согласно которому, счётчики в домах должны быть установлены до 1 января 2012 года.

Построить однородную вычислительную сеть городского масштаба в короткие сроки не представляется возможным для небольшой организации.

Проектируемая сеть будет гетерогенна: отличаются узлы сети – приборы учёта, каналы связи, способы взаимодействия.

Системы автоматического управления технологическими процессами (АСУ ТП) повышают производительность труда, увеличивают выход продукции, снижают процент брака, экономят ресурсы и позволяют на 10-15 лет продлить срок службы технологического оборудования. Диспетчерское управление и сбор данных (SCADA – Supervisory Control And Data Acquisition) являются основным и, в настоящее время, остаётся наиболее перспективным методом автоматизированного управления сложными динамическими системами (процессами) в жизненно важных и критичных, с точки зрения безопасности и надёжности, областях.

Особого внимания заслуживают процедуры обработки входных и выходных данных. В измерительном тракте (в общем случае датчик=>УСО=>контроллер) происходит преобразование реальной физической величины (температуры, давления и т.п.) в один из следующих "инженерных" видов:

- в число, соответствующее амплитуде некоторого электрического сигнала (в том числе унифицированного – 0-10V, 4-20mA и т.д.);
- в число, соответствующее проценту от диапазона изменения некоторого электрического сигнала;
- в двоичный код (после АЦП).

Для отображения поступающих данных требуется переводить "инженерные" данные в реально измеряемые (например, если требуется отображать значение температуры в её физических единицах – градусах). Управляющий сигнал во многих случаях требуется сглаживать.

Для решения подобных задач выбрана SCADA-система TRACE MODE 6. Согласно идеологии, принятой в этой системе, данные обрабатываются в каналах. Например, канал типа FLOAT снабжён встроенными алгоритмами обработки, параметры которых могут быть заданы как в редакторе, так и в реальном времени.

Канал INPUT позволяет осуществлять следующие виды операций над данными:

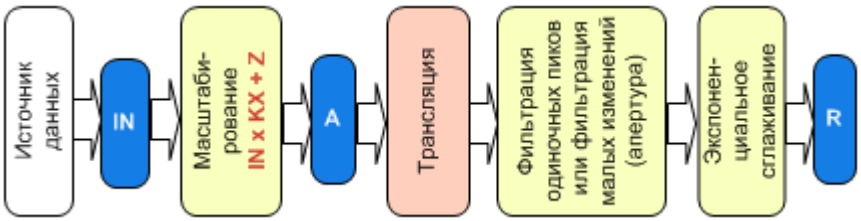
- масштабирование;
- фильтрация одиночных пиков;
- фильтрация малых изменений (апертура);
- экспоненциальное сглаживание;

Канал OUTPUT допускает:

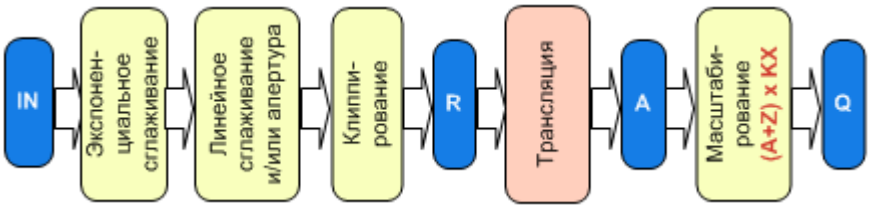
- экспоненциальное сглаживание;
- линейное сглаживание;
- фильтрация малых изменений (апертура);
- клиппирование;
- масштабирование.

Каждый канал связан с множеством атрибутов. Атрибуты **Входное значение** (2, **In**), **Аппаратное значение** (1, **A**), **Реальное значение** (0, **R**) и **Выходное значение** (9, **Q**) задействованы во внутренних алгоритмах канала FLOAT следующим образом:

канал INPUT:



канал OUTPUT:



Проектируемая система сбора данных учета тепловой и электрической энергии предоставляет доступ к данным и обеспечивает наглядность этих данных.

Список литературы

1. SCADA система TRACE MODE 6 [Электронный ресурс] // Режим доступа: http://www.adastra.ru/products/dev/scada/
2. Андреев Е.Б., Куцевич Н.А., Синенко О.В. SCADA-системы: взгляд изнутри.

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ДЛЯ ПРОВЕДЕНИЯ OFF-LINE КОНФЕРЕНЦИЙ

Стариков Е.С. – студент, Сучкова Л.И. – к.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

В настоящее время информационные технологии занимают важное место во всех сферах жизни и деятельности человека. Особое место в многообразии информационных технологий занимают распределенные системы, основное назначение которых – автоматизация деятельности, связанной с хранением, передачей и обработкой информации. Такие системы зачастую развертывают в сети Интернет, они позволяют создать единое информационное пространство с распределенными правами доступа для пользователей и администраторов.

Проблема заключается в том, что проведение научно-технической конференции является узкоспециализированной задачей, требующей индивидуального подхода к разработке программного обеспечения. Распределенная система для проведения off-line конфеенций со стороны участника должна обеспечивать механизм отправки данных, а так же сортировку, хранение, публикацию и редактирование полученной информации со стороны оргкомитета.

На сегодняшний день существуют решения, которые позволяют автоматизировать процесс проведения научно-технической конференции, однако они не подходят, так как не учитывают всех особенностей предметной области. Подобные программные продукты

выпускаются под заказ и стоят довольно дорого. Кроме того, внедрение таких продуктов так же предполагает материальные затраты на техническую поддержку и обучение персонала работе с программой.

Предполагаемое решение по созданию распределенной системы для проведения off-line конференций имеет мультиязычный, интуитивно понятный пользовательский интерфейс, и модуль администрирования, разработанный для автоматизации некоторых аспектов деятельности оргкомитета. В качестве программных средств для реализации поставленной задачи используется PHP (скриптовый язык общего назначения), в роли СУБД выступает MySQL. Этот набор позволяет создать полноценное кроссплатформенное web-приложение, в функционирующее в любой ОС. Сочетание бесплатных продуктов программного обеспечения делают его мощным и гибким.

Для реализации описанного выше способа автоматизации проведения конференции требуется спроектировать и реализовать распределенный программный комплекс, который бы позволил максимально автоматизировать процесс подготовки и проведения научно-технической конференции. В рамках решения поставленной задачи выполнено следующее:

а) спроектирована структура базы данных для хранения всей необходимой в работе оргкомитета информации;

б) разработан программный комплекс, состоящий из интерактивного WEB сайта конференции и более защищенного интерактивного WEB-сайта, который будет являться модулем для администрирования.

