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

НАУКА И МОЛОДЕЖЬ – 2010

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

СЕКЦИЯ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

подсекция

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Барнаул – 2010

УДК 004

VII Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь – 2010". Секция «Информационные технологии». Подсекция «Вычислительные системы и информационная безопасность». / Алт. гос. техн. ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2010. – 75 с.

В сборнике представлены работы научно-технической конференции студентов, аспирантов и молодых ученых, проходившей в 21 апреля 2010 г.

Научный руководитель подсекции: д.т.н., профессор, Якунин А.Г.
Секретарь подсекции: к.в.н., профессор, Загинайлов Ю.Н.

Компьютерная верстка: Сорокин А.В.

СОДЕРЖАНИЕ

РАЗРАБОТКА МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПОСТРОЕНИЯ БЕЗОПАСНЫХ СЕТЕЙ ПРЕДПРИЯТИЯ

Ананьев И. А. – студент, Шарлаев Е. В. – к.т.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Сегодня многие предприятия объединяют свои вычислительные ресурсы в информационные сети для обработки коммерчески значимой информации. Из этого можно сделать вывод, что на предприятиях существует необходимость разработки безопасных сетей, в которых циркулируют потоки информация. Есть два варианта: обратиться за помощью в специализированные центры для построения безопасной сети, либо построить сеть самостоятельно, используя методику построения безопасной сети предприятия. На данный момент не существует четкого методологически проработанных принципов построения безопасных сетей. Разработкой подобных методик занимаются лишь специализированные центры, учитывая специфику конкретного предприятия. В большинстве учебных центров не разрабатывались методические рекомендации подобного рода[1].

Эта проблема характерна для специалистов по защите информации проектирующих комплексную систему защиты информации в организации.

Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами. Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в Internet-сообществе это средство действительно работает, и весьма эффективно[2].

Отмеченная роль стандартов зафиксирована в основных понятиях закона РФ "О техническом регулировании" от 27 декабря 2002 года под номером 184-ФЗ (принят Государственной Думой 15 декабря 2002 года):

- стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;
- стандартизация - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Также в число принципов стандартизации, провозглашенных в статье 12 упомянутого закона, входит принцип применения международного стандарта как основы разработки национального, за исключением случаев, если "такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация, в соответствии с установленными процедурами, выступала против принятия международного стандарта или отдельного его положения". С практической точки зрения, количество стандартов и спецификаций (международных, национальных, отраслевых и т.п.) в области информационной безопасности бесконечно.

Основные международные стандарты информационной безопасности[3]:

1) ISO 17799 – построение системы информационной безопасности, менеджмент в области технологий защиты информации.

2) ISO 15408 - Единые критерии информационной безопасности. Основные направления – средства защиты: разработка, эксплуатация; профиль защиты: набор защитных средств и систем; стандарт защиты: детальные требования к программно-техническим средствам обеспечения информационной безопасности.

3) BS 7799 - построение систем аудита информационной безопасности, описание типовых угроз и контрмер, характеристики принятых программных средств аудита информационной безопасности.

4) TCSec – определяет требования, предъявляемые к аппаратному, программному и специальному обеспечению компьютерных систем, выработке соответствующих методик и технологий анализа степени поддержки политики безопасности. Три вида требований: к политике безопасности, к аудиту систем, к корректности работы систем. Принят в США.

5) BSI/IT Baseline – руководство по обеспечению информационной безопасности базового уровня. Принят в ФРГ.

При этом все эти международные стандарты и наши российские имеют некоторые противоречия, которые могут привести в замешательство специалистов по защите информации при построении безопасной сети предприятия.

Следовательно, возникает потребность в разработке методических рекомендаций, предназначенных для специалистов по защите информации на предприятии, по организации построения безопасной сети в которой циркулируют потоки коммерческой информации.

На рисунке 1 представлен проект методических рекомендаций, составленных на основе международных стандартов и нормативно-правовой базы РФ регламентирующих организацию построения сетей.

В методических рекомендациях рассмотрены шаги (рис.1) организации построения безопасной сети с учетом анализа всех факторов, влияющих на безопасность информационных потоков предприятия, циркулирующих в вычислительной сети.

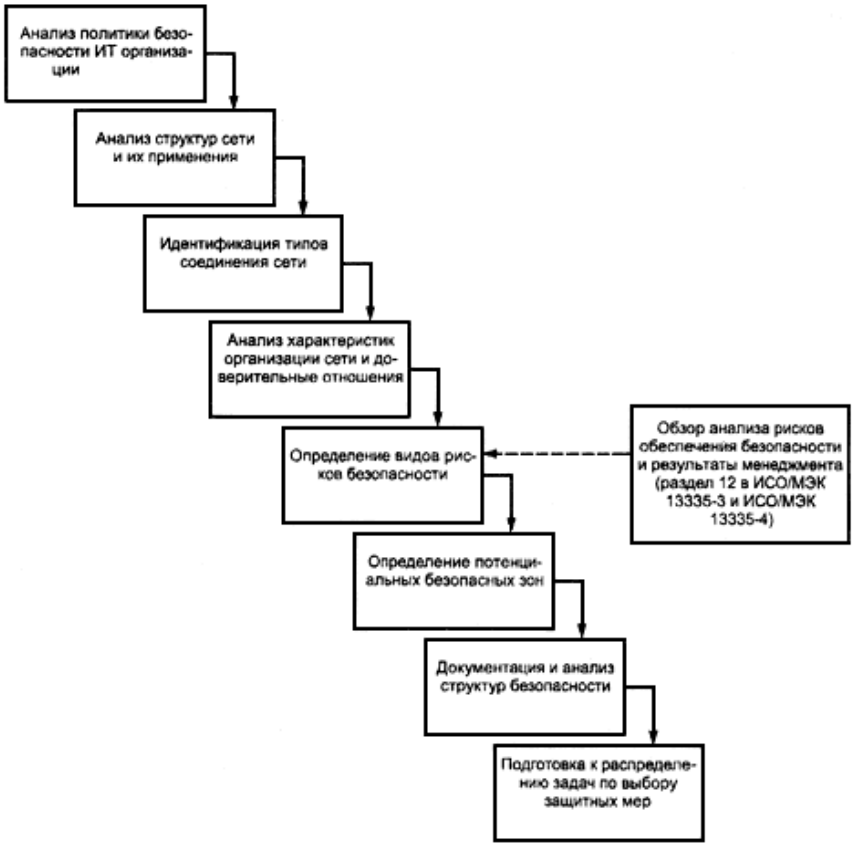

Рисунок 1 – Шаги построения вычислительной сети

Данный программный продукт позволяет существенно сэкономить время специалиста по

защите информации на организацию построения безопасной сети на предприятии.

Список литературы

1. Машкина А.А., Рахимов Е.А., Васильев В.И. Методика построения модели комплексной оценки угроз информации, циркулирующей на объекте информатизации [электронный ресурс]. - http://www.contrterror.tsure.ru/site/magazine7/07-27-Mashkina-Rahimov-Vasilyev.htm
2. Руководящий документ от 14 фев. 2008г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [электронный ресурс]. - http://www.fstec.ru/_razd/_isp0o.htm
3. Алгоритм модели анализа угроз и уязвимостей [электронный ресурс].- http://www.dsec.ru/download/threats_vuln.pdf

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО ОЦЕНКЕ КАЧЕСТВА ПЕДАГОГИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бондаренко А.Ю. – студент, Архипова А.Б. – аспирант,
Белов В.М. – к.ф.-м.н., д.т.н., профессор

Алтайский государственный технический университет (г. Барнаул)

Понятие “качество образования” сформировалось и получило международное гражданство в 1998 г. на состоявшейся в Париже Всемирной конференции по высшему образованию, которая констатировала, что повышение качественного уровня становится одной из главных задач высших учебных заведений на длительную перспективу [1].

Действительно, на сегодняшний день понятия “качество жизни”, “качество человека”, “качество образования” тесно переплетаются между собой. Данная связь выстраивается так: “качество образования – качество человека – качество жизни”. На первый взгляд выражение “как учим, так и живем” кажется несколько поверхностным, но, в сущности, это правильное и глубокое суждение [2]. Еще Р. Киплинг справедливо отмечал, что “образование – важнейшее из земных благ, если оно наивысшего качества”.

На современном этапе содержание понятия “качество образования” рассматривается как интегральная характеристика системы образования, результирующей которой является качество контингента абитуриентов, а затем студентов; качество преподавательского состава; качество содержания образования; качество условий организации обучения; качество педагогических технологий; качество образовательного процесса; качество его ресурсного обеспечения; качество участия специалиста в производстве товаров и услуг по окончании вуза; качество его социокультурной деятельности в обществе; наконец, качество жизни самого специалиста, возможностей его самореализации [3]. Это комплексный показатель, синтезирующий все этапы обучения, развития и становления личности, условий и результатов образовательного процесса. Центральной тенденцией достижения качества образования служит ориентация на запросы обучающихся и создание оптимальных условий для их личностного развития. Т.е. качество образования – это критерий эффективности деятельности образовательного учреждения, основной продукцией которого являются качественно подготовленные выпускники.

Следует отметить, что ключевой фигурой в образовательном процессе является преподаватель. Поэтому понятие качество образования неразрывно связано с понятием качество педагогической деятельности.

Более того, на сегодняшний день одной из важных задач управления качеством профессионального образования становится разработка системы оценки качества педагогической деятельности, позволяющей не только оперативно диагностировать качество такой работы, но и управлять им.

В настоящее время разработано программное обеспечение для оценки качества работы преподавателей по информационной безопасности, использующая в своей основе нечеткую логику. При разработке данной системы были поставлены следующие задачи:

1.Усилить заинтересованность преподавателей в повышении своей профессиональной квалификации, в освоении передового педагогического опыта, в творческом подходе к преподаванию;

2.Обеспечить большую объективность оценок деятельности преподавателя за счет повышения полноты достоверности информации;

3.Усилить коллективную заинтересованность преподавателей в улучшении конечных результатов по подготовке специалистов;

4.Повысить качество преподавания как важнейший фактор улучшения качества подготовки специалистов, а именно:

- повысить мотивацию к учебно-познавательной и научной деятельности;
- повысить общественную активность преподавателей.

Отметим, что в качестве модели оценки существует ряд вариантов математического описания как модели педагогической деятельности, так и оценок качества педагогической деятельности. Среди таких моделей и методов предпочтение было отдано подходу, использующего в своей основе нечеткую логику.

С данных позиций оценка качества педагогической деятельности проходит в несколько этапов.

Начальным этапом оценки является выбор экспертов в области информационной безопасности, т.е. выбор из некоторого множества специалистов (кандидатов в эксперты) лиц, наиболее компетентных в области информационной безопасности, и составления из них экспертных групп. В качестве методики выбора эксперта использован энтропийный подход.

Второй этап заключается в тестировании экспертов. Оценка преподавателя складывается из результатов работы по каждому виду деятельности с учетом весовых коэффициентов. Схематически это выглядит следующим образом:

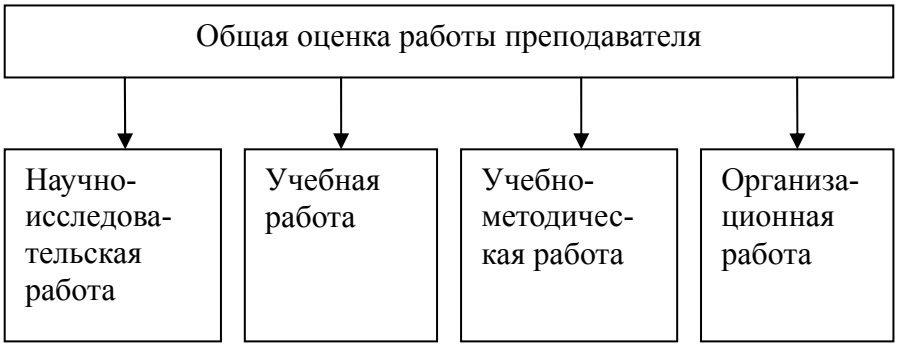

Рисунок 1 – Общая оценка работы преподавателя

Оценка результатов по каждому виду деятельности является частью общей оценки работы преподавателя. Критерии оценки деятельности преподавателей были выбраны таким образом, чтобы максимально учитывать его вклад в показатели кафедры в целом. Каждый вид деятельности имеет свои особенности и специфику, поэтому предполагает свои критерии оценки результативности.

Такая система оценки работы преподавателей, во-первых, охватывает все виды деятельности, во-вторых, позволяет сопоставлять результаты работы преподавателей разных

кафедр, в-третьих, исключается субъективный подход к оценке.

Список литературы

1. Болотов В.А. Система оценки качества образования: Учебное пособие / В. А. Болотов, Н. Ф. Ефремова. – М.: Университетская книга; Логос, 2007. – 192 с.
2. Панасюк В.П. Школа и качество: выбор будущего / В. П. Панасюк. – Спб.: КАРО, 2003. – 384 с.
3. Шиян Л.К. Аналитический обзор системы измерений качества профессиональной деятельности современного педагога: Мониторинговые исследования. – М., 2006. – 116 с.

ОБОБЩЕННЫЙ МЕТОД ЦЕНТРА НЕОПРЕДЕЛЕННОСТИ ДЛЯ ОЦЕНКИ ПАРАМЕТРОВ ФУНКЦИЙ РАСПРЕДЕЛЕНИЯ ЛАПЛАСА И РЭЛЕЯ

Быков Р.В. – студент, Архипова А.Б. – аспирант, Белов В.М. – к.ф.-м.н., д.т.н, профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Измерение величины это операция, в результате которой мы узнаем, во сколько раз измеряемая величина больше или меньше соответствующей величины принятой за эталон. Общая черта измерений – невозможность получения истинного значения измеряемой величины, т.к. результат измерения всегда содержит какую-то ошибку. Объяснить это можно как ограниченной точностью измерения, так и природой самих измеряемых объектов.

Обработка результатов измерений невозможна без использования математических методов, которые позволяют выбрать оптимальное направление исследований. Для случаев, когда входные и выходные переменные задаются интервалами, используется интервальный анализ [1].

Интервалом называют замкнутый отрезок вещественной оси, а интервальная неопределенность – это состояние неполного (частичного) знания об интересующей величине, когда известна лишь ей принадлежность некоторому интервалу, т.е. когда указываются лишь границы возможных значений этой величины (либо пределы её измерения). Соответственно, интервальный анализ – это отрасль математического знания, исследующая задачи с интервальными неопределенностями и методы их решения [2].

Интервальный анализ и его методы имеют наивысшую ценность в задачах, где неопределенность и неоднозначность возникают с самого начала и являются неотъемлемой частью постановки задачи.

Постановка задач оценивания параметров функции распределения

Пусть получены экспериментальные данные, содержащие интервальные значения переменных $[x_i^-; x_i^+], [y_i^-; y_i^+]$ для $i \in \overline{1,n}$ и известно, что истинные значения переменных лежат внутри соответствующих интервалов. Таким образом, каждому измеренному интервальному значению $[y]_i$ соответствует интервальное значение входной величины $[x]_i$. Известно, что ошибки измерения как входной, так и выходной переменных не превышают известных величин:

$$|\Delta x| \le \varepsilon_1, \ |\Delta y| \le \varepsilon_2,$$

где Δx - ошибка измерений x_i, Δy – ошибка измерений y_i, ε_1 и ε_2 - верхние границы оценок Δx и Δy соответственно. Наша задача – определить точечные и интервальные значения параметров функции при наличии информации об x_i, y_i, Δx и Δy [3].

Распределение Лапласа

Распределение Лапласа – распределение вероятностей случайной величины *X*, заданное плотностью:

$$p(x;\lambda,\mu)=\frac{\alpha}{2}\ e^{-\alpha|x-\beta|},$$

где $\alpha > 0$ - параметр масштаба и $-\infty < \beta < +\infty$ – параметр сдвига.

Функция распределения имеет вид:

$$F(x)=\int_{-\infty}^{x} f(t)dt=\frac{\alpha}{2}\int_{-\infty}^{x} e^{-\alpha|t-\beta|}dt.$$

Для интегрирования необходимо рассмотреть два случая: $x\le\beta$ и $x>\beta$:

$$F(x)=\begin{cases}\frac{1}{2}e^{\alpha(x-\beta)}, & x\le\beta;\\ 1-\frac{1}{2}e^{-\alpha(x-\beta)}, & x>\beta.\end{cases}$$

1. Рассмотрим случай $x\le\beta$. Для решения задачи оценивания найдем параметры $[\alpha]$ и $[\beta]$ следующей функции распределения:

$$[y]=\frac{1}{2}e^{[\alpha]([x]-[\beta])}.$$

После преобразований функция имеет вид:

$$[\alpha][x]-[\alpha][\beta]=\ln(2[y]).$$

Пусть даны два интервала входных и выходных данных $[x_1]$, $[x_2]$ и $[y_1]$, $[y_2]$ соответственно. Тогда после преобразования исходной функции распределения запишем систему уравнений:

$$\begin{cases}[\alpha][x_1]-[\alpha][\beta]=\ln(2[y_1]),\\ [\alpha][x_2]-[\alpha][\beta]=\ln(2[y_2]).\end{cases}$$

Решение данной системы для задачи оценивания параметров имеет вид:

$$[\alpha]=\frac{\ln(2[y_1])}{[x_1]-[\beta]},\ [\beta]=\frac{\ln(2[y_2])[x_1]-\ln(2[y_1])[x_2]}{\ln(2[y_2])-\ln(2[y_1])}.$$

2. Рассмотрим случай $x>\beta$. Для решения задачи оценивания найдем параметры $[\alpha]$ и $[\beta]$ следующей функции распределения:

$$[y]=1-\frac{1}{2}e^{-[\alpha]([x]-[\beta])}$$

После преобразований функция имеет вид:

$$-[\alpha][x]+[\alpha][\beta]=\ln(2(1-[y])).$$

Пусть даны два интервала входных и выходных данных $[x_1]$,$[x_2]$ и $[y_1]$, $[y_2]$ соответственно. Тогда после преобразования исходной функции распределения запишем систему уравнений:

$$\begin{cases}[\alpha][\beta]-[\alpha][x_1]=\ln(2[1-y_1]),\\ [\alpha][\beta]-[\alpha][x_2]=\ln(2[1-y_2]).\end{cases}$$

Решение данной системы для задачи оценивания параметров имеет вид:

$$[\alpha]=\frac{\ln(2(1-[y_1]))}{[\beta]-[x_1]},\ [\beta]=\frac{\ln(2(1-[y_1]))[x_2]-\ln(2(1-[y_2]))[x_1]}{\ln(2(1-[y_1]))-\ln(2(1-[y_2]))}.$$

Для определения точечных оценок параметров α, β от истинных значений во всех рассмотренных случаях воспользуемся приближенными формулами:

$$\hat{\alpha}=0.5(\alpha^{+}+\alpha^{-}),\ \hat{\beta}=0.5(\beta^{+}+\beta^{-}).$$

Абсолютные и относительные отклонения оценок параметров α, β от истинных значений определяем из соотношений:

$$\varepsilon_\alpha = 0.5(\alpha^+ - \alpha^-),\ \varepsilon_\beta = 0.5(\beta^+ - \beta^-).$$

$$\varepsilon_\alpha^{om} = (100 \cdot \varepsilon_\alpha)/(\min(|\alpha^-|,|\alpha^+|),\ \varepsilon_\beta^{om} = (100 \cdot \varepsilon_\beta)/(\min(|\beta^-|,|\beta^+|).$$

Рекуррентные формулы позволяющие уточнить вид зависимостей при поступлении новой информации о входных и выходных параметрах функции распределения в случае, когда $x \leq \beta$ имеют вид:

$$[\alpha_{i+1}] = \frac{\ln(2[y_n])}{[x_n] - [\beta_i]},\ [\beta_{i+1}] = [x_n] - \frac{\ln(2[y_2])}{[\alpha_{i+1}]};$$

в случае, когда $x \leq \beta$ имеют вид:

$$[\alpha_{i+1}] = \frac{\ln(2(1-[y_n]))}{[\beta_i] - [x_n]},\ [\beta_{i+1}] = [x_n] + \frac{\ln(2(1-[y_2]))}{[\alpha_{i+1}]}.$$

Распределение Рэлея

Распределение Рэлея – распределение вероятностей случайной величины X, заданное плотностью:

$$\mathrm{p(x;\delta)} = \frac{\mathrm{x}^2}{\delta^2} 1 - \exp(\frac{-\mathrm{x}^2}{2\delta^2}),$$

где $x \geq 0,\ \delta > 0$ - параметр масштаба.

Функция распределения имеет вид:

$$\mathrm{F\ (x)} = 1 - \exp(\frac{-\mathrm{x}^2}{2\delta^2}).$$

Для решения задачи оценивания параметров функции распределения:

$$[\mathrm{y}] = 1 - \exp(\frac{-[\mathrm{x}]^2}{2[\delta]^2}),$$

найдем параметры $[\delta]$.

После преобразований функция имеет вид:

$$[\delta]^2 = \frac{-[\mathrm{x}]^2}{2\ln(1-[y])}.$$

Введем обозначение:

$$[a] = \frac{-[\mathrm{x}]^2}{2\ln(1-[y])}.$$

Тогда уравнение примет вид:

$$[\delta]^2 = [a].$$

Для нахождения приемлемого интервального приближения в данном случае используют метод фиксированного аргумента [4], идея которого состоит в следующем. Центр искомого прямоугольника $[\delta]$ помещают в точку, найденную по средним интервальным значениям коэффициентов уравнения – $[\delta_{ср}]$. По теореме Виета корни уравнения связанны соотношениями, которые должны выполняться при любых значениях коэффициентов. Это позволяет записать интервальную систему двух уравнений:

$$\delta_1 + \delta_2 = [0;0], \delta_1 \cdot \delta_2 = -[a].$$

Подставляя в эту систему среднее значение корня $\delta_{ср} = \sqrt{a_{ср}}$, получаем два интервальных уравнения относительна корня $\delta_1 : \delta_{ср} + [\delta_2] = 0$ и $\delta_{ср} \cdot [\delta_2] = -[a]$, которое легко решается относительно неизвестного интервала $[\delta_2]$. Проделав аналогичные действия для фиксированного корня $\delta_{ср} = -\sqrt{a_{ср}}$ получаем два интервальных уравнения относительно корня $\delta_2 : [\delta_1] + \delta_{ср} = 0$ и $\delta_{ср} \cdot [\delta_1] = -[a]$. В качестве решения системы берется наиболее

«узкое» решение, которое удовлетворяет условиям $[a]>0$ и $\delta>0$.

Таким образом, получили решение задачи оценивания параметров функций распределения Рэлея и Лапласа обобщенным методом центра неопределенности, который учитывает все неопределенности и неоднозначности возникающие в ходе измерения величин.

Список литературы

1. Белов В.М. Оценивание параметров эмпирических зависимостей методом центра неопределенности / В. М. Белов, Ф. Г. Унгер, Ю. А. Карбаинов, В. И. Порлубников, Н. П. Тубалов. – Новосибирск: Наука, 2001. – 176 с.
2. Шарый С.П. Конечномерный интервальный анализ / С. П. Шарый. – 2003
3. Гончаров С.А. Оценивание параметров линейных экспериментальных зависимостей обобщенным методом центра неопределенности / С. А. Гончаров, В. М. Белов, Е. В. Рябова, В. Т. Гетманов. – Рубцовск: РИО, 2005. – 130 с.
4. Вощинин А.П. Метод анализа данных с интервальными ошибками в задачах проверки гипотез и оценивания параметров неявных линейно параметризованных функций, Заводская лаборатория, том 66, №3, 2000.

НЕЧЕТКИЕ МОДЕЛИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Быков Р.В. – студент, Архипова А.Б. – аспирант, Белов В.М. – к.ф.-м.н., д.т.н, профессор

Алтайский государственный технический университет (г. Барнаул)

Одним из наиболее ценных товаров на сегодняшний день является информация. В условиях жесткой конкурентной борьбы современные компании вынуждены уделять повышенное внимание её сохранности. В связи с этим, трудно переоценить значимость специалистов по информационной безопасности. Они принимают участие во всех этапах процессов системы информационной безопасности (рисунок 1).

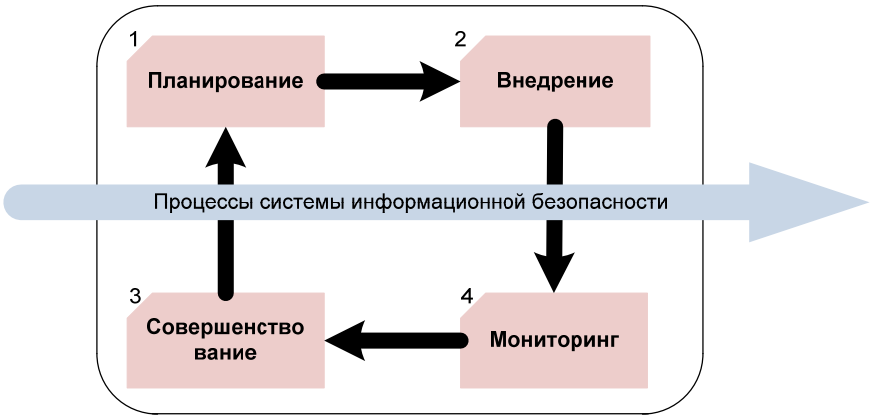

Рисунок 1 – Процессы системы информационной безопасности.

При всей своей значимости, рынок специалистов в области информационной безопасности имеет некоторые неравновесия, и ключевой проблемой, тормозящей развития этого рынка, является недостаток высококвалифицированных специалистов. В этих условиях возникает необходимость разработки новых процедур обеспечения, контроля и оценки качества образования, которые способствовали бы решению ключевой проблемы высшего образования – подготовка высококвалифицированных специалистов. Оценка качества деятельности профессорско-преподавательского состава является одной из процедур такого рода.

Начальным этапом оценки является определение критериев и показателей качества деятельности преподавателей. Однако возникает задача правильной интерпретации результатов, которая будет учитывать особенности объекта оценки, характеризующиеся большой степенью неопределенности, случайности, нестабильности и т.п. Указанные факторы учитывают нечеткие модели.

В основе организации нечетких моделей оценивания качества педагогической деятельности, положим нечеткие модели с лингвистической шкалой, которые основаны на логико-лингвистическом подходе и операциях нечеткой арифметики.

Схема нечеткой модели с лингвистической шкалой представлена на Рисунке 2.

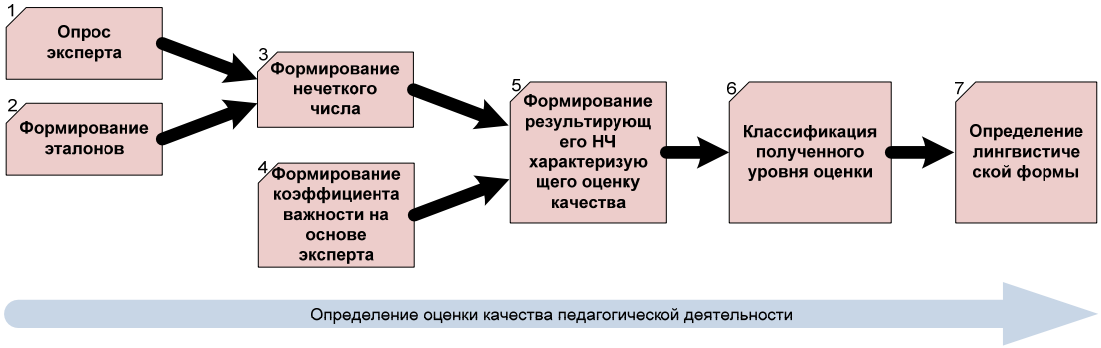

Рисунок 2 – Нечеткая модель с лингвистической шкалой.

Определение оценки качества педагогической деятельности в соответствии с нечеткой моделью с лингвистической шкалой реализуют по результатам опроса экспертов согласно составленным критериям, компоненты которого предварительно ранжируют через определение коэффициента важности P_j ($j = [1,n]$; n – количество критериев). Для этого используют метод ранжирования на основе преобразованной матрицы $A' = (a'_{vw})$, полученной на основании матрицы парных сравнений (суждений) $A = (a_{ij})$ (таблица 1). Элемент преобразованной матрицы определяют как:

$$a'_{vw} = \begin{cases} 100/(a_{ij}+1) * a_{ij}, \forall i < j : v = i, w = j, \\ 1 \qquad\qquad\qquad \forall i < j : v = w = i = j, \\ 100/(a_{ij}+1), \qquad \forall i < j : v = j, w = i, \end{cases}$$

где $i = j = [1; n]$;

n – количество критериев [1].

Таблица 1 – Шкала для построения матрицы суждений

Оценка значимости	Качественная оценка	Примечание
1	Одинаковая значимость	Альтернативы имеют одинаковый ранг
3	Слабое преимущество	Преимущество одной альтернативы перед другой малоубедительное
5	Сильное преимущество	Есть надежные доказательства существенного преимущества одной альтернативы
7	Очевидное преимущество	Существуют убедительные свидетельства в пользу одной альтернативы
9	Абсолютное преимущество	Свидетельство в пользу преимущества одной альтернативы над другой с наибольшей мерой убедительности
2, 4, 6, 8	Промежуточные значения	Используются, если необходим компромисс

Значения КВ (P_i, $i = [1;n]$) для каждого из разделов (вопросов) программы вычисляют по формуле:

$$Pi = \sum_{i=1}^{n} a_{ij} \ (i \neq j).$$

После определения коэффициентов важности осуществляют их нормализацию по выражению:

$$PN_i = P_i / (\sum_{i=1}^{n} P_i),$$

таким образом, чтобы выполнялось условие:

$$\sum_{i=1}^{n} PN_i = 1.$$

Кроме ранжирования критериев по степени важности эксперты, осуществляющие проверку, строят нечеткие эталоны, которые отображают лингвистическую переменную «Оценка качества», являющуюся образцом для сравнения нечетких чисел.

Нечеткая модель с лингвистической шкалой предполагает, что группа из N экспертов отвечает на n критериев соответственно составленных по нечеткой шкале. По ответам экспертов формируют нечеткое число (НЧ) Z_t ($t = [1;N]$), которому ставят в соответствие одно из эталонных. Значения НЧ, соответствующие оценке ответов всей группы экспертов на j-й криерий ($j = [1;n]$), определяют по формуле:

$$\underset{\sim}{L}_j = (\sum_{t=1}^{N} \underset{\sim}{Z}_t) / N,$$

где $\sum$ – нечеткое сложение, выполненное по одному из методов реализации операций нечеткой арифметики [2].

Суммарную оценку определяют с учетом ранее вычисленных коэффициентов важности:

$$\underset{\sim}{LS} = (\sum_{j=1}^{n} PN_i * \underset{\sim}{L}_j).$$

Образованное $\underset{\sim}{LS}$ сравнивают с эталонными нечетким числом, для чего используют α-уровневое расстояние [3]:

$$d(\underset{\sim}{LS}, \underset{\sim}{LV}_j) = (\sum_{j=1}^{k} \sum_{i=1}^{m} | x_i - y_j |) / k,$$
$$(\forall X_{y_{3y}} \geq \alpha)$$

где α – заданное значение α-уровня ($0 \leq \alpha \leq 1$);

x_i и y_i – носители полученного и эталонного НЧ $\underset{\sim}{LS}$ и $\underset{\sim}{LV}_j$;

m – количество компонентов НЧ $\underset{\sim}{LS}$;

k – количество компонентов НЧ $\underset{\sim}{LV}_j$ с ФП $\mu_y \geq \alpha$.

Критерием соответствия $\underset{\sim}{LS}$ одному из эталонных нечетких чисел считают минимальное α-уровневое расстояние $d\min_i$, которое и определяет уровень качества педагогической деятельности:

$$d\min_i = \bigwedge_{j=1}^{k} d(\underset{\sim}{LS}, \underset{\sim}{LV}_j),$$

где $\underset{\sim}{LV}_j$ – эталонные нечеткие числа [1].

Таким образом, получили алгоритм оценивания качества педагогической деятельности методом нечетких моделей с лингвистической шкалой. Данный алгоритм позволяет экспертам в ходе оценивая деятельности преподавателя оперировать лингвистическими переменными и сравнивать вычисленное значение нечеткого числа с эталонным, устанавливая соответствие.

Список литературы

1. Корченко А.Г. Построение систем защиты информации на нечетких множествах / А. Г. Корченко. - Киев: МК-Пресс, 2006. – 316 с.
2. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – М.: Мир, 1976. – 166 с.
3. Корченко А.Г. Черныш Л.Г. Расстояние α-уровня для сравнения нечетких чисел // Проблемы информатизации и управления: Сб. науч. тр. – К.: КМУГА, 1997. – Вып. 2. – С. 117-124.

МОДЕЛИРОВАНИЕ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ОБОБЩЕННОГО МЕТОДА ЦЕНТРА НЕОПРЕДЕЛЕННОСТИ

Варламов К.К. – студент, Архипова А.Б. – аспирант

Алтайский государственный технический университет (г. Барнаул)

Цели защиты информации в самом общем виде могут быть сформулированы как построение оптимальных систем защиты информации и организация оптимального их функционирования. На первый взгляд, здесь могли бы быть с успехом реализованы методы классической теории систем. На практике, однако, они оказываются непригодны для решения задач создания, организации и обеспечения функционирования систем защиты информации, поскольку эти методы разрабатывались применительно к потребностям технических, т.е. в основе своей формальных, систем, в то время как процессы защиты информации подвержены сильному влиянию случайных факторов, прежде всего, связанных со злоумышленными действиями людей. Кроме того, зачастую при исследовании систем защиты информации отсутствуют данные, необходимые для определения таких параметров как вероятности проявления угроз безопасности информации в различных условиях функционирования той или иной системы, вероятности успешной реализации этих угроз злоумышленником, показатели эффективности функционирования различных средств защиты и многих других. В связи с этим возникает актуальная задача расширения арсенала классической теории за счет использования методов, позволяющих адекватно моделировать процессы, существенно зависящие от воздействия трудно предсказуемых факторов в условиях неполноты доступной информации.