WEB-сайт научно-технической конференции позволяет участнику конференции осуществлять:

- регистрацию участника на сайте при внесении интересующей оргкомитет информации об участнике и организации, которую он представляет;
- идентификацию участника по электронному адресу и паролю;
- отправку доклада с указанием информации о докладе, а именно, его названия, авторов доклада, раздела конференции, к которому относится доклад;
- заказ сборников конференции, в котором необходимо указать информацию о количестве сборников, количестве страниц, посланных участником конференции, адрес, по которому отправлять сборник;
- расчет стоимости сборника после заказа его участником;
- возможность загрузки ранее введенных данных для просмотра или редактирования;
- оповещение участников о получении присланных ими оргвзносов.

Результаты работы сайта сохраняются на WEB-сервере в базе данных конференции.

Модуль администрирования реализует ведение разработанной БД оргкомитета конференции. В модуле реализованы следующие функции:

- добавление, редактирование и удаление всей имеющейся в базе данных информации;
- формирование ведомости для бухгалтерии, которая должна содержать название организаций, фамилии возможных плательщиков и сумму ожидаемого платежа;
- расчет оргвзносов;
- расчет необходимого тиража сборников;
- формирование списка авторов конференции;
- добавление новостей;
- рассылку информационных сообщений.

Данная распределенная система разрабатывалась для организации и проведения международной научно-технической конференции «Измерение, контроль, информатизация», проводимой кафедрой ВСиБ. Проведя некоторые изменения в данной модели ее можно легко адаптировать для другой конференции.

Список литературы

1. Ананьев П.И., Кайгородова М.А. Основы баз данных.: Учебное пособие / Алт. госуд. технич. ун-т им. И.И. Ползунова.- Барнаул: 2010.- 189 с. - ил.
2. Маклаков С.В. Разработка и внедрение информационных систем. [Электронный ресурс] / С.В. Маклаков, Е.Н. Павловская // Режим доступа: http://www.betec.ru/process

РАЗРАБОТКА И РЕАЛИЗАЦИЯ АВТОНОМНОЙ МИКРОКОНТРОЛЛЕРНОЙ СИСТЕМЫ КОНТРОЛЯ И ОГРАНИЧЕНИЯ ДОСТУПА

Щегольков С.В. – студент
Алтайский государственный технический университет (г. Барнаул)

В общем случае под СКУД обычно понимают совокупность программно-технических и организационно-методических средств, с помощью которых решается задача контроля и управления помещениями комплекса, а также оперативный контроль над передвижением персонала и времени его нахождения на контролируемой территории.

Эффективность использования любых технических средств зависит от применяемой технологии контроля доступа и квалификации оперативно-технического персонала. Роль человеческого фактора в конечном итоге может привести к неэффективному использованию самых передовых технических решений. Поэтому особого внимания заслуживает степень автоматизации процессов управления доступом, контроля действий персонала объекта, а так же устойчивость внутреннего алгоритма работы микроконтроллера и физическая устойчивость аппаратного комплекса.

Устройство проектировалось для помещений кафедр или компьютерных аудиторий с средне проходным потоком людей в сутки. Устройство будет состоять из двух идентификаторов: Tought Memory (ibutton) и кодовой панели (клавиатуры). Постоянным посетителям, например, лаборантам на кафедрах, заведующим и преподавателям выдается ключ-брелок Tought Memory (ibutton), который работает в течение не ограниченного времени. Касаемо кодовой панели, можно отметить, что её функционал обусловлен несколькими моментами и является неотъемлемой частью разрабатываемой СКУД: во-первых, клавиатура обеспечивает надёжность доступа, так как ключ можно потерять и процесс его восстановления более сложен, чем восстановление забытого пароля; во-вторых, именно с помощью кодовой панели будет выдаваться временный доступ в помещение, например, выдача пароля преподавателю на 90 минут для проведения семинара; в-третьих, будет осуществлён более удобный и простой процесс журналирования и диспетчеризации, ведь более просто смотреть, кто и когда взял “ключ” в оконном приложении написанным на ЯВУ чем по записям в журналах; в-четвертых, физическая надежность будет достигаться путём реализации программно-аппаратного комплекса на основе современных технологий, например, кодовая панель будет реализована на основе датчика объёмного прикосновения QT1101, т.е. будет сенсорная клавиатура, которая более надёжна от кнопочной целым рядом параметров.

Говоря о внутреннем алгоритме работы МК (микроконтроллера) необходимо отметить наиболее значимые аспекты работы: надежность, т.е. программный алгоритм должен обеспечивать целостность и надёжность системы, так же необходимо наличие обратной связи, т.е. возможность вернуться в любой другой функциональный блок (например процесс администрирования), возможность изменения и дополнения функциональных блоков.

Роль исполнительного устройства выполняет электромеханический замок. Использование именно этого устройства позволяет в случае возникновения необходимости осуществить открытие/закрытие обычным ключом.

Из всего выше сказанного следует, что данная СКУД сочетает в себе функции автономных систем, что является выгодным и наиболее предпочтительным при необходимости СКУД малых размеров, а так же сочетает в себе несколько подсистем, что является гарантом более высокой надёжности и эффективности контроля помещений.

РАЗРАБОТКА УСТРОЙСТВА РЕГИСТРАЦИИ ПЕРЕМЕЩЕНИЯ НА БАЗЕ ЛИНЕЙНОГО ПЕРЕМЕННОГО ДИФФЕРЕНЦИАЛЬНОГО ТРАНСФОРМАТОРА

Костин М.Ю. – студент
Алтайский государственный технический университет (г. Барнаул)

Зачастую на производстве возникают задачи измерения линейных перемещений виброустановок с целью изучения:

- переходных процессов;
- продолжительность выхода на режим;
- паразитных биений и колебаний;
- общих характеристик процесса работы виброустановки.

В качестве решения данной задачи предлагается создание программно-аппаратного измерительного комплекса состоящего из следующих компонентов:

- датчик
- преобразующее устройство
- прикладное ПО для ЭВМ

Для данного комплекса характерны :

1. измерение линейного перемещения в диапазоне 10 — 100 мм;
2. регистрация колебаний с частотой до 20 Гц;
3. высокая точность измерений — до 5%;
4. высокая надежность;
5. простота в эксплуатации.

В качестве датчика использован линейный переменный дифференциальный трансформатор (LVDT-датчик). К его отличительным особенностям можно причислить очень большой динамический диапазон измеряемых перемещений (от десятков микрон до ±0,5 м) и возможность работать в самых жестких условиях эксплуатации. [1]

На рисунке 1 схематично представлена конструкция LVDT-датчика, основными составляющими которого являются первичная и две вторичные обмотки (как правило, обмотки расположены на неподвижном сердечнике) и подвижное ядро. Первичная обмотка размещена симметрично между двумя идентичными вторичными обмотками. Подвижное ядро, выполненное из высокопроницаемого магнитного материала, имеет цилиндрическую форму и свободно перемещается по внутренней полости датчика.

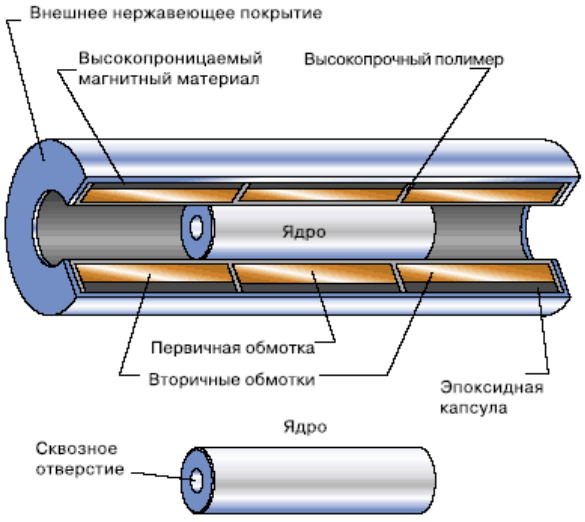


Рисунок 1 − Устройство LVDT-датчика

Электропитание первичной обмотки осуществляется переменным синусоидальным напряжением — типовое значение 3 В, 3 кГц. Выходным сигналом датчика является разность напряжений вторичных обмоток — дифференциальное напряжение.

На рисунке 2 проиллюстрирован принцип действия LVDT-датчика. Если подвижное ядро находится строго в центре (так называемая нулевая позиция), то магнитное поле, создаваемое первичной обмоткой P, симметрично, следовательно магнитные потоки через вторичные обмотки S1 и S2 равны, а значит равны и ЭДС E1 и E2, индуцируемые в этих обмотках, а значит равно нулю дифференциальное напряжение. Если же подвижное ядро смещается относительно нулевого положения, то искажается симметрия магнитного поля — через одну из вторичных обмоток, в зависимости от положения ядра, проходит больший магнитный поток, нежели чем через другую (см. рис. 2). Следовательно, различаются и ЭДС, индуцируемые во вторичных обмотках, — чем больше магнитный поток, тем больше ЭДС.

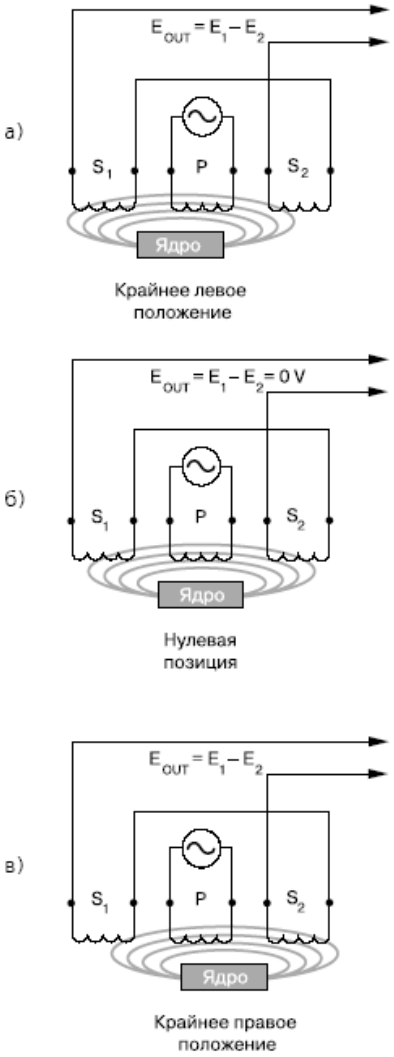


Рисунок 2 − Принцип действия LVDT-датчика

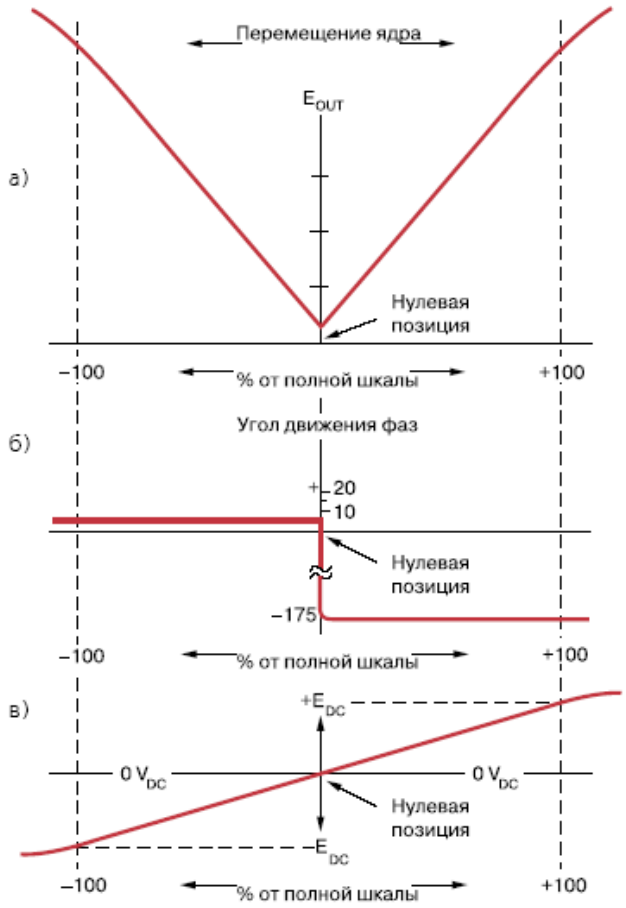


Рисунок 3 − Параметры сигнала LVDT-датчика:
а) дифференциальное напряжение
б) сдвиг фазы дифференциального напряжения относительно первичного напряжения
в) знакопеременный выходной сигнал постоянного тока

На рисунке 3а показано, как изменяется амплитуда дифференциального выходного напряжения E_{OUT} в зависимости от положения ядра внутри сердечника. Максимальное значение E_{OUT} обычно достигает нескольких вольт. Угол сдвига фаз выходного напряжения E_{OUT} относительно первичного напряжения остается постоянным вплоть до нулевой позиции, при пересечении которой сдвиг фаз изменяется на 180 градусов (см. рис. 3б). Сдвиг фазы можно использовать для определения направления движения относительно нулевой позиции при преобразовании сигнала переменного тока электронным модулем. Тогда выходной сигнал последнего будет иметь вид, как показано на рисунке 3в.