В такой ситуации естественно прибегнуть к эвристическим методам, основанным на оценках специалистов – экспертов в соответствующей области. Из подобных неформальных методов оценивания наиболее известными являются методы экспертных оценок. К достоинствам этих методов относится возможность их использования для широкого класса объектов исследования, относительная простота и нетребовательность к качеству исходной информации. Вместе с тем, методы экспертных оценок не лишены существенных недостатков. В их числе – субъективность оценок, основанных на интуитивном мнении экспертов, трудная сопоставимость мнений ввиду преимущественно качественного характера оценок. Частично избежать присущего экспертному прогнозированию субъективизма суждений помогает использование методов коллективной экспертной оценки с применением различных процедур и методов обработки мнений экспертов, а также использование в

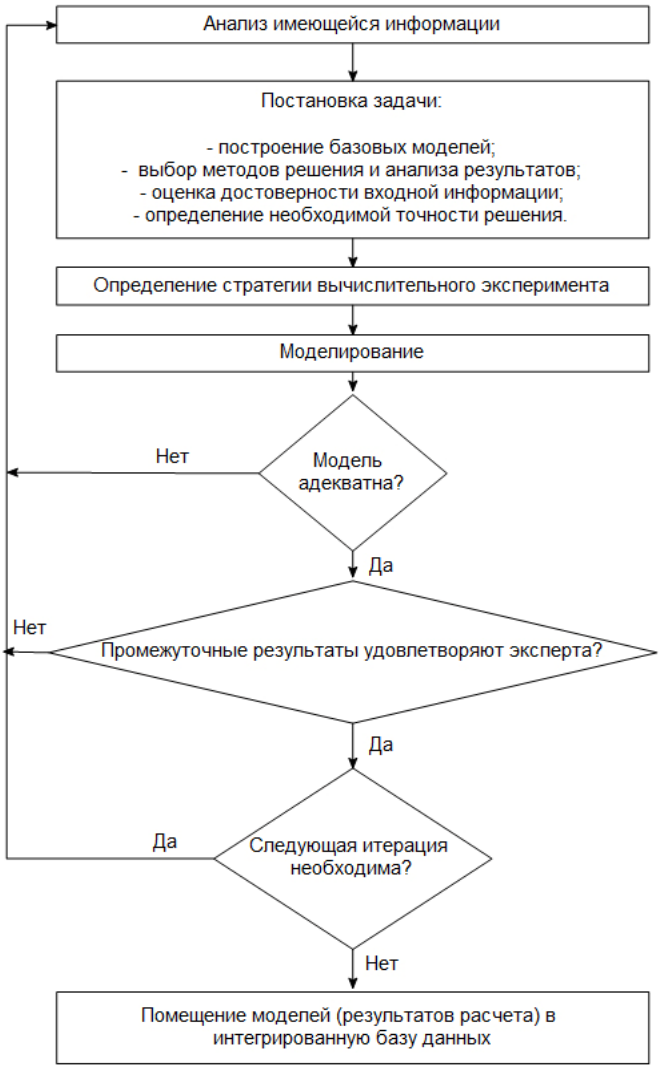

Рисунок 1 – Этапы автоформализации знаний

дополнение к экспертной оценке методов математического и имитационного моделирования. Единственным реальным способом создания моделей исследуемой ситуации на основе формализации алгоритмов аналитической деятельности в этих условиях является автоформализация знаний эксперта, т.е. возникает проблема разработки технологии формализации экспертом своих профессиональных знаний. В работах [3], [4] предложена форма автоформализации знаний, основанная на проведении вычислительного эксперимента с моделями, описывающими конкретные объекты предметной области и построенными самими экспертами. Результатом автоформализации в этом случае являются как те новые сведения, которые эксперт получил в ходе эксперимента, так и сами модели, отражающие его глубинные представления о структуре исследуемого объекта и присущих ему качественных и количественных зависимостях. Генерация моделей является ключевой в реализации процесса автоформализации знаний. С ее помощью эксперт формализует свои представления о структуре исследуемого объекта и взаимосвязях отдельных элементов в виде системы динамических моделей, позволяющей ему в дальнейшем проводить с ее помощью вычислительный эксперимент (имитационное моделирование).

На первом этапе генерации модели сущность процесса формулируется в наиболее общей, часто вербальной форме. При этом должны быть отобраны наиболее существенные переменные и показатели, достаточно полно характеризующие систему. Затем необходимо найти связь между этими показателями в виде некоторых математических зависимостей. При этом нужно использовать любую доступную «априори» информацию об объекте. Широко распространены так называемые модели «вход-выход», основанные на применении методов идентификации объектов по результатам экспериментов и испытаний. Результатом идентификации объекта является его математическая модель. Вне зависимости от способа получения модели, она является лишь приближенным, упрощенным описанием исследуемой системы, так как модели строятся в условиях неопределенности и неполноты информации. Неточность модели объекта обусловлена целым рядом причин. В частности, показатели системы практически всегда зависят от большого числа различных факторов, причем часть из них может быть даже неизвестна исследователю. При построении модели ограничиваются отбором лишь наиболее существенных переменных, неизбежно не учитывая какие-то из них, что приводит к огрублению модели. Это особенно актуально для задачи защиты информации, когда, как упоминалось выше, приходится действовать в условиях значительной неопределенности.

Из-за искажения моделей вследствие неопределенных факторов исследователь получает приближенное описание системы. Для описания факторов неопределенности могут быть

использованы различные модели, в частности, статистическая, нечеткая, интервальная. Интервальное представление факторов неопределенности имеет ряд преимуществ. Зачастую на практике нет оснований или недостаточно информации для того, чтобы рассматривать факторы неопределенности как случайные. Это приводит к необходимости учета неопределенности нестатической природы, когда относительно факторов неизвестно ничего, кроме их свойства быть ограниченными. Кроме того, как правило, отсутствует или почти отсутствует достоверная статистика. В таких условиях наиболее общей и наиболее естественной моделью описания факторов является их представление в интервальной форме, когда задают диапазон возможных значений переменных, причем переменная может принимать любое значение из интервала, и ему нельзя приписать никакой вероятностной меры. Метод анализа интервальных данных позволяет естественно и просто учесть всю априорную информацию о структуре модели и ошибке и получить достаточно точные результаты даже при небольшом числе наблюдений.

В качестве конкретного метода оценивания параметров моделируемых зависимостей предлагается использовать обобщенный метод центра неопределенности (ОМЦН). В основе ОМЦН лежит смешанная модель обработки данных, которая объединяет вероятностный и детерминированный подход. Таким образом, ОМЦН является интервально-статистическим методом. Постановку задачи на ОМЦН можно сформулировать следующим образом. Необходимо оценить параметры $[a] \in IR^n$ эмпирической зависимости

$$[y]_i = F([x]_i, [a]) \text{ для } [x]_i \in IR^n$$

по известным приближенным значениям с точностью ε функции $F([x], [a])$ в точках $[x]_i \in IR^n$. В этом случае истинные значения $[a]^* \in IR^n$ удовлетворяют системе неравенств

$$y_i^- = y_i - \varepsilon \le F([x]_i, [a]^*) \le y_i + \varepsilon = y_i^+ .$$

Данное соотношение при использовании понятия множества неопределенности

$$\Omega = \left\{ [a]^* \in R / y_i^- \le F([x]_i, [a]^*) \le y_i^+, \ i \in \overline{1,n} \right\}$$

принимает вид

$$[a]^* \in \Omega .$$

Для получения точечной оценки параметра для непустого множества неопределенности Ω по ОМЦН можно взять либо геометрический центр множества неопределенности, либо найти решение экстремальной задачи

$$\max_{1 \le i \le N} \left| F([x]_i, [a]) - [y]_i \right| \to \min_{a \in R^n} .$$

Решение данной задачи есть центр множества неопределенности Ω, т.к. в этом случае минимизируется максимально возможное отклонение теоретического значения $[y]_i^*$ от экспериментальных значений $[y]_i$.

Если множество Ω пусто, то это означает, что либо зависимость $y = F(x, a) \in R$ для $x \in R^n$ на самом деле не осуществима, либо $\min_a \max_i \left| F(x_i, a) - y_i \right| > \varepsilon$, т. е. завышена погрешность измерения y_i^* для $i \in \overline{1,N}$.

Так как определение центра множества неопределенности Ω в общем случае является сложной задачей, то при практическом использовании ОМЦН представляют интерес аппроксимации множества Ω простыми геометрическими фигурами сверху и снизу. Для простейшего случая линейной двухпараметрической зависимости аппроксимацию проводят прямоугольником, параллелограммом, кругом и эллипсом. Для многопараметрического пространства аппроксимации множества неопределенности используют эллипсоиды, шары и параллелепипеды.

Список литературы

1. Белов В.М. Оценивание параметров эмпирических зависимостей методом центра неопределенности / В. М. Белов, Ф. Г. Унгер, Ю. А. Карбаинов, В. И. Пролубников, Н. П. Тубулов. – Новосибирск: Наука, 2001. – 176 с.
2. Гончаров С.А. Оценивание параметров линейных экспериментальных зависимостей обобщенным методом центра неопределенности / С. А. Гончаров, В. М. Белов, Е. В. Рябова, В. Т. Гетманов. – Рубцовск: РИО, 2005. – 130 с.
3. Громов Г.Р. Национальные информационные ресурсы: проблемы промышленной эксплуатации / Г. Р. Громов. – М.: Наука, 1985. – 238 с.
4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А. А. Малюк – М.: Горячая линия-Телеком, 2004. – 280 с.
5. Жилин С. И. Нестатические модели и методы построения и анализа зависимостей: Дис. канд. физ.-мат. наук / С. И. Жилин. – Барнаул, 2004. – 119 с.
6. Вощинин А.П. Оптимизация в условиях неопределенности / А. П. Вощинин, Г. Р. Сотиров. – М. – София: МЭИ (СССР); Техника (НРБ), 1989. – 224 с.

К ВОПРОСУ ОБ ОЦЕНКЕ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ИНТЕРВАЛЬНОГО ФАКТОРНОГО АНАЛИЗА

Веснин Я.А. – студент, Архипова А.Б. – аспирант

Алтайский государственный технический университет (г. Барнаул)

Зачастую, в своей повседневной деятельности руководству практически каждого предприятия приходится принимать оперативные управленческие решения, находясь в условиях неопределенности. И это, в первую очередь, касается сферы обеспечения информационной безопасности (СОИБ) предприятия. СОИБ должна оценивать состояние критичности ситуации, связанной с нарушением информационной безопасности предприятия, уровнем риска ее нарушения, а также оказывать поддержку в принятии решений относительно действий в данной ситуации. Реализация замыслов в такой системе затруднена по ряду причин: не всегда возможно сформировать полное множество угроз информационной безопасности, количественно оценить степень критичности возникшей ситуации, построить прогноз ее развития. Другими словами, основная проблема заключается в зачастую неполных и неопределенных исходных данных о состоянии системы защиты информации, возможных угрозах, дестабилизирующих факторах.

В такой ситуации принять эффективное решение помогает интервальный анализ, который в своем классическом представлении разработан для данных, полученных при измерениях по интервальным, строго недетерминированным шкалам.

В частности, одной из возможных моделей, которые используются в интервальном анализе для описания объекта исследования, является модель "вход-выход", основанная на применении методов идентификации объекта по результатам экспериментов и исследований [1]. Но зачастую в реальных условиях невозможно предположить (даже гипотетически) возможность многократного повторения эксперимента, т.к. слишком высока цена неудачи. Ведь после данной ошибки предприятие может перестать существовать или понести огромные потери.

Все это приводит к необходимости учета и подробного описания всех факторов неопределенности. Для решения данной проблемы используют интервальную форму описания неопределенности [2]. На практике источниками неопределенности ожидаемых условий в развитии предприятий служат поведение конкурентов, персонала организации, технические и технологические процессы, изменения конъюнктурного характера и др. [4]. Именно конкретные значения этих показателей и должны быть преобразованы в объекты

интервальной модели.

На начальном этапе формулируют гипотезы или предположения развития событий. Причем данные гипотезы должны соответствовать аксиомам, на которых базируется метод интервального анализа данных. Они состоят в том, что зависимости между выходными переменными (которые и будут решением) и независимыми переменными (которые непосредственно оказывают влияние на решение) должны быть линейнопараметризованными, а данные экспериментов - описаны совокупностью опытов. Адекватной моделью объекта будет функция, проходящая через все интервальные измерения [1].

Далее формируют область возможных значений параметров модели. С этой целью в функцию, олицетворяющую модель объекта, подставляют результаты экспериментов. Результат подстановки - система линейных неравенств, графическое отображение которых представляет собой область возможных значений. Выделяют несколько вариантов построения:

1. Если проводилось несколько экспериментов, то область значений - выпуклый многоугольник.

2. В случаях, когда многократное повторение эксперимента невозможно, область значений имеет вид прямой и называется единственной линейной моделью, адекватной интервальным измерениям [1].

Следующий этап состоит в определении точечных оценок коэффициентов. Для этого вычисляют минимаксную оценку как половину модуля разности двух наиболее отдаленных угловых точек множества. Среднюю оценку вычисляют как центр тяжести допустимого множества, т.е. как значение частного от суммы всех значений угловых точек допустимого множества и количества этих точек [3].

Используя полученные оценки коэффициентов, записывают модель выходной переменной при фиксированном векторе входных переменных. В этом случае точечная оценка определяет некоторую модель прогноза как функцию заданного вида, проходящую через все интервальные измерения, а интервальная оценка определяет множество функций заданного вида, проходящих через все интервальные измерения.

Как и любой математический метод, интервальный анализ обеспечивает достоверные результаты лишь при выполнении исходных предпосылок, в справедливости которых на практике необходимо убедиться путем проверки гипотез. В своем классическом представлении интервальный анализ допускает интервальные ошибки измерения. К таким ошибкам относятся ошибочное расширение или ошибочное сужение интервалов [3].

В результате решения адекватной моделью считается та, точечные оценки которой принадлежат области допустимых значений, если последнее не пусто. Выбрать наилучшую модель из нескольких получившихся несложно. В интервальном анализе более простая модель оказывается одновременно и более точной, т.к. у нее меньше максимальная и средняя ширина коридора ошибок. На основе этого утверждения можно сделать вывод о том, что наилучшей интервальной моделью следует считать наиболее простую функцию с наименьшим числом коэффициентов или наиболее простой структуры, проходящей через все интервальные измерения.

Список литературы

1. Вощинин А.П. Оптимизация в условиях неопределенности / А. П. Вощинин, Г. Р. Сотиров. — М.:МЭИ, София: Техника, 1989. — 224 с.
2. Вощинин А.П. Интервальный анализ данных: развитие и перспективы / А. П. Вощинин. — Заводская Лаборатория. — 2002. — №1.
3. Вощинин А.П. Интервальный метод калибровки / А. П. Вощинин, Н. В. Скибицкий. — Заводская Лаборатория. — 2002. — №7.
4. Викторов В.И., Шашнов С.А. Анализ факторный [электронный ресурс] — http://www.ecsocman.edu.ru/db/msg/88190.html.

РАЗРАБОТКА УНИВЕРСАЛЬНОГО ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА «ЛАБОРАТОРИЯ НА ОДНОМ ДИСКЕ «ЭЛЕКТРОМАГНИТНЫЕ ИЗМЕРЕНИЯ»

Донцов А.А., Прокопов Д.А., Петрицкий Р.В. – студенты
*Дмитриев С.Ф. – к.т.н., докторант, Ишков А.В. – к.х.н., д.т.н., профессор
Алтайский государственный аграрный университет (г. Барнаул)
*Алтайский государственный университет (г. Барнаул)

Реализуемая нами концепция виртуализированных приборов - программно-аппаратных (ПА) комплексов, используемых для проведения оперативных измерений физических и физико-химических величин в образовании, научных исследованиях и в быту, базируется на максимальной виртуализации функций прибора не связанных с непосредственным получением измерительной информации от контролируемого объекта и среды [1].

Ранее в Алтайском государственном университете и Алтайском государственном аграрном университете был разработан ряд виртуализированных приборов, предназначенных для решения частных задач электромагнитных измерений: измерения предельно-допустимого уровня электромагнитных излучений (по магнитной компоненте ЭМИ), измерения напряженности постоянного и переменного магнитного поля, исследование спектральной характеристики ЭМИ в звуковом диапазоне, измерение электропроводности неферромагнитных материалов, измерение электропроводности полупроводников и пр. [2].

Эти приборы реализуют неразрушающий метод вихревых токов (МВТ) или магнитометрический метод, либо их частные случаи, и построены по общей схеме ПА-комплекса, состоящего из выносного трансформаторного или *L*-датчика, с электрическими параметрами, позволяющими непосредственно подключать его к входу-выходу звуковой карты ЭВМ и специализированного ПО, выполненного в формате самоисполняемого в среде ОС Windows *.exe файла.

Виртуализированные приборы МВТ работают следующим образом: цифровой сигнал от виртуального генератора поступает на ЦАП звуковой карты и преобразуется в аналоговый. Аналоговый сигнал, с выхода усилителя мощности (У) нагружен на генераторную катушку (Г) ВТП. Электромагнитное поле наводит ЭДС в приемной катушке (П) ВТП. ЭДС, усиленная микрофонным усилителем, поступает на вход АЦП звуковой карты. Оцифрованный сигнал поступает далее на блок обработки и управления ПО. Блок обработки и управления фиксирует уровень цифрового сигнала в условных единицах. Этот уровень принимается за уровень нуля и соответствует уровню напряжения на сигнальной катушке без объекта контроля. На индикатор интерфейса выводится ноль, который соответствует нулевому значению измеренного параметра.