Преобразующее устройство состоит из:

– генератора синусоидального напряжения частотой 5 кГц и амплитудой 1 В для питания датчика

– преобразователя выходного сигнала

– АЦП

– контроллера интерфейса передачи данных в ЭВМ.

Первые два блока собраны на дискретных компонентах, ввиду дефицитности готовых решений и высокой цены на них. Роль третьего и четвертого блока исполняет микроконтроллер ATMega8 фирмы Atmel. Данный микроконтроллер достаточно распространен и имеет низкую стоимость, при высокой производительности и широком наборе интегрированной периферии.

В качестве интерфейса выбран последовательный интерфейс RS-232 ввиду его популярности и простоты программирования и использования. Также путем применения аппаратных преобразователей серии FTDI данный интерфейс легко преобразуется в стандартный уже для современных ЭВМ интерфейс USB.

ПО написано на объектно-ориентированном языке программирования C# и реализует достаточный и функциональный пользовательский интерфейс для проведения измерений и наблюдений.

Внешний вид интерфейса приведен на рисунке 4.

Программное обеспечение позволяет строить график перемещения, имеет возможности настройки частоты оцифровки данных, а также проведение измерений в течение заданного интервала времени. Также имеется возможность калибровки устройства.

Опытный образец данного комплекса запущен в эксплуатацию на кафедре пищевых производств для проведения лабораторных работ по изучению динамики работы камнеотбора.

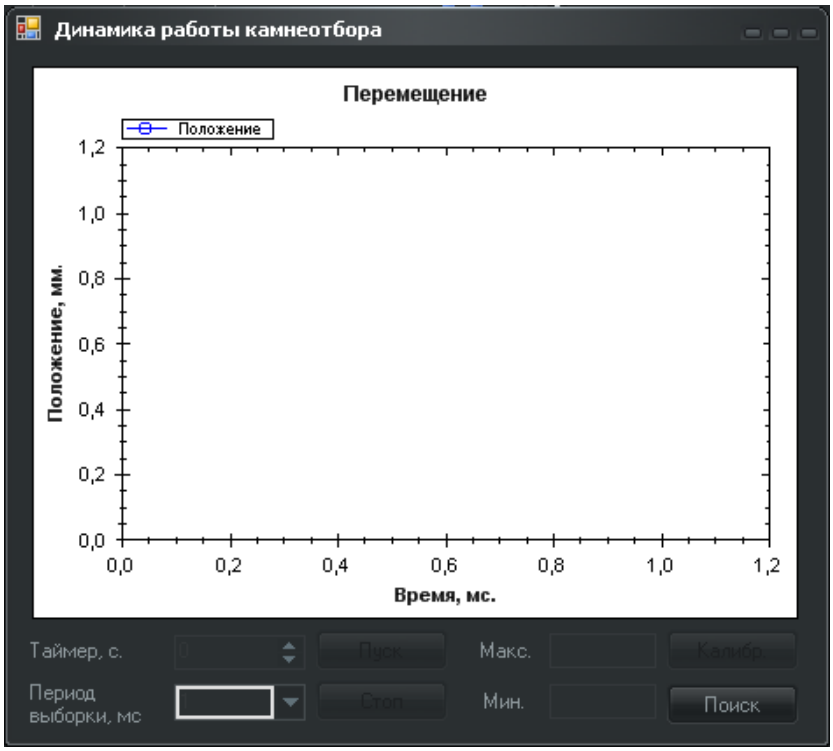


Рисунок 4 − Внешний вид интерфейса

Список литературы

1. LVDT-датчики перемещения. [Электронный ресурс] / Режим доступа: http://www.russianelectronics.ru/ leader-r/review/printing/doc/739/

РАЗРАБОТКА ПОДСИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ ПО РАДИОКАНАЛУ В СИСТЕМАХ КОНТРОЛЯ И УЧЕТА ЭНЕРГОРЕСУРСОВ

Гаврилов С.А. – студент
Алтайский государственный технический университет (г. Барнаул)

Современное производство не может обойтись без автоматизации. Применение Автоматических систем управления технологическими процессами (АСУ ТП) позволяет повысить производительность труда, увеличить выход продукции, снизить процент брака, (экономить ресурсы) уменьшить энергопотребление и на 10-15 лет продлить срок службы технологического оборудования [1]. На рисунке 1 представлена общая схема SCADA – системы контроля и управления.

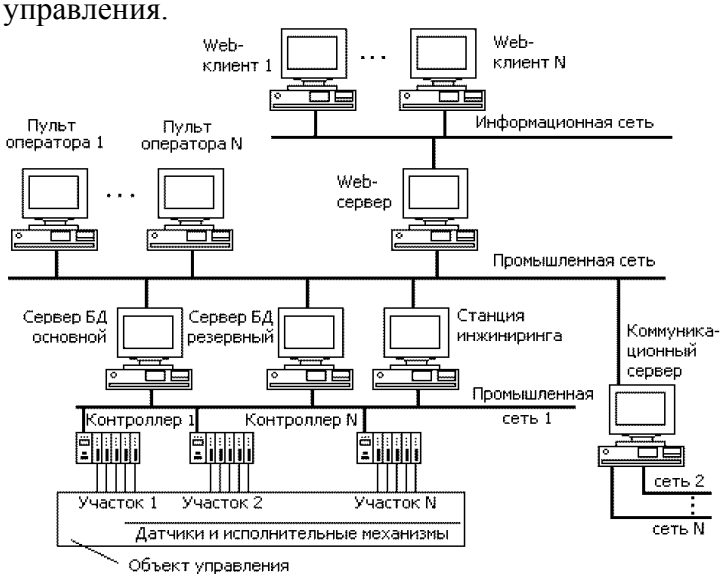


Рисунок 1 – Обобщенная схема SCADA – системы контроля и управления

Все элементы системы управления объединены между собой каналами связи. Обеспечение взаимодействия элементов SCADA - подсистем с локальными контроллерами, контроллерами верхнего уровня, офисными и промышленными сетями возложено на так называемые коммуникационные средства. Это программно – аппаратный комплекс, включающий в себя широкий спектр технологий обработки и передачи данных такие как:

- линии связи и каналы передачи данных;
- средства и методы передачи данных;
- Протоколы, интерфейсы, стеки протоколов.

Особый интерес представляют беспроводные каналы связи, так как они имеют наиболее универсальную среду передачи данных и как следствие, не требуют монтажа кабелей, а аппаратные средства могут свободно перемещается в процессе эксплуатации. Узкополосные радиомодемы малого радиуса действия предназначены для работы в не лицензируемых полосах частот, в которых не действуют нормы на частотное разделение каналов и не выделяются частоты для работы отдельных радиосетей. В соответствии с определением ГКРЧ, устройство малого радиуса действия – это «…техническое средство, предназначенное для передачи и (или) приёма радиоволн на короткие расстояния. Данные устройства используются при условии, что они не создают помех другим радиоэлектронным средствам (РЭС) и не требует защиты от помех со стороны других РЭС». Еще одним фактором является низкое энергопотребление РЭС малого радиуса действия, что снижает стоимость эксплуатации. Таким образом, радиоканалы связи на основе узкополосных радиомодемов малого радиуса действия обладают рядом преимуществ [2]:

- универсальность среды передачи данных;
- отсутствие кабелей для передачи данных;

– свободное перемещение;
– не лицензируемые частоты;
– не создают помех для других РЭС;
– малое энергопотребление;
– низкая стоимость устройств и их эксплуатация.

Существующие на рынке узкополосные радиомодемы малого радиуса действия являются универсальными средствами передачи данных, что усложняет их настройку и увеличивает цену. Еще одним минусом является сложность электрической схемы данных устройств, что снижает срок эксплуатации и усложняет ремонт. Целесообразным является разработка и внедрение узкоспециализированных систем передачи данных, что позволит снизить стоимость и упростить настройку, так же это позволит упростить электрическую схему, что увеличивает срок эксплуатации за счет снижения риска выхода из строя отдельных элементов системы.

Рассмотрим один из видов каналов передачи данных на основе узкополосного радиомодема малого радиуса действия. Структурная схема системы радиомодемов малого радиуса действия для передачи данных с приборов учета на электронно-вычислительную машину (ЭВМ) представлена на рисунке 2.

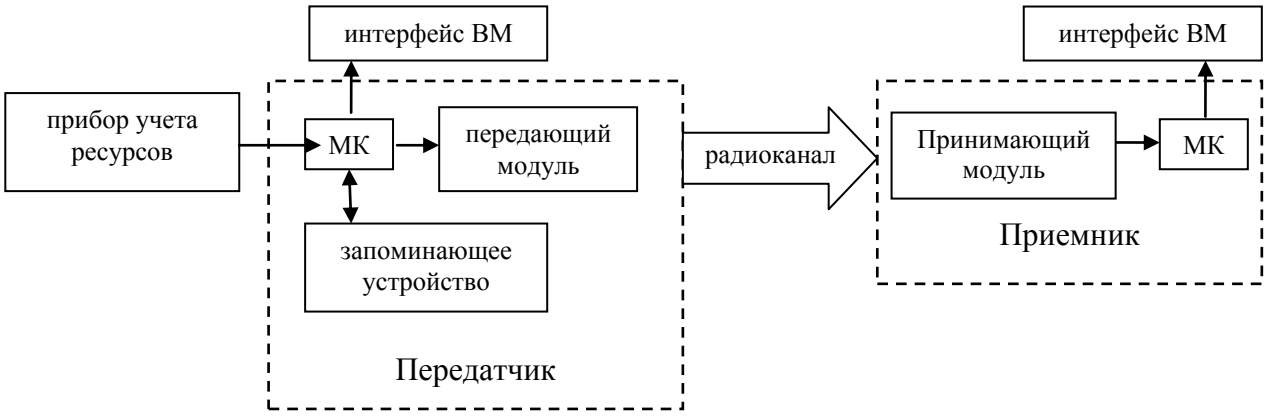


Рисунок 2 – структурная схема устройства

Данная система обеспечивает одностороннюю передачу данных по радиоканалу с прибора учета на устройство обработки и хранения данных.

Как видно на рисунке, система состоит из передатчика, приемника, управляющих контроллеров и запоминающего устройства.

Сигнал поступает с прибора учета на передатчик, где записывается до следующего сеанса передачи. Сеанс передачи данных выполняется с фиксированным интервалом времени. Вначале формируется пакет из передаваемых данных и служебной информации, обеспечивающей целостность передачи. Затем пакет подается на передающий модуль и дублируется в циклически перезаписываемое запоминающее устройство, для обеспечения учета в случае отключения приемника. Каждый пакет данных передается трижды для обеспечения целостности данных. Между сеансами связи модули переходят в режим экономии электроэнергии.

Пакет данных, полученный от передатчика, проверяется и передается на ЭВМ через её интерфейс. Целостность получаемых данных обеспечивается за счет сверки с дублирующими пакетами и контроля четности.

На передатчике также реализован интерфейс ЭВМ для снятия истории передачи из запоминающего устройства в случае сбоя приема.

Исходя из вышесказанного, можно сделать вывод, что предлагаемый канал связи обладает:

сравнительно низкой стоимостью;

– малой энергоёмкостью;
– сокращенной элементной базой;
– простотой настройки.

Что, в свою очередь, позволяет снизить стоимость всей системы автоматизации производства и учета. Так же на основе данного канал можно реализовать каналы связи для снятия показаний с различных датчиков, что расширяет круг применения данной системы.

Список литературы

1. Елизаров И.А. Технические средства автоматизации. Программно-технические комплексы и контроллеры: Учебное пособие [Текст]// И.А. . М.: Машиностроение, 2004. – 180 с.
2. ИнтернетДом – создание и проектирование систем «Умный дом» [Электронный ресурс] / Режим доступа: http://www.i-dom.ru/

СИСТЕМА ОПЕРАТИВНОГО КОНТРОЛЯ И КОММЕРЧЕСКОГО УЧЕТА ЭНЕРГОРЕСУРСОВ АЛТГТУ

Кунц Р.В, Жердев Р.Ю. – студенты
Алтайский государственный технический университет (г. Барнаул)

Информационный век немыслим без точного анализа и учёта ценностей, а ограниченность ресурсов привёла к тому, что человек просто обязан рационально относиться к имеющимся ценностям. Мы всё больше должны контролировать процессы учёта, быть ответственными и принимать решения, относящиеся к тем или иным процессам.

Проблемой является локализированный учёт материально-технических ценностей. Бухгалтерский учёт ценностей не может дать точных данных о ценностях, которые после своего поступления формально списываются и не присутствуют ни в каких документах. Руководителю для того, чтобы оценить свои ресурсы подразделения или организации на текущий момент, требуется полная и точная информация обо всех имеющихся ценностях, которые присутствуют и отсутствуют, чтобы принять верное решение о необходимости приобретения для проведения соответствующих работ.