В случае взаимодействия ВТП с объектом происходит изменение уровня и характеристик входного сигнала АЦП, как по отношению к нулевому сигналу, так и по отношению к сигналу на выходе ЦАП.

Например, для контроля полупроводниковых материалов, топологии интегральных микросхем и элементной базы РЭА, был разработан виртуализированный прибор ИЭПП-1. ИЭПП-1, который позволяет определять основные физические параметры полупроводниковых материалов, состояние омических и выпрямляющих контактов, качество исполнения планарных структур. Исследование физических характеристик полупроводниковых структур основано на зависимостях напряженности поля вихревых токов от свойств материала, а топологические характеристики планарных структур могут быть определены из функции напряжения измерительной обмотки вихретокового трансформаторного датчика-преобразователя (ВТП) от расстояния до объекта при восстановлении траектории перемещения датчика над его поверхностью.

Также нами были разработаны ПА-комплексы для измерения уровня напряженности переменного магнитного моля - виртуализированный измеритель переменного магнитного поля со встроенным Фурье-анализатором спектра ИНПМП-5 ФА, измеритель напряженности постоянного магнитного поля ИНПМП-1, измеритель электропроводности неферромагнитных материалов ИЭНМ-20 [3].

Чувствительным элементом во всех приборах является универсальный сверхминиатюрноый ВТП-датчик (СМВТП), конструкция которого приведена ниже.

Датчик выполнен по схеме дифференциального ВТП с тремя катушками, одна из которых является калибровочной, а другие - возбуждающей и измерительной.

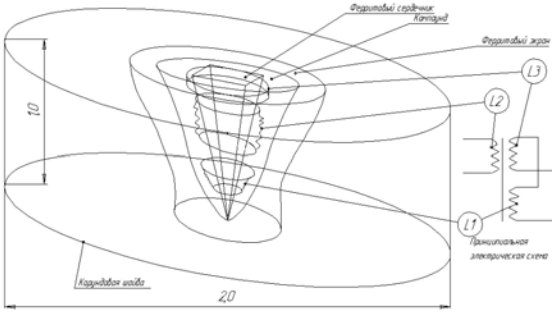

Рис. 1. Конструкция универсального широкополосного, самокалибрующегося СМВТП

Раздельное или совместное использование катушек датчика позволяет использовать его либо как широкополосный *L*-датчик для магнитометрии, либо как самокалибрующийся ВТП в МВТ, а дифференциальное включение катушек датчика и фокусировка возбуждающего поля его сердечником позволяет проводить локальные исследования различных материалов на площади до 500-1 000 нм^2. Электрические же характеристики датчика позволяют подключать его непосредственной к входу и выходу звуковой карты ЭВМ.

ПО обработки измерительных сигналов в приборах на основе этой конструкции датчика выполнено на языке высокого уровня C++ в инструментальной оболочке Builder C++ v.6.0 и устанавливается на любые типы современных ПК, функционирующих под управлением ОС Windows 95/98/2000/XP.

Для реализации специализированных приложений нами был выбран интерфейс низкого уровня, включающий самый элементарный уровень сервиса, обычно предоставляемого непосредственно драйвером устройства. Низкий уровень позволяет приложениям получить доступ к буферам, содержащим воспроизводимые или записываемые звуковые данные, работать с внутренней структурой файлов, содержащих звуковую информацию, а также использовать другие дополнительные возможности [4].

В отличие от интерфейса MCI, где многие параметры воспроизведения/записи принимаются по умолчанию, интерфейс низкого уровня требует учета всех деталей этого процесса, позволяя получить большую гибкость и возможность работы со звуковыми данными в реальном времени, необходимые для реализации прибора МВТ.

Так как звуковое устройство, используемое нами как высокоскоростное АЦП/ЦАП в составе ПА-комплекса, в Windows может одновременно использоваться не только специализированным приложением, но и любой другой программой или самой ОС, требуется надежный контроль его переменных параметров в процессе работы виртуализированного прибора (любое из приложений, обращающихся к адаптеру через mmsystem.dll, может изменить параметры входного и выходного сигнала, уровень громкости записи/воспроизведения, частоты каналов и пр.).

Микшеры, как вполне самостоятельные блоки звуковых адаптеров и виртуальных синтезаторов, также управляются в MME отдельной подсистемой, но в отличие от

дополнительных устройств, в отношении которых из Windows доступно только управление громкостью, микшер позволяет осуществлять приложению коммутацию источников и приемников звука, регулировку уровня, панорамы, тембра и других параметров звука, смешивать несколько источников звука в единый звуковой сигнал, осуществлять контрольное прослушивания и корректировку сигнала, на одной или нескольких линиях.

С использованием описанного выше подхода управления звуковым адаптером, его настройками и связи со стандартными библиотеками ОС Windows, а также оригинальной конструкции СМВТП, нами был разработан универсальный виртуализированный измерительный комплекс для электромагнитных измерений (лаборатория на одном диске «Электромагнитные измерения»).

Комплекс состоит из компьютерной оболочки, с интуитивно-понятным интерфейсом, запускающим различные измерительные, калибровочные, преобразовательные и иные модули программ – отдельных виртуальных приборов, и систему автоматического перенастраивания параметров внешнего ВТП-датчика (рис. 2).

Рис.2. Различные варианты комплектации лаборатории на одном диске «Электромагнитные измерения»

Использование такого подхода позволило интегрировать в составе одного программно-аппаратного комплекса все разработанные ранее измерительные устройства.

Лаборатория на одном диске «Электромагнитные измерения» может найти широкое применение в научных исследованиях, образовательном процессе ВУЗ-ов и школ, а также в повседневной жизни, так как стоимость всего комплекта не превышает 6 000 - 8 000 руб., а для превращения пользовательско ПК в измерительный прибор требуется только подключение универсального датчика и запуск программы-оболочки.

Список литературы

1. Ишков А.В., Дмитриев С.Ф. Современная концепция сопряжения измерительных приборов с ЭВМ. // Мат. Междунар. научн.-техн. конф. «ИКИ-2007». -Барнаул: Изд-во АлтГТУ, 2007. С.3-6.
2. Дмитриев С.Ф., Панов С.Г., Ишков А.В. // Ползуновский альманах. № 2. 2008. С. 15-20.
3. Рябинин А.А., Маеренко А.А., Панов С.Г. и др. // Горизонты образования. Вып.10. 2008.
4. Ишков А.В, Дмитриев С.Ф., Новоженов А.В., Лященко Д.Н. Программное обеспечение приборов неразрушающего контроля, реализующих метод вихревых токов. // Труды VII-ой научн.-техн. конф. «Научное программное обеспечение в образовании и научных исследованиях». – СПб.-М.: Изд-во Нестор, 2009. С. 82-89.

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ В ОРГАНИЗАЦИИ

Ефименко К.Н. – студент, Плетнев П.В. – аспирант, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Развитие современной цивилизации характеризуется переходом от индустриального общества к обществу информационному. В информационном же обществе сейчас циркулируют большие потоки информации и соответственно человеку, чтобы обрабатывать эти потоки информации самостоятельно, просто не хватает времени, поэтому появляется необходимость в создании средств автоматизации его деятельности [1]. Эта проблема характерна для специалистов по защите информации проектирующих комплексную систему защиты информации в организации.

При проектировании комплексной системы защиты информации выполняются следующие задачи:

1) Аудит состояния объектов информатизации в организации;
2) Разработка организационно-распорядительной и нормативно-методической документации по вопросам защиты;
3) Выбор, установка и ввод в эксплуатацию технических средств защиты;
4) Аттестацию объектов информатизации.

Разработка организационно-распорядительной документации в современных условиях является сложным, объемным и трудоемким процессом.

На разработку пакета документов у специалиста по защите информации уходит в среднем 2 рабочих дня (16 часов) при наличии типовых документов (шаблонов). Для автоматизации этого процесса разработан программный продукт “Автодок-ЗИ”, который позволяет выполнить указанную работу не более чем за один час.

Разработанный программный продукт предназначен для автоматизации процесса заполнения организационно-распорядительной документации.

Данная программа написана на языке Java 2 [2]. Для корректной работы программы необходимо установить Java-машину, создать массив шаблонов документов. Шаблоны документов нужно составить при помощи программного продукта OpenOffice.

В программе реализовано заполнение 28 документов, но их количество может быть еще большим лишь бы в шаблонах указывались те переменные которые существуют в программе иначе процесс замены попросту не произойдет.

Перед началом работы с программой необходимо указать пусть к шаблонам документов и путь куда будут сохраняться уже готовые документы.

В данной программе предусмотрено создание не всех сразу документов, а выборочно.

Программа состоит из двух модулей: первый модуль программы заполняет практически все документы по принципу поиска переменной и ее замены на ранее введенную специалистом по защите информации (то есть первым этапом работы программы является ввод необходимых переменных, в некоторых случаях переменная вводится во всех падежах), вторая часть программы реализует заполнение документа «модель угроз». Пример работы первого модуля представлен на рисунке 1.

Заполнение документа «модель угроз» вынесено во вторую часть, потому что там от специалиста по защите информации требуется заполнение полей угроз безопасности персональным данным, которые не характерны для заполнения остальных документов и также для построения модели угроз необходим расчет коэффициентов, которые производит данная программа.

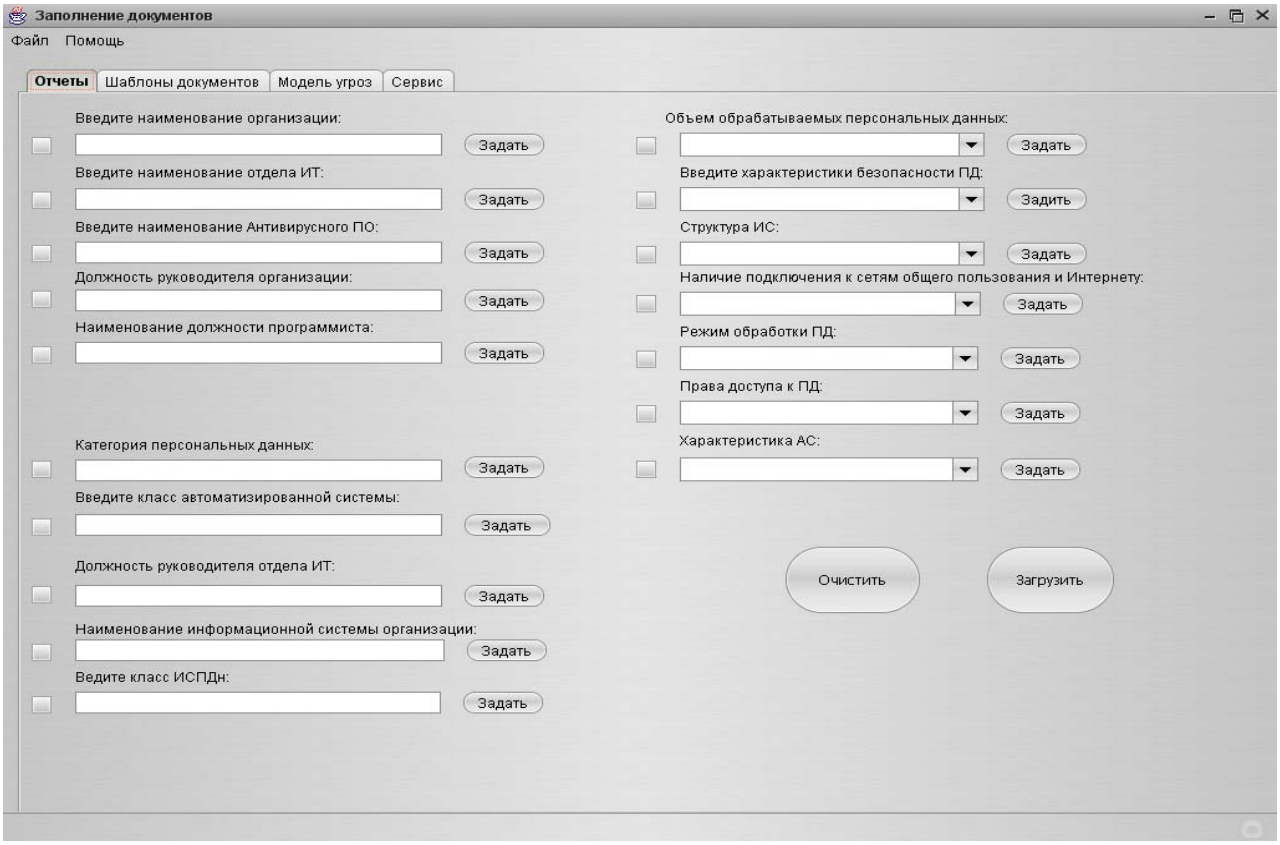

Рисунок 2 – Работа первого модуля программы

Теперь перейдем непосредственно к самому алгоритму создания модели угроз:

1. Необходимо собрать нужную информацию об информационных системах персональных данных (ИСПДн), ее можно получить из таблицы 1.

Таблица 1 – Показатели исходной защищенности информационных систем персональных данных

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности			Уровень защищенности		
	Высокий	Средний	Низкий	Высокий	Средний	Низкий
1. По территориальному размещению						
Распределённая ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			+			
Городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			+			
Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации		+			1	
Локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий		+				
Локальная ИСПДн, развернутая в пределах одного здания	+					

В данной статье приведен лишь фрагмент таблицы, а именно 1 характеристика ИСПДн - по территориальному размещению. Полная таблица содержит помимо этой, следующие характеристики: по наличию соединения с сетями общего пользования, по встроенным (легальным) операциям с записями баз персональных данных, по разграничению доступа к персональным данным, по наличию соединения с другими базами персональных данных иных ИСПДн, по уровню (обезличивания) персональных данных, по объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки.

Специалист по защите информации в этой таблице заполняет лишь 3 последние колонки: он ставит 1 в ту колонку на пересечение с которой находится «+».

Далее идет подсчет единиц в каждом столбце в процентном содержании от 7, затем рассчитывается показатель защищенности (Y_1), он равен 0, если в столбце с уровнем защищенности низкий появится 0% и в столбце с уровнем защищенности средний окажется меньше либо равно 30%, показатель защищенности равен 5 , если столбец с уровнем защищенности высокий меньше либо равен 30%, в противном случае показатель защищенности равен 10 [3].

2. Далее определяется структура ИСПДн (АРМ, локальная ИС, распределенная ИС) и наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена. В зависимости от выбора те или иные угрозы безопасности персональным данным будут присутствовать или отсутствовать. Каждая организация которая занимается разработкой моделей угроз определяет свой перечень угроз в зависимости от места функционирования [4].

3. Идет подсчет возможности реализации угрозы(низкая, средняя, высокая, очень высокая), вероятность реализации угрозы определяется экспертной комиссией, в которую входит сотрудник организации, которая проектирует модель угроз и несколько сотрудников организации для которой модель угроз проектируется [3].

4. Создается сама модель угроз в которой, помимо таблиц с угрозами и вероятностями их реализации отдельным пунктом отмечены угрозы с высокой и очень высокой вероятностью реализации. Программа подсчитывает коэффициент реализуемости угрозы для каждой из угроз в зависимости от места функционирования угрозы и выделяет угрозы с высокой и очень высокой вероятностью реализации.

Завершающим этапом работы программы является создание документа и его сохранение по указанному в программе маршруту.

Использование программного продукта “Автодок –ЗИ” позволяет существенно сэкономить время специалиста по защите информации на разработку пакета организационно-распорядительной документации по защите информации и повысить эффективность работы ООО “Центр Информационной Безопасности”, в котором планируется его применение.

Список литературы

1. Машкина И. В.,Рахимов Е.А., Васильев В.И. Методика построения модели комплексной оценки угроз информации, циркулирующей на объекте информатизации [электронный ресурс]. - http://www.contrterror.tsure.ru/site/magazine7/07-27-Mashkina-Rahimov-Vasilyev.htm
2. Хорстманн К., Корнелл Г. “Java 2”, Изд-во: Вильямс, 2008. – 812 с.
3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [электронный ресурс]. - http://www.fstec.ru/_razd/_isp0o.htm
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [электронный ресурс]. - http://www.fstec.ru/_razd/_isp0o.htm

ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗ С ПОМОЩЬЮ ИСЧИСЛЕНИЯ ПРЕДИКАТОВ

Кайзер Ф.Ю. – студент, Плетнёв П.В. – аспирант
Алтайский государственный технический университет (г. Барнаул)

В условиях повсеместной компьютеризации и автоматизации деятельности организаций необходимо эффективно обеспечивать защиту информации, для чего необходимо правильно оценивать информационные риски, возникающие на объекте информатизации. Оценка рисков предприятия является очень сложной задачей, в связи с наличием у предприятий большого количества активов, а также угроз и уязвимостей, присущих этим активам. Процедура оценки рисков также предъявляет высокие требования к квалификации специалиста. В подобных условиях представляется актуальным рассмотреть возможность применения исчисления предикатов для автоматизации процесса оценки рисков.

Для определения уровня риска необходимо определить два показателя: вероятность реализации угрозы (ее актуальность для предприятия) и величину ущерба от реализации данной угрозы. Так как вопрос определения величины ущерба, в большой степени, относится к области экономики, то далее в данной статье рассматривается применение предикатов только для определения вероятности реализации угрозы.

Исчисление предикатов (логика первого порядка) — формальное исчисление, допускающее высказывания относительно переменных, фиксированных функций, и предикатов. Исчисление предикатов расширяет логику высказываний и, в свою очередь, является частным случаем логики высшего порядка.