На сегодняшний день существуют в области материально-технического и складского учёта , которые могут применяться в данном сегменте. Однако они не подходят для решения вышеупомянутых задач, так как не учитывают всех особенностей предметной области и требований для многопользовательского режима доступа к данным.

Подобные продукты на рынке выпускаются под заказ, но стоят они довольно дорого и обслуживание системы требует специализированного обучения.

Предлагаемое решение по созданию информационной системы материально-технического учёта просто в администрировании и интуитивно понятно обычному пользователю. Сочетание в ней бесплатных продуктов программного обеспечения(MySQL) и детального моделирования процессов позволило создать мощное и гибкое приложение. Данное решение поддерживает технологию клиент-сервер для удобного и распределённого доступа к базе данных материально-технического учёта.

Архитектура клиент-сервер имеет следующие достоинства:

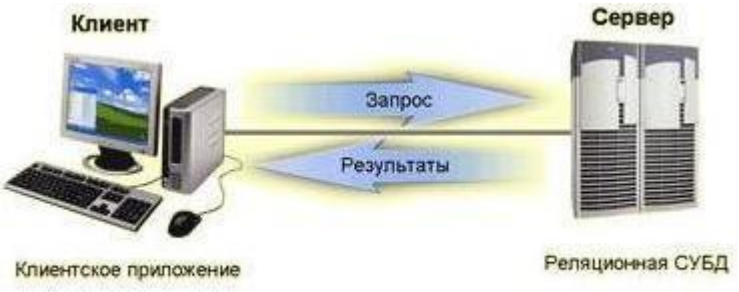


Рисунок 1. Архитектура клиент-сервер

1. Большинство вычислительных процессов происходит на сервере; таким образом, снижаются требования к вычислительным мощностям компьютера клиента;
2. Снижается сетевой трафик за счет посылки сервером клиенту только тех данных, которые он запрашивал;
3. Упрощается наращивание вычислительных мощностей в условиях развития программного обеспечения и возрастания объемов обрабатываемых данных
4. БД на сервере представляет собой, как правило, единый файл, в котором содержатся таблицы БД, ограничения целостности и другие компоненты БД. Взломать такую БД, даже при наличии умысла, тяжело;
5. Сервер реализует управление транзакциями и предотвращает попытки одновременного изменения одних и тех же данных;

На данный момент для разрабатываемой информационной системы материально-технического учёта создана концептуальная модель базы данных представленная на рисунке 2.

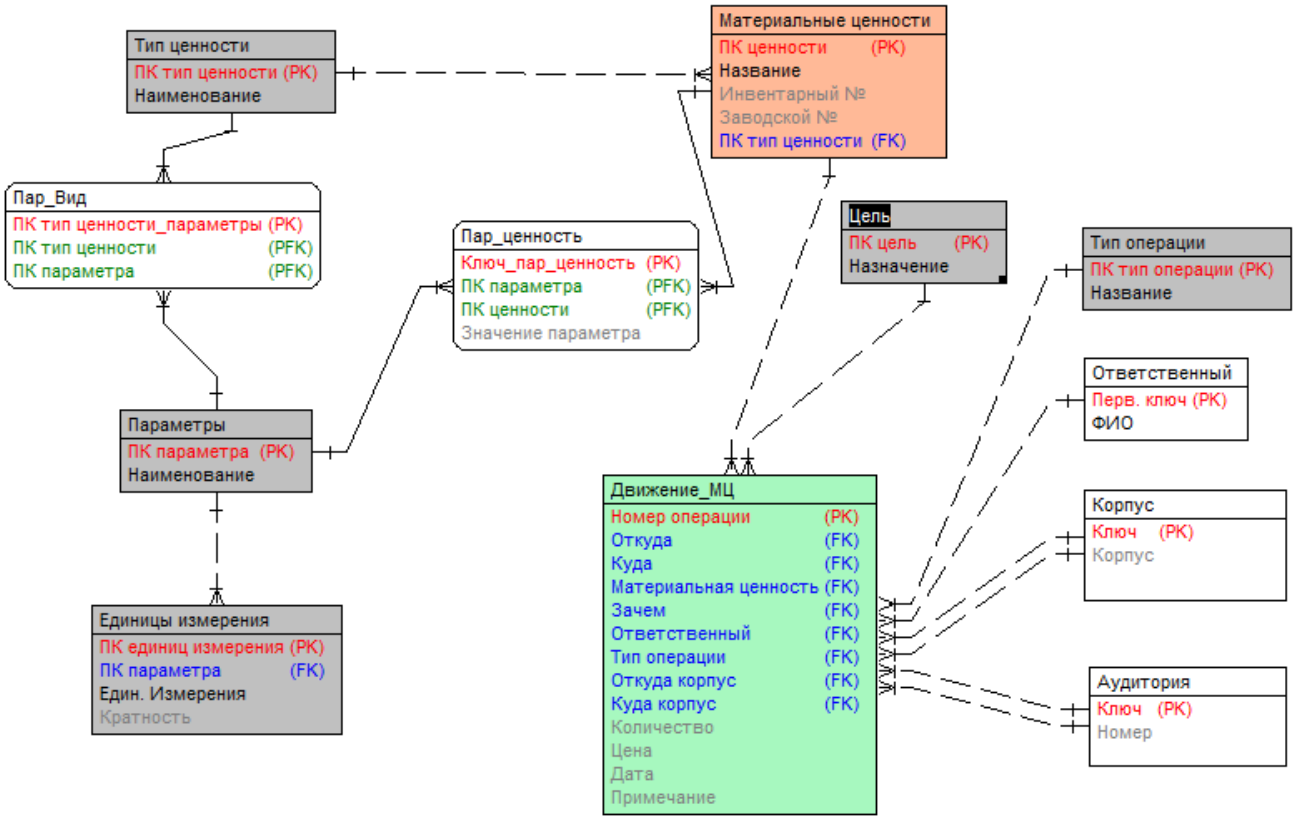


Рисунок 2 − Концептуальная модель

Каждое действие, совершенное над предметом, должно фиксироваться в информационной системе. Это способствует улучшению анализа ценностей и уменьшает вероятность того, что какие бы то ни было материальные ценности пропадут бесследно. Данная информационная система разрабатывается для организации материально-технического учёта на кафедре ВСИБ АлтГТУ.

Проведя некоторые изменения в данной модели, её можно легко адаптировать для материально-технического учёта на других предприятиях.

Список литературы

1. Маклаков С.В. Разработка и внедрение информационных систем. [Электронный ресурс] / С.В. Маклаков, Е.Н. Павловская // Режим доступа: http://www.betec.ru/process

РАЗРАБОТКА И ИНТЕРПРЕТАЦИЯ ЯЗЫКА ОПИСАНИЯ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Крысин А.В. – студент, Сучкова Л.И. – к.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Сетевой протокол – набор правил, позволяющий осуществлять соединение и обмен между двумя и более включенными в сеть устройствами. Эти правила задают единообразный способ передачи информации, регистрацию и обработку ошибок. Интернет полностью основан на протоколах.

Разработка и реализация протокола передачи данных очень трудоёмкая и долгая процедура, которая решается в несколько этапов, некоторые из которых могут многократно повторяться. На рисунке изображен примерный технологический цикл разработки протокола.

Рисунок 1 − Технологический цикл разработки протоколов

Разрабатывая новый протокол, необходимо учитывать множество факторов, например:

- надежность физической среды передачи данных
- пропускная способность сегментов и ее характер
- количество и тип узлов в сети

В такой ситуации эффективным решением будет разработка языка формального описания и интерпретатора сетевых протоколов, позволяющего оценить эффективность нового протокола еще на раннем этапе разработке (до стадии реализации) не прибегая к реальному тестированию работы протокола на физических компьютерах.

Язык, используемый в разработанной программе, является Си-подобным и описывается КС-грамматикой. Описанием протокола является совокупность описаний всех модулей и сообщений, передаваемых между ними. Каждый модуль представляет из себя расширенный конечный автомат, имеющий внутренние переменные. Взаимодействие между модулями осуществляется посредством сообщений. Модули могут, как передавать сообщения, так и реагировать на сообщения, генерируемые другими модулями. Все данные, передаются только посредством сообщений. Описание каждого модуля включает в себя перечисление множества состояний, в которых может находиться модуль. Каждое состояние может включать в себя перечень событий, на которые будет реагировать модуль, находясь в этом состоянии. По каждому событию возможны переходы в разные состояния, в зависимости от условий (которые также указываются разработчиком). Данная схема описания протокола на основе расширенного конечного автомата является достаточно формальной и позволяет очень строго его описать. С другой стороны, эта схема является простотой в реализации и интерпретации.

Программа-интерпретатор моделирует работу протокола как совокупность независимых модулей, обменивающихся сообщениями. Результатом работы программы является отчет, содержащий результаты моделирования.

Список литературы

1. Зайцев С.С. Транспортировка данных в сетях ЭВМ. – М.: Радио и связь, 1985. – 128 с.
2. Свердлов С.З. Языки программирования и методы трансляции: Учебное пособие. – СПб.: Питер, 2007. – 638 с.

АНАЛИЗ МЕТОДИК ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Плетнёв П.В. – аспирант, Белов В.М. – д.т.н., профессор
кафедра «Безопасность и управление в телекоммуникациях»
Сибирский государственный университет
телекоммуникаций и информатики (г.Новосибирск)

В нашей работе сделана попытка систематизации, анализа нескольких методов управления рисками информационной безопасности. На основе произведенного анализа, рассматриваются «плюсы и минусы» предложенных методик, в результате чего даются рекомендации для разработки нового метода анализа, управления рисками, учитывающего все сильные и слабые стороны существующих методик.

Для анализа были выбраны 100 методов, отвечающих следующему условию, – рассматривались только авторефераты , статьи, опубликованные в научных журналах или представленные на научных конференциях. Такой выбор методов заключается в доступности материалов, возможности их исследования и использования. В отличие от методов, применяемых в организациях, научные материалы содержат последние результаты в

исследованиях по рассматриваемой проблеме, авторы не боятся экспериментировать, предлагать новые идеи в своих методиках.

Хотя из рассмотренных статей можно выделить ряд новых, интересных для реализации идей, чаще всего введение сложных математических теорий ухудшает прозрачность итоговой оценки для эксперта, требует от него достаточной математической подготовки. Поэтому при проведении анализа рассмотренных статей, часто для таких методов заносились пометки об отрицательной стороне подхода.

Не редко информационные активы систем, являющиеся критичными объектами для работы всей организации, требуют повышенного внимания и исключительного, индивидуального подхода к обеспечению информационной безопасности. Однако для остальных случаев возможно использовать наработки, опыт в обеспечении безопасности, описанные в стандартах, федеральных нормативных документах, рекомендациях. Хотя и не стоит слепо доверять безопасность системы всем перечисленным документам, такой подход экономит время, работу специалистов по защите информации.

Перечисленные очевидные плюсы использования стандартов безопасности, не отражены в большинстве проанализированных методиках. Как будет показано ниже, лишь небольшое количество подходов основано или хотя бы использует некоторые рекомендации стандартов.

Использование методов анализа рисков, описанных в анализируемых документах хотя и возможно, тем более что многие организации до сих пор не доверяют анализу, управлению рисками, а придерживаются старых методов точечного управления уязвимостями, однако такой подход затрудняет возможную сертификацию организации, требует от специалистов по безопасности освоения, повышения опыта в новых для них системах анализа рисков. Кроме того, работа с такими методиками затрудняет использование обязательных в настоящий момент рекомендаций, нормативных документов ФСТЭК, ФСБ.

Отсюда использовать рассматриваемые методики лучше не полностью, а выбирать некоторые рекомендации, подходы, которые не нарушат полностью работу по анализу рисков, однако могут повысить точность итоговых результатов, сократить время работы экспертов.

Процесс анализа рисков является составной частью общей системы управления организацией, поэтому для более качественной работы с рисками информационной системы, используется общая процессная модель. Модель отражает работу стандартного цикла управления Деминга, определяет: Планирование – Выполнение – Проверку – Корректировку. В стандартах ISO и BS содержится проекция данного процесса на работу по анализу и управлению рисками. [1]

В большинстве рассмотренных нами методик, осуществляется работа чаще всего только по пункту оценки рисков, то есть непосредственно раздел «выполнения». Таким образом, подсчет рисков, выполненная на его основе закупка новых средств и разработка методов по повышению безопасности, не намного отличается по качеству от рассмотренного ранее «заплаточного» метода. [2] Только полностью осуществленный цикл управления, последующее его циклическое повторение с корректировкой, пересмотром рисков позволит осуществить задумку обеспечения безопасности на основе анализа рисков.