Предикат — это функция с множеством значений {0,1} (или «ложь» и «истина»), определённая на множестве $M = M_1 \times M_2 \times \ldots \times M_n$. Таким образом, каждый набор элементов множества M он характеризует либо как «истинный», либо как «ложный».

Предикат называют тождественно-истинным и пишут $P(x_1, \ldots, x_n) \equiv 1$ если на любом наборе аргументов он принимает значение 1. Предикат называют тождественно-ложным и пишут $P(x_1, \ldots, x_n) \equiv 0$ если на любом наборе аргументов он принимает значение 0. Предикат называют выполнимым, если хотя бы на одном наборе аргументов он принимает значение 1.

Для построения формул используются знаки логических связок. В качестве таких связок выступают конъюнкция, дизъюнкция и отрицание, а также импликация.

В исчислении предикатов используются два квантора: квантор общности и квантор существования. Первый обозначается как $\forall$, а запись $\forall x P(x)$ эквивалентна утверждению «Для всех x из области его определения имеет место P(x)». Второй квантор обозначается как $\exists$, а запись $\exists x P(x)$ эквивалентна утверждению «Найдется по крайней мере один x* в области определения x, такой, что истинен P(x*)». Переменные, находящиеся в сфере действия кванторов, называются связанными, остальные переменные — свободными.

Для автоматизации процесса оценки актуальности угроз с помощью исчисления предикатов должно быть изначально задано пять множеств и три предиката.

Изначально задаваемые множества:

1. X – множество фактов (например, сервер установлен в отдельном помещении, кабели проложены в специальных коробах и т.д.);
2. Y – множество уязвимостей (уязвимых звеньев);
3. Z – множество угроз безопасности информации;
4. Q – множество вопросов, задаваемых пользователю для определения актуальности угроз.
5. W – множество ответов.

Используемые предикаты:

1. P1(x,y) – предикат, определенный на множествах значений X и Y и задающий отношение «если на предприятии имеет место факт x, то имеется и уязвимость y».

2. P2(y,z) – предикат, определенный на множествах значений Y и Z и задающий отношение «если на предприятии имеется уязвимость y, то имеется и угроза безопасности z».
3. P3(q,w) – предикат, определенный на множествах значений Q и W и задающий отношение «ответом на вопрос q, является ответ w».

На основе исходных данных о предприятии выбирается некоторое подмножество $X_1 \subseteq X$. С помощью предиката P_1 определяется подмножество $Y_1 \subseteq Y$ – множество уязвимостей предприятия. С помощью предиката P_2 определяется подмножество $Z_1 \subseteq Z$ – множество угроз безопасности информации на предприятии.

Затем пользователь, отвечая на вопросы, определяет значения предиката P_3 для всего множества значений Q и W. Каждому элементу множества W соответствует некоторая вероятность. Далее с помощью предиката P_3 заполняется матрица $P'' = |P_{ij}|$ - каждое значение которой показывает вероятность того, что могут сложиться благоприятные условия для использования j-ой уязвимости для реализации i-ой угрозы.

При этом вероятность наличия благоприятных условий для реализации i-ой угрозы определяется из соотношения:

$$P^*_i = 1 - \prod_{k=1}^{n} (1 - p''_{ik}),$$

где n – количество уязвимостей.

Таким образом, получив количественную оценку актуальности угрозы можно осуществить качественную интерпретацию.

Данный метод может дополняться выводом на семантических сетях. Семантическая сеть это информационная модель предметной области, имеющая вид ориентированного графа, вершины которого соответствуют объектам предметной области, а дуги (рёбра) задают отношения между ними. Объектами могут быть понятия, события, свойства, процессы. Таким образом, семантическая сеть является одним из способов представления знаний. Семантическая сеть наглядно отражает взаимосвязи между элементами «модельного мира» и позволяет значительно упростить дальнейший анализ сложившейся на предприятии ситуации в области информационных рисков.

Список литературы

1. Поспелов Д. А. Моделирование рассуждений. Опыт анализа мыслительных процессов. – М.: Радио и связь», 1989.
2. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры утвержденная заместителем директора ФСТЭК 18 мая 2007 года.

О ПОСТАНОВКЕ ЗАДАЧИ ВЫБОРА ЭКСПЕРТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ЭНТРОПИЙНОГО ПОДХОДА

Козлова С.Б. – студент, Архипова А.Б. – аспирант, Белов В.М. – к.ф.-м.н., д.т.н., профессор

Алтайский государственный технический университет (г. Барнаул)

Среди современных проблем проектирования комплексных систем защиты информации на объектах информатизации предприятия актуальными являются проблемы, связанные с:

- оценкой угроз информационной безопасности;
- выбором оптимального варианта системы защиты;

– оценкой текущего уровня информационной безопасности;
– оценкой эффективности системы защиты;
– принятием управленческих решений в области обеспечения информационной безопасности.

Решение задач такого класса невозможно без использования методов экспертного оценивания, которые представляют собой процедуру получения оценки интересующего вопроса на основе группового мнения специалистов (экспертов).

При использовании этих методов возникает проблема выбора экспертов в области информационной безопасности, т.е. выбора из некоторого множества специалистов (кандидатов в эксперты) лиц, наиболее компетентных в области информационной безопасности, и составления из них экспертных групп.

Понятие компетентности специалиста подвергают анализу на предмет выделения отдельных характеристик (свойств, качеств), выражающих это понятие. Затем производят измерение этих характеристик.

Достаточно трудно составить список характеристик компетентности так, чтобы он был полон и в то же время содержал действительно существенные характеристики. В свою очередь, «компетентность» должна быть не только содержательно описана и определена, но также и измерена, это означает, что предложенные характеристики должны поддаваться выявлению, измерению и наблюдению.

В литературе описывают два подхода к этой задаче:

1. Априорный – заключается в оценке компетентности до начала экспертизы и направлен на выбор экспертов и формирование экспертных групп.

2. Апостериорный – направлен на определение компетентности по результатам экспертизы и нацелен на учет компетентности при обработке данных опроса и на отбор экспертов для будущих экспертиз. Данный подход применим как способ отбора в тех случаях, когда производят регулярную серию повторяющихся однотипных экспертиз [1].

В рамках этих подходов существуют методы оценки компетентности, которые можно представить в таблице:

Таблица 1 – Подходы к выбору экспертов

Подход	Группа методов	Содержание
Априорный	Эвристические оценки	• самооценка эксперта (субъективная оценка) • объективная оценка эксперта • взаимная оценка • оценка аргументированности • оценка знакомства с объектом экспертизы • оценка рабочей группы
	Тестовые оценки	• оценка воспроизводимости результатов • оценка квалиметрической компетентности • оценка объективности корректирования оценок
	Методы номинальной классификации	• метод построения классов, основанный на энтропии
Апостериорный	Статистические оценки	• оценка по отклонению от среднего мнения экспертной группы • оценка согласованности экспертов

Эвристические оценки экспертов определяет человек, и основаны на том, что представление, сложившееся о данном эксперте у окружающих (или у него самого), достаточно правильно отражает его истинное качество [2].

Тестовые методы представляют собой проведение испытаний, в ходе которых оценивают

некоторые психофизиологические особенности, от которых зависит качество эксперта. Тестирование заключается в решении экспертами задач, подобных реальным, с известными (но не экспертам) ответами. На основании результатов тестирования устанавливают компетентность и профпригодность экспертов.

Методы номинальной классификации применяют для анализа качественных характеристик экспертов. Сначала организуют тестирование кандидатов в эксперты или опрос на предмет интересующих качественных характеристик. Затем на основе полученных ответов проводят энтропийный анализ, в результате которого кандидаты классифицируются по тестам с максимальной различающей способностью. На основе полученных классов оценивают компетентность экспертов.

Статистические оценки применяют с целью уменьшения по мере возможности погрешностей, возникающих при экспертных оценках. Случайная погрешность зависит от психофизиологических особенностей эксперта, его собранности, внимательности и т.д. Случайную погрешность экспертной оценки можно уменьшить многократным повторением оценок, однако, систематическая погрешность при этом останется неизменной, так как основная причина систематической погрешности – недостаточная или неправильная информированность эксперта [3].

В последние несколько лет было показано, насколько велико значение общей или совместной энтропии, используемой в качестве меры дисперсии переменных, измеренных в номинальной шкале. К. Шэннон объяснил, что существует зависимость между длиной закодированного сообщения и энтропией [5]. С. Кулбэк обобщил понятие канала информации для большинства статистических экспериментов [6]. Для решения задач классификации энтропия впервые была применена в работах [7]. Отмечается, что «результатом классификации является упорядоченный набор классов, каждый из которых описывается как можно большим числом дедуктивных высказываний, которые наилучшим образом описывают характеристики индивидов данного класса». С помощью энтропии оценивают дисперсию каждого теста и определяют наиболее информативные тесты, на основе которых происходит построение классов. Теорему Шеннона используют для того, чтобы определить, сколько тестов должно быть в наборе, чтобы индивиды классифицировались правильно.

Не смотря на наличие работ в ряде областей, методы классификации, основанные на энтропии в области информационной безопасности еще практически не применялись. В большинстве случаев на начальном этапе выбор экспертов проводился на основе объективной оценки и самооценки эксперта.

На сегодняшний день необходимо адаптировать существующий энтропийный подход к задаче выбора экспертов в области информационной безопасности.

Список литературы

1. Панкова Л.А. Организация экспертизы и анализ экспертной информации / Л.А. Панкова, А. М. Петровский, М. В. Шнейдерман. – М.:Наука, 1984. – 120 с.
2. Шибанов Г.П. Информационные технологии // Порядок формирования экспертных групп и проведения коллективной экспертизы. – 2003 - №12.
3. Бешелев С.Д. Математико-статистические методы экспертных оценок /С. Д. Бешелев, Ф. Г.Гурвич – М.:1980.
4. Rescigno A. The Information Content of Biological Classifications // Information Theory. A Symposium Held at the Royal Institution. L.: Butterwood, 1960.
5. Shannon C.E. A Mathematical Theory of Communication // Bell System Tech. J. 1948. 27.
6. Kullback S. Information Theory and Statistics. N.Y.: Wiley, 1959.
7. Мёллер Ф. Роль энтропии в номинальной классификации / Математика социологии. Моделирование и обработка информации / Под ред. А. Аганбегяна, Х. Блейлока, Ф. Бородкина, Р. Будона, В. Капекки. М.: Мир, 1977.

ПРАВОВЫЕ ОСНОВЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лесковец О.С. – студент, Пивкин Е.Н. – к.т.н., ст. преподаватель
Белов В.М. – к.ф.-м.н., д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Аудит информационной безопасности (ИБ) позволяет оценить текущую безопасность функционирования информационных систем (ИС) организации, оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы организации, корректно и обоснованно подойти к вопросу обеспечения безопасности ее информационных активов, стратегических планов развития, содержимого корпоративных баз данных и т.д.

Под аудитом ИБ понимают независимую оценку текущего состояния системы ИБ, устанавливающую уровень ее соответствия определенным критериям (требованиям), отраженным в нормативных документах по ИБ: стандартах, руководящих документов и т.д.

Стандарты ИБ, затрагивающие основы аудита ИБ условно разбивают на 4 группы (рисунок 1):

1) Зарубежные стандарты и методики, правовые аспекты и руководства по основам аудита ИБ.

2) Национальные стандарты и руководства по основам аудита ИБ.

3) Отечественные стандарты по основам аудита ИБ, руководящие документы ФСТЭК.

4) Стандарты организаций в области аудита ИБ.

Рисунок 1 – Правовые основы аудита ИБ

Практические вопросы управления ИБ организации отражены в зарубежных (международных) правовых аспектах, стандартах и руководствах по основам аудита ИБ: стандарты управления ИБ ISO 15408, ISO 17799 (BS7799), BSI, стандарты аудита ИС и ИБ COBIT, NIST, SysTrust и некоторые другие, аналогичные им.

Международные стандарты ISO 17799, ISO 27001 и ISO15408 служат основой для проведения аудита ИБ организации [1]. Стандарт ISO 17799 сосредоточен на вопросах организации и управления безопасностью, стандарт ISO 27001 устанавливает подход к процессу создания, обеспечения, управления, мониторинга, контроля, поддержания и улучшения системы управления ИБ организации, а стандарт ISO 15408 определяет детальные требования, предъявляемые к программно-техническим механизмам защиты информации (ЗИ).

Немецкий стандарт «BSI\IT Baseline Protection Manual» содержит руководство по обеспечению безопасности информационных технологий (ИТ) и представляет практическую ценность для всех специалистов, занимающихся вопросами ИБ.

Для совершенствования системы ИБ используют стандарт ITIL, в котором отражены оптимальные методы и принципы, определяющие интегрированный подход по управлению ИТ.

В России аудит ИБ осуществляют в соответствии с законом РФ от 5 марта 1992 г. №

2446-I «О безопасности», нормативными документами ФСТЭК России в области персональных данных и другими нормативными актами по обеспечению безопасности организации в экономической, социальной, информационной и других сферах предпринимательской деятельности.

ФСТЭК в своих документах регулирует проведение как внутреннего, так и внешнего контроля состояния ЗИ (аудита ИБ). Обладатель информации, оператор ИС обязан обеспечить постоянный контроль (аудит) за обеспечением уровня защищенности информации [2].

Методика аттестационных испытаний автоматизированных систем по требованиям ИБ определяет основы обязательного аудита ИБ [3]. Организации разрабатывают документы и стандарты, предназначенные для проведения аудита ИБ объекта информатизации.

Основные подходы к обеспечению ИБ организаций банковской системы (БС) РФ, сформулированы в стандарте Банка России СТО БР ИББС-1.0 [4], в котором определены основные понятия основ аудита ИБ: аудит ИБ, критерии оценки (аудита) ИБ, свидетельства оценки соответствия (аудита) ИБ установленным критериям, выводы аудита ИБ, аудиторское заключение, область аудита ИБ и программа аудита ИБ.

Основным видом проверки уровня ИБ в организациях БС РФ является аудит ИБ [5]. Мировой опыт в области обеспечения ИБ определяет аудит ИБ как важнейший процесс в непрерывном цикле процессов менеджмента ИБ организации.

Основными целями аудита ИБ организаций БС РФ являются:

– повышение доверия к организациям БС РФ;

– оценка соответствия ИБ организаций БС РФ критериям аудита ИБ [4].

Национальные стандарты и руководства по основам аудита ИБ отличается от Руководящих документов ФСТЭК России 1992–1998 годов, большей формализацией процесса обеспечения безопасности и более детальным комплексным учетом качественно и количественно проверяемых и управляемых показателей ИБ организации.

В национальном стандарте РФ ГОСТ Р ИСО 27001 [6] (прототип международного стандарта ISO 27001:2005) стандарт ГОСТ Р ИСО 19011 указан как полезное руководство для проведения внутренних аудитов СМИБ. Стандарт ГОСТ Р ИСО 19011 охватывает вопросы аудита систем менеджмента качества в организациях и экологии и не покрывает полностью аудит всей сферы деятельности организации, включая деятельность по обеспечению ИБ во всех деталях и подробностях.

ФСТЭК России и Госстандарт России совместно с другими министерствами и ведомствами приняли ряд национальных стандартов РФ, идентичных одноименным международным стандартам, в области ИБ и аудита ИБ:

1) Три национальных стандарта РФ ГОСТ Р ИСО/МЭК 15408 (части 1, 2, 3), определяющие критерии оценки безопасности ИТ, которые позволяют определить требования по формированию заданий по безопасности в соответствии с положениями международных стандартов.

2) Национальный стандарт РФ ГОСТ Р ИСО/МЭК 17799, устанавливающий рекомендации по управлению ИБ лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями.

3) Пять национальных стандартов РФ ГОСТ Р ИСО/МЭК 13335 (части 1, 2, 3, 4, 5), определяющих методы и средства обеспечения безопасности. Рассматривают такие вопросы как: концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий, менеджмент безопасности сети и методы менеджмента безопасности информационных технологий.

Действующие национальные стандарты и другие нормативные документы в области ИБ и аудита ИБ позволяют решать проблемы защиты информации в АС, информационных

системах, вычислительных и телекоммуникационных сетях, обеспечивать проведение аудитов ИБ: испытаний и сертификацию компонентов и средств ИТ на соответствие требованиям ИБ.

Анализ правовых основ аудита ИБ показывает, что стандарты рассматривают только отдельные вопросы в области ИБ. Выбор вида, способа проведения аудита ИБ всегда остается за организацией-заказчиком, которым в силу многообразия стандартов по аудиту ИБ (требований) сложно сделать выбор в пользу того или иного.

Для получения более полной и объективной оценки защищенности аудируемой организации и разработки эффективной программы построения системы обеспечения ИБ организации необходимо проводить комплексный аудит ИБ с рассмотрением требований (рекомендаций) нескольких стандартов. Данное решение способствует принятию эффективных и адекватных мер по обеспечению ИБ (защите от наиболее значимых угроз) и повышению уровня ИБ организации.

Список литературы

1. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография / В. А. Игнатьев. – Старый Оскол: ООО «ТНТ», 2005. – 448 с.
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
3. Положения по аттестации объектов информатизации по требованиям безопасности информации» (утв. Председателем Государственной технической комиссии при Президенте Российской Федерации «25» ноября 1994 г.
4. Стандарт Банка России СТО БР ИББС-1.0-2008. Общие положения. – Взамен СТО БР ИББС_1.0_2006. – М. : Банк России, 2008. – 38 с.
5. Стандарт Банка России СТО БР ИББС-1.1-2007. Аудит информационной безопасности. – М. : Банк России, 2007. – 14 с.
6. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М. : Стандартинформ, 2008. – 26 с.

МЕТОДОЛОГИЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лесковец О.С. – студент, Пивкин Е.Н. – к.т.н., ст. преподаватель

Белов В.М. – к.ф.-м.н., д.т.н., профессор

Алтайский государственный технический университет (г. Барнаул)

Возрастающая роль информационных технологий и возрастающая сложность информационных процессов и сетей связи требуют целостного взгляда на обеспечение информационной безопасности (ИБ), сформировать которую невозможно без получения информации о состоянии дел по защите информации (ЗИ) в организации. Аудит ИБ позволяет оценить текущую безопасность функционирования информационных систем (ИС) организации, оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы организации, корректно и обоснованно подойти к вопросу обеспечения безопасности ее информационных активов.

Под аудитом ИБ понимают независимую оценку текущего состояния системы ИБ, устанавливающую уровень ее соответствия определенным критериям (требованиям), отраженным в нормативных документах по ИБ: стандартах, руководящих документов и т.д.

Целью аудита ИБ является проверка и оценка соответствия ИБ организации

соответствующим требованиям.

Задачи аудита ИБ:

1. Повышение уровня ЗИ до необходимого поставленным целям.
2. Оптимизация и планирование затрат на обеспечение ИБ.
3. Обоснование инвестиций в системы защиты информации.
4. Получение максимальной отдачи от инвестиций, вкладываемых в системы ЗИ.
5. Подтверждение того, что используемые внутренние средства контроля соответствуют задачам организации и позволяют обеспечить эффективность и непрерывность работы организации.

При проведении аудита ИБ применяются прикладные исследования [1], представляющие собой познавательные работы, проводимые для реализации конкретной практической цели (определения уровня соответствия ИБ, предъявляемым требованиям в области ИБ). Прикладные исследования включают работы по внедрению полученных результатов, так для действующих систем это означает их совершенствование, а для вновь создаваемых – проектирование и внедрение.

Исследование, проводимое в ходе аудита, предусматривает изучение совокупности свойств элементов и подсистем ОИ в их взаимосвязи и взаимодействии между собой, с другими подсистемами и их элементами, а также с внешней средой, т.е. является системным.

В общем виде методология проведения аудита ИБ включает: методы (способы исследования), принципы (обобщенные правила, требования к выполнению каких-либо процессов, указывающих путь к истине) и критерии (стандарты, правила, регулирующие вопросы по ИБ) [2].

Как правило, исследования в ходе аудита проводятся с использованием эмпирических методов, которые основаны на использовании методов опытного исследования, позволяющие получить фактическую информацию об исследуемом объекте. Именно эмпирическая совокупность сведений дает первичную информацию о новых знаниях и многих свойствах исследуемых [2].

При проведении аудита ИБ экспертами используются следующие эмпирические методы исследования [2]:

– метод наблюдения – способ сбора информации, осуществляемого на основе регистрации и фиксации первичных данных об исследуемом объекте;

– метод опроса – способ сбора информации посредством устного взаимодействия с персонала, непосредственно взаимодействующего с исследуемым объектом;

– метод изучения первичной документации – основан на исследовании документированной информации, непосредственно зафиксированной ранее в организации;

– метод экспертной оценки – способ оценки, основанный на мнении экспертов;

– методы математической статистики – способы оценки, целью которых является получение достоверной информации о данных, собранных в результате исследования объекта;

– инструментальные методы сбора и обработки информации – способ определения фактических численных значений показателей свойств исследуемого объекта посредством соответствующих инструментальных средств (программ).

Методы наблюдения, опроса, изучения первичной документации и инструментальный метод необходимы на этапе сбора информации, метод экспертной оценки непосредственно используется экспертами при оценке уровня выполнения каждого требования, предъявляемого законодательством в области ИБ, метод математической статистики совместно с инструментальным методом необходимы для конечных расчетов, анализа выставленных экспертами оценок. Данные методы достаточно просты и понятны, что делает процедуры проведения аудита ИБ прозрачными.

Принципы исследования представляют собой основные правила (положения) применяемые при проведении аудита ИБ.

Проведение аудита ИБ основывается на ряде принципов, следование которым является предпосылкой для обеспечения объективных заключений по результатам аудита ИБ. Эти принципы должны быть признаны и соблюдены всеми сторонами, участвующими в аудите ИБ. Выполнение принципов способствует повышению безопасности организации.

Основные принципы аудита ИБ [3]:

– Независимость аудита ИБ. Аудит ИБ должен проводиться независимыми организациями или независимыми аудиторами. Независимость является основанием для беспристрастности при проведении аудита ИБ и объективности при формировании заключения по результатам аудита ИБ.

– Полнота аудита ИБ. Аудит ИБ должен охватывать все области ИБ и защитные меры, указанные в договоре на проведение аудита ИБ. Кроме того, полнота аудита ИБ определяется достаточностью предоставленных материалов, документов и уровнем их релевантности. Полнота аудита ИБ является необходимым условием для формирования объективных заключений по результатам аудита ИБ.

– Оценка на основе свидетельств аудита ИБ. Оценка на основе свидетельств является единственным способом, позволяющим получить повторяемое заключение по результатам аудита, что повышает к нему доверие. Для повторяемости заключения свидетельства аудита ИБ должны быть воспроизводимыми.

– Необходимость понимания аудитором деятельности проверяемой организации. При проведении аудита аудитор должен понимать деятельность проверяемой организации в достаточной степени, чтобы идентифицировать и правильно оценивать события, процессы, относящиеся к области ИБ, с учетом возможностей применения методов и способов оценки рисков, которые могут оказывать существенное влияние на достоверность проверяемых данных, на ход проведения проверки или на выводы, содержащиеся в аудиторском заключении. До проведения проверки аудиторская организация должна получить первоначальные знания особенностей отрасли, права собственности, управления и деятельности организации, подлежащей аудиту, и оценить их достаточность для проведения аудита.

– Компетентность и этичность. Доверие процессу аудита зависит от компетентности тех, кто проводит аудит, и от этичности их поведения. Компетентность базируется на личных качествах аудитора и способности применять знания и навыки. Этичность поведения подразумевает ответственность, неподкупность, умение хранить тайну, беспристрастность.

Под критериями аудита ИБ понимают совокупность политик ИБ, процедур или требований, установленных Федеральными стандартами и нормативами, с которыми сравнивается свидетельство аудита ИБ [4]. Свидетельство аудита ИБ определяют как записи, изложения фактов или другой информации, связанной с критериями аудита ИБ, которая может быть перепроверена. Любые свидетельства аудита, в том числе свидетельства, содержащие информацию об инцидентах ИБ, должны быть доступны для лиц выполняющих аудит ИБ.

При проведении аудита ИБ должны рассматриваться системы критериев, отраженные в нормативных документах, регулирующих вопросы обеспечения ИБ, например, при аттестации (руководящие документы ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»), декларировании (Положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное

приказом директора ФСТЭК России от 5 февраля 2010 г. №58) и сертификации (ГОСТ Р ИСО/МЭК 27001).

Определение полноты свидетельств аудита ИБ, признаваемой достаточной для оценки организации по необходимым критериям аудита, должно производиться с учетом целей и условий деятельности аудируемой организации, в том числе рисков, связанных с ее информационной сферой.

По результатам аудита готовится отчет о текущем состоянии ИБ обследуемой организации (объекте исследования), содержащий описание всех выявленных в ходе аудита технологических уязвимостей ИС, комплексную оценку системы управления ИБ и разработанные на основе полученных результатов развернутые рекомендации по повышению уровня защищенности ИС как за счет организационно-технических и административных мер, так и за счет применения специальных средств защиты информации и использования возможностей имеющихся программных и технических средств. Структура отчета может существенно различаться в зависимости от характера и целей проводимого аудита. В общем случае отчет содержит:

1) описание целей проведения аудита,
2) характеристику обследуемого ОИ,
3) указание границ проведения аудита
4) используемые методы,
5) результаты анализа данных аудита,
6) выводы, содержащие оценку уровня защищенности ОИ или соответствие ее требованиям стандартов,
7) рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.

Список литературы

1. Ярочкин В.И. Аудит безопасности фирмы: теория и практика: Учебное пособие для вузов / В.И. Ярочкин, Я.В. Бузанова. – М.: Академический проект. – 2005. – 352 с.
2. Мишин В.М. Исследования систем управления: Учебник для вузов / В.М. Мишин. – М.: ЮНИТИ-ДАНА, 2007. – 527 с.
3. Курило А.П. Аудит информационной безопасности / А.П. Курило, С.Л. Зефиров, В.Б. Голованов. – М.: БДЦ-Пресс, 2006. – 304 с.
4. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография / В.А. Игнатьев. – Старый Оскол: ООО «ТНТ», 2005. – 448 с.

ОСОЗНАНИЕ И МЕНЕДЖМЕНТ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лесковец О.С. – студент, Пивкин Е.Н. – к.т.н., ст. преподаватель

Белов В.М. – к.ф.-м.н., д.т.н., профессор

Алтайский государственный технический университет (г. Барнаул)

Обеспечение информационной безопасности (ИБ) включает реализацию и поддержку процессов осознания ИБ и процессов менеджмента ИБ. Стратегия обеспечения ИБ организации заключается в развертывании, эксплуатации и совершенствовании системы менеджмента ИБ организации, включающей процессы менеджмента ИБ и управляемой процессами осознания ИБ.

Осознание ИБ организации – это понимание организацией необходимости самостоятельно на основе принятых в ней ценностей и накопленных знаний формировать и учитывать в рамках основной деятельности прогноз результатов от деятельности адекватно прогнозу [1]. Осознание ИБ является позволяет инициировать и поддержать деятельность организации по менеджменту ИБ.

Для успешного осуществления политик ИБ и обеспечения работоспособности системы управления ИБ необходимо осознание ИБ всеми сотрудниками организации.

Система менеджмента информационной безопасности (СМИБ) является частью общей системы менеджмента организации и предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения уровня ИБ с учетом всех рисков организации. Современная СМИБ представляет собой процессно-ориентированную систему управления, включающую организационный, документальный и программно-аппаратный компоненты. Согласно спецификации международного стандарта ISO/IES 27001 [2] процессы СМИБ организации функционируют в соответствии с циклической моделью «Планирование – осуществление – проверка – совершенствование».

СМИБ нуждаются в дополнительной координации и управлении со стороны руководства организации, эффективность СМИБ во многом зависит от соблюдения и выполнения правил политик ИБ сотрудниками организации.

К процессам осознания ИБ организации относят [1]:

- Анализ проблем ИБ и определение потребности организации в обеспечении ИБ.
- Поддержку деятельности по планированию СМИБ.
- Поддержку деятельности по реализации и эксплуатации СМИБ.
- Поддержку деятельности по проверке СМИБ.
- Поддержку деятельности по совершенствованию СМИБ.

Процессы проверки СМИБ организации позволяют проверить и оценить результаты процессов планирования СМИБ, а также процессов реализации и эксплуатации СМИБ. Кроме того, результаты процессов проверки СМИБ являются входными данными для процессов совершенствования СМИБ.

Внедрение СМИБ подразумевает разработку и внедрение процедуры, направленной на систематическую идентификацию, анализ и снижение рисков ИБ.

Для снижения рисков ИБ, полученных в результате аудита ИБ, в организации внедряют следующие процессы [3]:

- управление внутренней организацией ИБ;
- обеспечение ИБ при взаимодействии с третьими сторонами;
- управление реестром информационных активов и правил их классификации;
- управление безопасностью оборудования;
- обеспечение физической безопасности;
- обеспечение ИБ персонала;
- обеспечение безопасности сети и т.д.

Под аудитом ИБ организации понимается систематический, независимый и документированный процесс получения свидетельств аудита ИБ и объективного их оценивания с целью установления степени соответствия ИБ организации установленным критериям аудита ИБ [4].

Осознание необходимости аудита ИБ формируется в результате анализа проблем ИБ организации и дальнейшего определения потребностей организации в оценке соответствия политик, процессов, процедур обеспечения ИБ организации установленным критериям ИБ. Основные элементы процесса осознания аудита ИБ представлены на рисунке 1.

Рисунок 1. – основные элементы процесса осознания аудита ИБ

Участниками процесса осознания ИБ являются руководители организации, принимающие решения и влияющие на решения по поддержке и развитию СМИБ организации.

Потребность в разработке и менеджменте программы аудита ИБ организации формируется исходя из аудита ИБ. Цели аудита определяются руководством организации на основе результатов деятельности организации, информации о внутренней и внешней среде организации, учитывающей риски ИБ. В качестве целей выделяют идентификацию уязвимостей системы обеспечения ИБ организации, оценку соответствия ИБ организации установленным критериям (требованиям) ИБ, повышение доверия к организации. При формировании решений о программе аудита ИБ анализируются стоимость программы и выгоды от ее реализации. Потребность в разработке и менеджменте программы аудита ИБ документирует и утверждает руководство.

Требования к программе аудита содержат требования к объему программы, методологии проведения аудита, компетентности аудиторов, осведомленности сотрудников организации о программе аудита ИБ и требования к пересмотру и корректировке программы аудита ИБ.

Осознание аудита ИБ приводит к реализации в организации программы аудита ИБ и обеспечивает плановое проведение аудита ИБ и самооценки ИБ в организации.

Список литературы

1. Курило А.П. Аудит информационной безопасности / А. П. Курило, С. Л. Зефиров, В. Б. Голованов. – М.: БДЦ-Пресс, 2006. – 304 с.
2. Астахов А. «Аудит безопасности информационных систем» [электронный ресурс - 2002] http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/audit-bezopasnosti-informacionnyh-sistem/
3. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А.Петренко, С.В.Симонов. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.
4. Ярочкин В.И. Аудит безопасности фирмы: теория и практика: Учебное пособие для вузов / В. И. Ярочкин, Я. В. Бузанова. – М.: Академический проект. – 2005. – 352 с.

РАЗРАБОТКА МЕТОДИКИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лесковец О.С. – студент, Пивкин Е.Н. – к.т.н., ст. преподаватель
Белов В.М. – к.ф.-м.н., д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Анализ и определение уровня защищенности объекта информатизации (ОИ) необходимы для своевременного выявления, оценки и прогнозирования источников и характера внутренних и внешних угроз информационной безопасности (ИБ), причин и условий, способствующих нанесению ущерба интересам субъектов информационных отношений, разработки и принятия мер оперативного реагирования на угрозы ИБ, проектирования и создания эффективной системы защиты.

Аудиторские организации, участвующие в проведении аудита ИБ, для каждого ОИ разрабатывают и согласовывают с организацией методику проведения аудита. Анализ источников литературы в области стандартизации подходов ИБ [1 – 4] показывает наличие небольшого количества методик проведения аудита ИБ.

Поэтому была предпринята попытка разработки методики, которую возможно использовать для проведения комплексного аудита ИБ организаций в части определения текущего уровня защищенности.

В разработанной методике для проведения аудита ИБ ОИ организаций рассматриваются требования ИБ, предъявляемые при проведении аттестации ОИ по требованиям безопасности информации (БИ), декларирования соответствия требованиям БИ информационных систем персональных данных (ИСПДн) и сертификации информационной системы (ИС) по стандарту ISO 27001. В качестве ОИ рассматривается автоматизированная система (АС).

Методику могут использовать организации любой формы собственности, как оказывающие услуги в области ИБ (аудит ИБ, аттестация ОИ, декларирование ИСПДн и т.п.), так и непосредственно внутренним подразделениям по ИБ организации, которые проводят данные мероприятия самостоятельно. При этом подразумевается, что в организации не обрабатывают сведения, составляющие государственную тайну, а только конфиденциальную информацию, включая персональные данные.

Методика устанавливает порядок проведения оценки уровня защищенности и методы оценивания выполнения требований по ИБ, которые изложенные в следующих нормативно-правовых актах и стандартах в области ИБ:

1. Руководящие документы ФСТЭК России по ИБ [5,6].
2. Документы ФСЭК России в области персональных данных [7].
3. Стандарт ISO/IEC 27001:2005 [4].

Метод оценки текущего уровня защищенности заключается в определении соответствия выполнения требованиям, предъявляемым при:

– аттестации ОИ по требованиям БИ;

– сертификации (аттестация) по требованиям БИ, либо декларирования соответствия требованиям БИ ИСПДн;

– сертификации ИС по стандарту ISO 27001.

Для оценки текущего уровня защищенности используется шкала степени их выполнения:

– «нет» – оценке присваивается значение нулю;

– «частично» – оценке присваивается значение 0,5;

– «да» – оценке присваивается значение, равное единице;

– «требование не применимо» – требование не оценивается и отмечается отметкой «н/о».

Результатом методики, наряду с определением соответствия текущего уровня защищенности ОИ набору предъявляемых требований, является выработка рекомендаций, направленных на повышение текущего уровня защищенности ОИ до требуемого.