Нельзя не заметить отсутствие в большинстве рассмотренных подходов экономической составляющей анализа. В результате некоторых таких методов получается, что управление рисками – это только закупка средств защиты, без учета возможностей рассматриваемой организации.

Хотя существует ряд отрицательных, с нашей точки зрения, моментов работы с предложенными подходами, в ходе их анализа были выделены и некоторые положительные стороны.

В первую очередь заметим, что в некоторых из рассмотренных статей, оценка риска базируется на определении вероятности при помощи статистических данных. Хотя при таком подходе можно выявить ряд минусов, однако в целом, данные методики могут успешно применяться для работы. Использование базы статистики позволяет свести к

минимуму субъективную точку зрения эксперта на решаемую задачу, позволяет производить работу по оценке специалистам, не имеющим большого опыта, квалификации.

В ряде работ осуществлены подходы на основе использования графов, нечеткой логики. Применение таких методов позволяет более наглядно представить причинно-следственные связи между объектами, потоками информационной системы, что в свою очередь способствует наиболее точному анализу системы на этапе ее проектирования. Кроме того, анализ рисков осуществляется боле формализовано, поддается более простой программной реализации.

Использование во многих работах нечетких множеств также позволяет повысить точность результата, облегчить работу эксперта по определению оценок. [3]

Для более простого анализа рассматриваемых методик в целом, в конце нашей работы представлена сводная таблица, осуществляющая сравнение характеристик подходов.

Сравнение методов производилось по следующим параметрам: субъективные оценки сложности вычисления и сложности программной реализации, метод получения данных о параметрах угроз – способ ввода входных данных в систему анализа, вид итогового результата анализа – вид выходных данных, т.е. результат после обработки данных в системе, использование стандартов информационной безопасности – использование в методе требований стандартов.

Оценка сложности вычисления представляет собой субъективную характеристику сложности использования рассматриваемых методик, может принимать значения: «Высокая», «Средняя», «Низкая» сложность. На результат «высокой» оценки наибольшее влияние оказывало использование специальных математических теорий, тогда как решения на основе таблиц, экспертных оценок, характеризовались низкой сложностью вычисления.

Сложность программной реализации также оценивалась на основе субъективного мнения. Хотя для выполнения программной реализации метода – экспертной системы, использование некоторых математических теорий не затруднительно, включение некоторых рядов, интегралов, может несколько затруднить реализацию. Использование математической логики, графов наоборот, по нашему мнению, облегчает задачу программиста.

Входные данные в систему анализа рисками могут поступать несколькими способами. Основные из них: статистические данные, экспертные оценки. Оба метода имеют свои плюсы и минусы, могут предназначаться для работы в различных ситуациях.

На рисунке 1 представлена статистика по использованию того или иного типа ввода данных в рассматриваемых методиках.

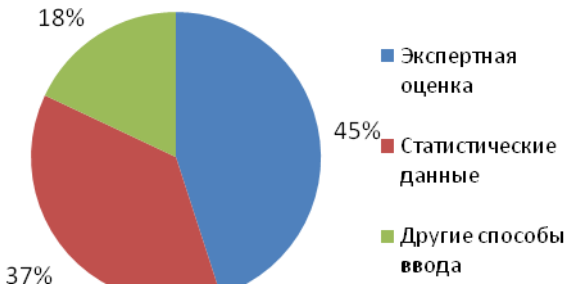


Рисунок 2 – Соотношение типов входных данных рассматриваемых методов

Аналогично входным данным, анализировались типы итоговых результатов. Чаще всего выходные данные представляются в виде количественной или качественной оценки. Хотя количественная оценка представляет собой конкретную оценку, вероятность риска, качественная характеристика более наглядна, представляет возможность более простого ранжирования рисков.

Статистика типов выходных данных анализируемых подходов представлена на рисунке 2

Рисунок 3 – Соотношение типов выходных данных рассматриваемых методов

Как видно из соотношения, количественная оценка преобладает в подходах, представленных в научных статьях, хотя большинство стандартов безопасности используют качественную шкалу оценки.

Последней исследуемой характеристикой сравнения методов является использование стандартов безопасности, нормативных документов. Плюсы и минусы были приведены выше, на рисунке 3 представлена статистика их использования.

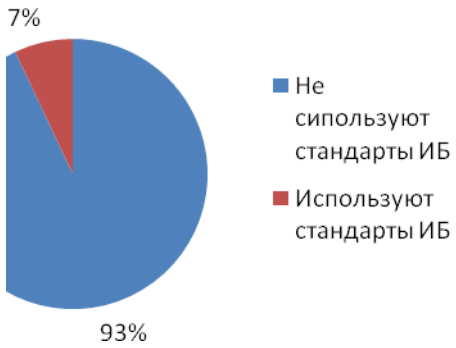


Рисунок 4 – Соотношение использования стандартов ИБ и нормативных документов в рассматриваемых методах

По результатам работы сделаны следующие выводы: большинство подходов не учитывают концепции, требования различных стандартов информационной безопасности, это может вызвать недоверие к применяемым методикам у экспертов, проводящих анализ рисков, затрудняет возможную сертификацию организации. Многие подходы, в основе которых лежит цель получить количественную оценку рисков с использованием математических формул, моделей, углубляясь в математические теории, теряют связь с практической оценкой рисков, реальными бизнес требованиями. Многие методики не обеспечивают полного процесса по оценке, управлению рисками, реализуя лишь некоторые его компоненты.

Анализ показывает, что большинство рассматриваемых методов имеют также и положительные стороны, многие подходы содержат свежие идеи, концепции по проведению оценки рисков. Учитывая все сильные и слабые стороны рассматриваемых методик можно попытаться спроектировать, реализовать новый, более совершенный подход по оценке рисков информационной безопасности.

Список литературы

1. Sanjay Goel, Vicki Chen. Анализ рисков информационной безопасности – матричный подход [Электронный ресурс] / University at Albany. – Электрон. дан. – University at Albany, 2009. – Режим доступа: http://www.docstoc.com/
2. Тенетко М.И. Концепция оценивания информационных рисков на основе нечетких множеств [Текст] / М.И. Тенетко, О.Ю. Пескова // Известия Южного федерального университета. Технические науки. – 2008. – Т. 85. – №8. – С. 24-30.
3. Кащенко А.Г. Нечеткие модели на основе проекции нечетких множеств в задачах оценки и управления рисками информационной безопасности [Текст] / А.Г. Кащенко, В.Г. Чернов, А.Н. Сонцев // Информация и безопасность. – 2006. – Т. 9. – №2. – С. 113-121.