Для оценки степени соответствия текущего уровня защищенности ОИ требованиям, предъявляемым при проведении мероприятий по ИБ (аттестация, декларирование, сертификация) используются показатели защищенности, которые разделены на три группы:

1 группа – показатели (требования), необходимые для проведения аттестации ОИ по требованиям БИ;

2 группа – показатели (требования), достаточные для сертификации (аттестация) ИСПДн по требованиям БИ, либо декларирования соответствия требованиям БИ ИСПДн;

3 группа – показатели (требования), достаточные для сертификация ИС по стандарту ISO 27001.

Оценка показателя формируется на основании степени выполнения требований, которая определяется посредством экспертного оценивания, т.е. анализа аудиторской группой свидетельств аудита.

В качестве основных источников свидетельств аудита используются:

– внутренние нормативные документы по ИБ проверяемой организации;

– устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;

– результаты наблюдений членов аудиторской группы за деятельностью сотрудников проверяемой организации в области ИБ.

В процессе проведения устного опроса сотрудников проверяемой организации и наблюдений за деятельностью указанных сотрудников аудиторская группа должна сделать вывод о степени соответствия оцениваемой деятельности требованиям внутренних нормативных документов проверяемой организации.

Оценивание показателя должно сопровождаться внесением символа, например «✓», в соответствующую графу разработанных форм (рисунок 1). При заполнении форм учитываются условия обработки защищаемой информации в АС (1 – однопользовательский режим обработки, = – многопользовательский с равными правами, ≠ – многопользовательский с разными правами).

№ п/п	Требования (мероприятия)	Степень выполнения				Вид	Персональные данные									Аттестация АС		Сертификация
							3 класс			2 класс			1 класс			3Б, 2Б, 1Д	1Г	ИСО 27001
		н/о	0	0,5	1		1	=	≠	1	=	≠	1	=	≠			
1.	**Подсистема 1**																	
	Требование 1					Т												
	Требование 2					О												
	Требование 3					Д												
	…																	

Рисунок 1 – Заполняемая форма при проведении аудита ИБ

В методике используется несколько типов показателей:

1. Показатели, в которых оценивается только степень документированности.

2. Показатели, в которых оценивается как степень документированности, так и степень выполнения требований.

3. Показатели, в которых оценивается только степень выполнения.

Текущий уровень защищенности представлен следующими уровнями:

– технический уровень защищенности (Т);

– документированный уровень защищенности (Д);

– организационный уровень защищенности (О).

Для получения оценки текущего уровня защищенности ОИ определяют степень выполнения требований по ИБ, предъявляемых при проведении аттестации, декларирования или сертификации, по техническому, документированному и организационному уровням защищенности соответственно.

Всего в методике учитывается более 140 требований по ИБ. Текущий уровень защищенности организации высчитывается по формуле:

$$R_j = \frac{\sum k_i}{t_j - x_j}, \text{ где}$$

R_j – текущий уровень защищенности организации по выбранному направлению (аттестация, декларирование или сертификация), $R = [0, 1]$;

k_i – коэффициент выполнения требования i для выбранного направления j аудита ИБ;

t_j – количество оцениваемых параметров (требований) для выбранного направления j;

x_j – количество неприменимых параметров (требований) для выбранного направления j.

В зависимости от полученного значения текущего уровня защищенности объекта ОИ делается вывод о возможности проведения мероприятий в организации:

– аттестации ОИ по требованиям БИ;

– сертификации (аттестация) по требованиям БИ, либо декларирования соответствия требованиям БИ ИСПДн;

– сертификации ИС по стандарту ISO 27001.

Представленная методика проведения аудита ИБ позволяет комплексно подойти к решению задачи определения текущего уровня защищенности ОИ организации при отсутствии необходимости обучения персонала организации перед ее применением.

Список литературы

1. Курило А.П. Аудит информационной безопасности / А. П. Курило, С. Л. Зефиров, В. Б. Голованов. – М.: БДЦ-Пресс, 2006. – 304 с.
2. Мишин В.М. Исследования систем управления: Учебник для вузов / В. М. Мишин. – М.: ЮНИТИ-ДАНА, 2007. – 527 с.
3. Ярочкин В.И. Аудит безопасности фирмы: теория и практика: Учебное пособие для вузов / В. И. Ярочкин, Я. В. Бузанова. – М.: Академический проект. – 2005. – 352 с.
4. ISO/IEC 27001:2005 – Информационная технология – Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности – Требования.
5. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.).
6. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.).
7. Положение о методах и способах защиты информации в информационных системах персональных данных (утв. приказом Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 58).

ОСОБЕННОСТИ СХЕМОТЕХНИКИ И РЕАЛИЗАЦИЯ ВИРТУАЛИЗИРОВАННЫХ ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ

Лященко Д.Н. – аспирант, Новоженов А.В. – аспирант
*Дмитриев С.Ф. – к.т.н., докторант, Ишков А.В. – к.х.н., д.т.н., профессор
Алтайский государственный аграрный университет (г. Барнаул)
*Алтайский государственный университет (г. Барнаул)

Классический подход к реализации любого измерительного прибора базируется на нескольких положениях, связанных с общими подходами к измерениям, их средствам, объектам измерения и их моделям, а также метрологическом эксперименте [1]. Во-первых, необходимо определиться с самой измеряемой характеристикой или сигналом, поступающим от объекта измерения, так, чтобы используемый для измерений сигнал обладал максимальной информативностью об интересующем наблюдателя объекте. Во-вторых, выбирается сам метод измерения (сравнения исследуемого сигнала с эталоном или шкалой), который в общем виде может быть абсолютным, прямым, относительным или косвенным. Далее выбирается само средство измерений - техническое устройство, имеющее нормированные метрологические показатели и реализующее выбранный ранее метод, и первичный преобразователь - устройство, перерабатывающее полученную от объекта измерительную информацию в форму, удобную для дальнейшего преобразования, передачи, хранения и обработки, но недоступную для непосредственного восприятия оператором. Причем, если в результате такого преобразования физическая природа измеряемого параметра не изменяется, а соотношение между входным и выходным сигналом измерительного преобразователя задается линейной функцией, то преобразователь часто называют усилителем, во всех других случаях в измерительном приборе используют устройства, изменяющие физическую природу измеряемой величины - электромеханические, магнитноэлектрические, пневмоэлектрические и др. преобразователи.

Затем преобразованный или усиленный измерительный сигнал поступает в основной узел прибора - измерительный преобразователь, осуществляющий процесс определения параметров сигнала, их сравнение с эталонами и шкалами и передачу сигнала далее - устройствам визуализации или устройствам управления (если в приборе кроме измерительных, реализованы еще и функции управления). Иногда этот узел называют также передающим преобразователем, что указывает на его непосредственную связь с оператором, проводящим измерение. Узел измерения прибора, как правило, является основным во всей его блок-схеме и определяет важные метрологические характеристики устройства - точность, чувствительность, воспроизводимость измерений.

В некоторых источниках [2], учитывая обстоятельство постоянного преобразования измерительного сигнала по мере его прохождения от объекта измерений через измерительный прибор к оператору (или приемнику), все его блоки функционально относят к преобразователям (первичным, промежуточным, передающим и пр.), которых в любом приборе оказывается как минимум четыре (рис. 1).

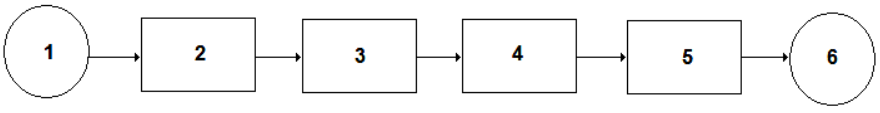

Рис. 1. Блок-схема измерительного прибора прямого действия:
1 - объект измерения, 2 - чувствительный элемент, 3 - первичный преобразователь, 4 - измерительный преобразователь, 5 - передающий преобразователь, 6 - оператор.

Вся описанная выше функциональная схема измерительного прибора может быть реализована как в аналоговом, так и в цифровом варианте и может работать под управлением оператора или автоматически.

Из сказанного выше понятно, что практически любой измерительный прибор содержит в себе специализированную архитектуру преобразовательных блоков с определенными характеристиками, создается под конкретные измерительные задачи и модели объектов измерения и не может быть универсальным средством измерения. При смене объекта измерения, изменении природы и характера первичной измерительной информации необходимо каждый раз перенастраивать блочную архитектуру прибора, оптимизировать осуществляемые им измерительные преобразования или создавать новый прибор с приемлемыми метрологическими характеристиками.

Это относится как к простым механическим устройствам, используемым для технических измерений, так и к современным измерительным установкам или системам для проведения сложных и точных измерений различных физических и физико-химических величин или количественного исследования реальных процессов.

При сопряжении такого измерительного прибора с ЭВМ, последняя, как правило, используется для вторичной обработки окончательно преобразованного сигнала, либо как мощное средство визуализации измерений. Зачастую в ЭВМ переносят и задачи исследования различных моделей объекта измерения, и проведение и поддержку метрологического эксперимента. И если опустить два первых методических положения, то основными узлами современного измерительного прибора, даже если он и сопряжен с ЭВМ, все равно являются считывающее устройство или чувствительный элемент, первичный преобразователь или усилитель, и измерительный преобразователь, связанный с персональным компьютером посредством АЦП/ЦАП (рис. 2).

Несложно заметить, что при таком подходе даже современный компьютеризированный измерительный комплекс сохраняет все недостатки обычного измерительного устройства, так как содержит в себе всю его блочно-преобразовательную архитектуру.

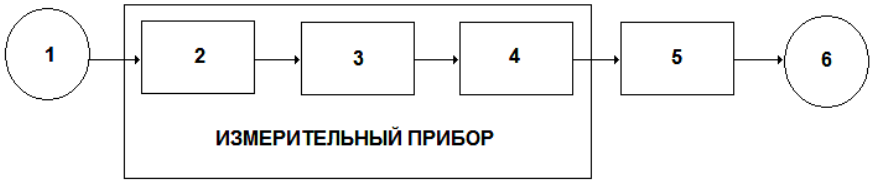

Рис. 2. Классическая схема сопряжения измерительного прибора с ЭВМ:
1 - объект измерения, 2 - первичный датчик-преобразователь, 3 - измерительный преобразователь, 4 - АЦП/ЦАП, 5 - ЭВМ, 6 - оператор.

Классический вариант сопряжения измерительного прибора с ЭВМ (рис. 2) *a priori* связывает все возможности такой измерительной системы, ее чувствительность, точность и другие метрологические характеристики, объем измерительной информации, получаемой от объекта и возможности ее преобразования со схемотехникой измерительного прибора, закладывающейся в его конструкцию. В этой схеме ограничены также и возможности обратной связи в системе и если у оператора возникает необходимость в увеличении чувствительности, точности измерений, изменении вида и параметров приборной (преобразовательной) функции или получении новых данных об объекте, то ему фактически приходится создавать новый измерительный прибор.

В то же время возможности современной вычислительной техники и периферийных устройств ЭВМ, несущих в своем составе многоканальные и высокоскоростные АЦП/ЦАП, позволяют совсем иначе реализовать схему сопряжения ЭВМ с измерительным прибором.

Высокая скорость и оптимальная маршрутизация обработки вычислительных данных современными многоядерными процессорами, а также большие объемы ОЗУ, предоставляемые операционными системами пользователю, уже сейчас позволяют реализовывать такие измерительные устройства, в которых все операции по оцифровке, усилению, измерительному преобразованию и визуализации измерительной информации можно реализовать «виртуально» (подобно тому, как виртуально реализуются симуляции

различных процессов и устройств в средах разработки LabView, MathCad и MatLab), используя возможности ПК, а в качестве внешнего «реального» устройства, получающего информацию от объекта измерений в составе такой системы, будет применяться только один блок архитектуры измерительного прибора - первичный датчик-преобразователь, подключаемый к ЭВМ через стандартные устройства ввода-вывода, например звуковой адаптер, LPT-, COM- или USB-порт, в зависимости от вида его выходного измерительного сигнала.

Фактически, если в классической схеме сопряжения измерительного прибора с ЭВМ, и прибор и ПК представляли собой отдельные системы, то в предлагаемой и реализуемой нами *концепции - это единая измерительная система, интегрированная в составе специализированного программно-аппаратного комплекса и решающая универсальные задачи по получению, преобразованию и визуализации измерительной информации, выбору и оптимизации модели объекта измерения, осуществляющая проведение всех стадий метрологического эксперимента, включая статистическую обработку результатов измерений и их представлению оператору в удобной для восприятия форме*.

Подобные схемы уже сейчас реализуются, например в упомянутой выше среде разработки специализированного программного обеспечения (ПО) LabView [3], либо приемами раздельной программной обработки data-файлов, содержащих измерительную информацию или параметры различных объектов стандартными средствами Windows. Однако, необходимость постоянного обращения к оболочке среды разработки (как в случае виртуальной лаборатории LabView), или «ручного» копирования и обработки файлов с данными (при втором подходе), снижают скорость измерений, увеличивают систематическую и случайную погрешность измерений и сильно ограничивают возможности обработки измерительных сигналов встроенным в среды ПО. Кроме того, специализированное ПО, разработанное в таких средах, представляет собой макеты (виртуальные приборы), неспособные самостоятельно запускаться на ПК при отсутствии на них предварительно установленной среды, что существенно ограничивает области применения таких измерительных приборов, увеличивает их стоимость и ставит в зависимость от лицензируемого программного обеспечения (ПО), их разработчиков, различных ключей и обновлений, ограничивающих работу тех или иных подпрограмм и функций, реализованных в этих средах.

Оригинальная концепция измерительных приборов, называемых по аналогии с виртуальными приборами, созданными в различных средах разработки - *виртуализированными измерительными приборами*, основана на реализации главных приборных измерительных и преобразовательных функций в одной специализированной, самоисполняемой компьютерной программе, не требующей установки на ПК дополнительных (кроме операционной) сред и связи ее с первичным датчиком-преобразователем, посредством имеющихся в ЭВМ АЦП/ЦАП [4]. На основе этой концепции, используя возможности встроенной звуковой карты ПК как многоразрядного и высокоскоростного АЦП/ЦАП и разъемов звукового адаптера как доступного канала ввода-вывода измерительной информации, нами разработаны несколько серий виртуализированных измерительных приборов, реализующих метод вихревых токов и используемых в образовании и научных исследованиях.

Список литературы

1. Марков Н.Н., Ганевский Г.М. Конструкция, расчет и эксплуатация измерительных инструментов и приборов. -М.: Машиностроение, 1981.
2. Димов Ю.В. Метрология, стандартизация и сертификация. -СПб.: Питер, 2008.
3. Жарков Ф.П., Каратаев В.В., Никофоров В.Ф., и др. Использование виртуальных инструментов LabView. -М.: Радио и связь, 1999.
4. Ишков А.В., Дмитриев С.Ф. Современная концепция сопряжения измерительных приборов с ЭВМ. // Измерение, контроль, информатизация: Материалы восьмой междунар. научн.-техн. конф. -Барнаул: Изд-во АлтГТУ, 2007. С. 3-6.

ПРИМЕНЕНИЕ CASE-ТЕХНОЛОГИЙ ДЛЯ АНАЛИЗА ВОПРОСОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мастевная О.А. – студент, Пивкин Е.Н. – к.т.н., ст. преподаватель
Белов В.М. – к.ф.-м.н., д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Современная технология освоения и внедрения CASE-средств базируется в основном на стандартах-рекомендациях IEEE (IEEE Std 1348-1995. IEEE Recommended Practice for the Adoption of CASE Tools и IEEE Std 1209-1992. IEEE Recommended Practice for the Evaluation and Selection of CASE Tools) [1].

Case-средства предоставляют возможность: облегчить разработку моделей, провести анализ деятельности предприятий, проследить: входные потоки, выходные данные и информационные потоки, циркулирующие внутри организации. Таким образом, формируется целостная картина информационной безопасности предприятия [2].

Современный рынок программных средств насчитывает около 300 различных CASE-средств.

CASE-средства могут быть классифицированы по типам и категориям:

– Классификация по типам отражает функциональную ориентацию CASE-средств на те или иные процессы.

– Классификация по категориям определяет степень интегрированности по выполняемым функциям.

Помимо этого, CASE-средства классифицируют по следующим признакам: применяемым методологиям, моделям систем баз данных, доступным платформам.

Российский рынок программного обеспечения располагает следующими наиболее развитыми CASE-средствами: Vantage Team Builder (Westmount I-CASE); Designer/2000; Silverrun; ERwin+BPwin; S-Designor; CASE.Аналитик; Rational Rose [3].

В качестве средства позволяющего строить диаграммы бизнес-процессов выбрано Case-средство BPwin. С его помощью строят модели, отображающие деятельность предприятия, входящие и исходящие сообщения и ресурсы, необходимые для их функционирования. Технология описания процессов обеспечивает прозрачность всех операций деятельности, позволяет выявлять возможные угрозы, влияющие на информационную систему предприятия, проанализировать последствия их реализации и своевременно выбрать меры по противодействию.

BPwin поддерживает три стандартные нотации – IDEF0 (функциональное моделирование), DFD (моделирование потоков данных) и IDEF3 (моделирование потоков работ), позволяющие описывать предметную область комплексно, что позволяет выявить слабые места в политике информационной безопасности предприятия.

В рамках информационной безопасности, предлагается использовать:

– нотацию IDEF0 для построения организационной структуры предприятия;

– нотацию IDEF3 для углубленного изучения угроз информационной безопасности;

– нотацию DFD для моделирования информационных потоков предприятия.

Основной целью проектирования структуры организации является построение ее модели или в соответствии с современной концепцией управления изменениями – процессной модели организации.

По методике IDEF0 описание системы (модели) организовано в виде иерархически упорядоченных и взаимосвязанных диаграмм. Вершина этой древовидной структуры – самое общее описание системы и ее взаимодействия с внешней средой, а в ее основании находятся наиболее детализированные описания выполняемых системой функций. Модели построенные по данной методике, позволяют провести оценку состояния информационной безопасности «как есть» и спланировать наиболее эффективную организацию «как будет», а так же рассчитать затраты, связанные с проектированием или совершенствованием информационной безопасности предприятия [4]. Признаком малоэффективной деятельности

могут быть бесполезные, неуправляемые и дублирующиеся работы, отсутствие обратных связей по управлению.

К очевидным преимуществам такого рода моделирования относят наглядность получаемых моделей и возможность типизации объектов и связей между ними, что особенно важно для принятия решений задач обеспечения безопасности.

Основные задачи, решаемые на данном этапе:

– объективная оценка текущего состояния информационной безопасности предприятия;

– проверка адекватности и эффективности политики безопасности предприятия;

– расчет необходимых затрат на совершенствование корпоративной системы защиты информации и повышение уровня информационной безопасности компании;

– анализ функциональной деятельности структурных подразделений предприятия и их взаимодействие.

Для моделирования угроз информационной безопасности применяют нотации: IDEF0 и IDEF3.

IDEF0 лучше всего применять как средство анализа и логического моделирования систем – ранние стадии работы над проектом. Данные анализа, полученные с использованием моделирования IDEF0, обычно используют на стадии разработки моделей IDEF3 и диаграмм потоков данных DFD.

Методология IDEF3 – методология моделирования, предназначенная для обеспечения структурированного подхода к описанию бизнес-процесса как упорядоченной последовательности событий одновременно с описанием любых участвующих в бизнес-процессе объектов и относящихся к ним правил. Под правилами в рамках информационной безопасности предприятия, рассматривается перечень угроз.

Использование CASE-средств анализа позволяет наглядно и эффективно представлять компоненты информационной инфраструктуры организации, выделять наиболее критичные из них [5]. Такая визуализация угроз влияющих на информационную безопасность компании позволяет оперативно генерировать различные варианты защиты, сравнивать их между собой с точки зрения экономической эффективности и в результате выбирать оптимальный вариант построения или модификации защиты корпоративной системы

Основные задачи, решаемые на данном этапе:

– детализация функциональной деятельности структурных подразделений предприятия;

– определения момента окончания моделирования;

– сбора информации о схеме работы моделируемого отдела предприятия;

– визуализации угроз, действующих на систему информационной безопасности.

Диаграммы IDEF3 обеспечивают дискретность моделирования процесса, что может использоваться для контроля за ходом выполнения работ.

Моделирование информационных потоков.

В соответствии с методологией (методологии Gane/Sarson) модель системы определяется как иерархия диаграмм потоков данных (DFD), описывающих асинхронный процесс преобразования информации от ее ввода в систему до выдачи пользователю. Диаграммы верхних уровней иерархии определяют основные процессы или подсистемы информационной системы с внешними входами и выходами. Они детализируются при помощи диаграмм нижнего уровня. Такая декомпозиция продолжается, создавая многоуровневую иерархию диаграмм, до тех пор, пока не будет достигнут такой уровень декомпозиции, на котором процесс становятся элементарными и детализировать их далее невозможно [6].

Источники информации (внешние сущности) порождают информационные потоки (потоки данных), переносящие информацию к подсистемам или процессам. Те в свою очередь преобразуют информацию и порождают новые потоки, которые переносят информацию к другим процессам или подсистемам, накопителям данных или внешним сущностям – потребителям информации. Поток данных определяет информацию, передаваемую через некоторое соединение от источника к приемнику. Реальный поток данных может быть информацией, передаваемой по кабелю между двумя устройствами,

пересылаемыми по почте письмами, магнитными лентами или дискетами, переносимыми с одного компьютера на другой и т.д.

Основные задачи, решаемые на данном этапе:

– анализ внутреннего документооборота структурных подразделений;

– определение информационных потоков между основными процессами деятельности;

– оценка объемов и интенсивности информационных потоков.

Таким образом, рассмотренное Case-средство, сочетает в себе нотации, позволяющие: проанализировать деятельность предприятия, объективно оценить состояние информационной безопасности предприятия, посчитать затраты необходимые для совершенствования корпоративной системы защиты информации, выявить угрозы действующие на информационную безопасность предприятия, проанализировать документооборот и отследить информационные потоки конфиденциальной информации.

Список литературы

1. Официальный сайт IEEE Standards Association [электронный ресурс]. – http://standards.ieee.org/catalog/olis/arch_se.html
2. Современные методы и средства проектирования информационных систем [электронный ресурс]. – http://www.codenet.ru/db/other/case/index.php
3. Сравнительный анализ Case-средств [электронный ресурс]. – http://www.itlab.unn.ru/file.php?id=112
4. Информационная логистика [электронный ресурс]. – http://ru.wikipedia.org/wiki/Информационная_логистика
5. Все о системном проектировании [электронный ресурс]. – www.idefinfo.ru
6. Кузнецов И.Н. Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе. М.: ООО Изд. Яуза, 2001.

ЗАЩИТА КОРПОРАТИВНОЙ IP-ТЕЛЕФОНИИ

Озеров И.М. – студент, Шарлаев Е.В. – к.т.н., доцент

Алтайский государственный технический университет (г.Барнаул)

IP-телефония это система связи, которая обеспечивает передачу речевого сигнала по IP-сетям в цифровом виде. Сигнал, как правило, перед передачей преобразовывается (сжимается) с тем, чтобы удалить избыточность.

IP-телефония опирается на две основных операции: преобразование двунаправленной аналоговой речи в цифровую форму внутри кодирующего/декодирующего устройства (кодека) и упаковку в пакеты для передачи по IP-сети [1].

В традиционной телефонии голос имеет гарантированную фиксированную задержку при передаче и гарантированную полосу пропускания для каждого звонка. В сети передачи данных для передачи голоса требуется низкая задержка, минимальные джиттеры и потери пакетов.

Для обеспечения стабильной телефонной связи по IP-сетям введены специальные протоколы передачи данных, например, H.323 и SIP. Краткие характеристики приведены в таблице 1 [2].

Таблица 1 – Характеристики протоколов SIP и H.323

Параметр сравнения	SIP	H.323
Дополнительные услуги	Набор услуг, поддерживаемых обоими протоколами примерно одинаков	
Персональная мобильность пользователей	Имеется хороший набор средств поддержки мобильности	Персональная мобильность поддерживается, но менее гибко
Расширяемость протокола	Удобная расширяемость, простая совместимость с предыдущими версиями	Расширяемость поддерживается, но существует ряд сложностей
Масштабируемость сети	Оба протокола обеспечивают хорошую масштабируемость сети	
Время установления соединения	Достаточно одной транзакции	Требуется несколько транзакций.
Сложность протокола	Простой, мало запросов, текстовый формат сообщений	Сложный, много запросов и протоколов, двоичное представление сообщений

Возможные угрозы IP – телефонии:

1. Прослушивание разговоров. Речь пользователя, полученная с телефонного аппарата, преобразовывается в цифровой вид с помощью какого-либо специального кодека. Затем эти данные упаковываются внутрь сетевых пакетов и отправляются получателю, аппаратура которого проводит все обратные действия, извлекая звук. Таким образом, злоумышленнику, который хочет прослушать ведущийся разговор, достаточно перехватить сетевые пакеты и декодировать полученную информацию в звуковой вид.

2. Подмена номера. В IP-телефонии номером служит обычный IP-адрес. Существуют возможности подменить его, присвоив своему компьютеру. С этого момента злоумышленник получает телефонные звонки, предназначенные пользователю.

3. Атаки на конечных абонентов. Если пользователь ведет разговоры при помощи компьютера, то его ПК фактически во время разговора подключен к КСПД, а значит, подвержен всем опасностям сети.

4. Атаки на узлы системы IP-телефонии. Система IP-телефонии - это достаточно сложный программно-аппаратный комплекс, состоящий из нескольких компьютеров и различного ПО. И практически на все узлы могут быть организованы различные удаленные атаки.

5. Атаки на отказ в обслуживание. Главная опасность атаки на отказ в обслуживании заключается в простоте ее реализации. Последствия такой атаки могу представлять собой от появлении во время разговора постороннего шума, искажении речи собеседника и пропаже некоторых его слов или фраз до полного выведения системы из строя [3].

В таблице 2 представлены сводные данные о возможных мерах защиты от угроз, представленных ранее.

Таблица 2 - Применимость мер защиты IP-телефонии

Атаки / Меры	Подслушива-ние	Подмена номера	Атаки на абонентов	Атаки на узлы	Отказ в обслуживание
Деление на сегменты	+/-	+/-	+	+/-	+/-
Фильтрация и контроль доступа	+	+	+	+	+
Защита от подмены	-	+	+	-	-
Защита от нарушения работоспособности	-	-	+	+	+
Криптографические меры	+	+	-	-	-
Организационные меры	+	+/-	+/-	+/-	+/-

\+ непосредственно используется для защиты от этой угрозы;
+/- частично применимо;
\- малая применимость для защиты от данной угрозы.

Меры защиты и их реализации:

1. Деление сети на сегменты. Главное, что необходимо сделать при построении инфраструктуры IP-телефонии, - отделить ее от сегментов, в которых передаются обычные данные (файлы, электронная почта и т.д.). Это можно сделать как с помощью технологии виртуальных локальных сетей (VLAN), так и с помощью межсетевых экранов (МЭ).

2. Фильтрация и контроль доступа. Голосовые шлюзы, подключенные к ТфОП, должны отвергать все протоколы IP-телефонии (H.323, SIP и другие), приходящие из сегмента данных корпоративной сети. Помимо встроенных в компоненты IP-телефонии механизмов фильтрации и контроля доступа существуют и специальные решения, защищающие элементы голосовой инфраструктуры от возможных несанкционированных воздействий. К таким решениям относятся межсетевые экраны (МЭ), шлюзы прикладного уровня и специализированные пограничные контроллеры.

Другая проблема, решение которой необходимо продумать до приобретения межсетевого экрана, - трансляция сетевых адресов (Network Address Translation, NAT). При установке вызова используются динамические порты, указанные в запросе на установление соединения между абонентами, эта технология скрытия топологии сети путем трансляции адресов делает телефонные переговоры невозможными. Решением проблемы является использование специальных прикладных шлюзов, выпускаемых в виде выделенных устройств или интегрированных в межсетевые экраны, "понимающие" протоколы с динамическими портами (например, SIP или RTCP).

3. Защита от подмены. В сети необходимо использовать различные стандартизированные протоколы, включая 802.1x, RADIUS, сертификаты PKI X.509 и т.д. И, конечно, нельзя сбрасывать со счетов уже упомянутые выше правила контроля доступа на маршрутизаторах и МЭ, усложняющие злоумышленникам задачу подключения к голосовым сегментам.

4. Защита от нарушения работоспособности. Несмотря на то что различные компоненты IP-телефонии потенциально подвержены атакам "отказ в обслуживании", существует целый ряд защитных мер, предотвращающих как сами DoS-атаки, так и их последствия [3].

5. Шифрование - наиболее эффективный способ сохранить телефонные переговоры в тайне, однако в результате этого возникают нежелательные задержки. В случае применения потокового шифрования задержка гораздо ниже, чем при использовании блочных шифров, но полностью от нее избавиться не удастся. Эта проблема решается путем использования более быстрых алгоритмов или включения механизмов QoS.

При шифровании возникают накладные расходы, связанные с увеличением длины передаваемых пакетов. Для протокола IPSec размер добавляемого заголовка составляет около 40 байт, что достаточно много для 50-70-байтовых пакетов IP-телефонии. А пока оптимальным решением обеих проблем является протокол SecureRTP [4].

6. Еще одна проблема безопасности IP-телефонии в недооценке существующих рисков и в непонимании новых технологий. Например, во многих организациях и компаниях существует классификатор конфиденциальной информации, обрабатываемой в автоматизированной системе. Но только в немногих организациях классифицируются еще и голосовые данные, передаваемые в рамках инфраструктуры IP-телефонии. А между тем информация, не включенная в такой классификатор, находится вне зоны внимания службы информационной безопасности и оказывается не защищенной.

Увеличение числа сетей IP-телефонии приведет к росту угроз для их существования и бесперебойного функционирования. Следовательно, обеспокоиться защитой внедряемой или уже внедренной инфраструктуры IP-телефонии необходимо с этапа планирования системы. Существуют технологии, значительно повышающие защищенность VoIP, более того, эти технологии зачастую уже внедрены в компоненты, применяемые в построении среды передачи голоса. А значит, надо просто воспользоваться ими.

Список литературы

1. Зырянов С. От корпоративной IP-телефонии к унифицированным коммуникациям [Электронный ресурс]/ С. Зырянов. — Режим доступа: http://www.connect.ru/article.asp?id=8400.
2. Гольдштейн Б.С. Протокол SIP. Справочник /Б.С. Гольдштейн. — СПб.: BHV-Санкт-Петербург, 2005, 456 с.
3. Лукацкий А. Практические аспекты защиты корпоративной сети IP-телефонии [Электронный ресурс] / А. Лукацкий. — Режим доступа: http://www.comkas.ru/tech/ip0206.html.
4. Рябко Б.Я. Криптографические методы защиты информации. Учебное пособие / Б.Я. Рябко, А.Н. Фионов А. – М.: Горячая Линия – Телеком. - 2005, 232 с.

ОЦЕНИВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МОДЕЛИ ЗРЕЛОСТИ ПРОЦЕССОВ

Пойманов К.И. – студент, Архипова А.Б. – аспирант

Алтайский государственный технический университет (г. Барнаул)

В настоящее время многие организации все большую роль уделяют вопросам информационной безопасности (далее ИБ). При оценивании ИБ очень важно определить, на каком уровне зрелости процессов обеспечения ИБ предприятие находится на данный момент, чтобы в дальнейшем принимать решения о необходимости внедрения средств обеспечения ИБ, принятия организационных, инженерно-технических, правовых и других мер по защите информации.

Большинство моделей зрелости процессов обеспечения ИБ в настоящее время основывается на универсальной модели зрелости процессов, определенной стандартом Cobit [1], которая определяет шесть уровней зрелости организации - с нулевого по пятый. На его основе, например, основаны такие стандарты, как стандарт банка России [2], стандарт бюджетной системы Российской Федерации [3].

Для оценки уровня зрелости конкретного процесса в организации предлагается способ оценки «от начального к максимальному», заключающийся в поглощении требований предыдущего уровня зрелости последующим. Например, процесс соответствует второму уровню зрелости только в случае, если выполняют все требования для первого уровня.

Оценка производится по следующим параметрам [4]:

- область действия системы менеджмента информационной безопасности;
- описание реализации процесса;
- гарантии на уровне бизнеса;
- информация о среде;
- идентификация задействованных активов;
- влияние процесса на достижение целей бизнеса;
- угрозы, уязвимости.

Для анализа должны быть предоставлены:

- документальные свидетельства выполнения анализа рисков информационной безопасности на основе идентификации информационных активов и их уязвимости и анализа угроз данным активам;
- документальные свидетельства выполнения оценки потенциальных потерь (ущерба) бизнесу организации в результате воздействия (возможной реализации) угроз информационной безопасности;

• документальные свидетельства выбора варианта минимизации (обработки) рисков применительно ко всем рискам, оцененным после выполнения процесса;

• документальные свидетельства снижения количества потенциальных инцидентов, вызванных рисками и выявленных постфактум;

• документальные свидетельства увеличения количества выявленных рисков, влияние которых было ослаблено.

В соответствии с критериями оценки организация относится к одному из шести, предусмотренных стандартом, уровней.

Нулевой уровень. На данном уровне наблюдается полное отсутствие определенного процесса по анализу и оценке рисков информационной безопасности.

Не проводится оценка рисков информационной безопасности для проектов, разрабатываемых стратегий и решений. Руководство организации не осознает возможных последствий для бизнеса организации, связанных с реализациями угроз информационной безопасности, в спектре рисков организации не рассматриваются риски информационной безопасности.

Ценность информационных активов с точки зрения сохранения свойств целостности, конфиденциальности и доступности не рассматривается как ключевая в целях бизнеса. Не ведется база инцидентов информационной безопасности, они не предупреждаются, не рассматриваются и не анализируются.

Первый уровень (“начальный”). В организации существуют документально зафиксированные свидетельства осознания руководством существования проблем обеспечения информационной безопасности. В частности, определена и документально зафиксирована область действия системы менеджмента информационной безопасности.

Информационные активы определены, составлен перечень их уязвимостей и вероятностей использования уязвимостей угрозами. Просчитан ущерб от возможной реализации угроз, а также определены оценки актуальности угроз.

Процесс анализа и оценки рисков как таковой нестандартизирован. Деятельности в рамках процесса оценки и анализа рисков применяются эпизодически и бессистемно. Так, например, определены риски раскрытия, модификации значимых информационных активов, но выбор метода идентификации рисков оставлен на усмотрение ответственного лица. Создана, но не обновляется база инцидентов информационной безопасности. Определены приоритеты рисков, но данные приоритеты учитывают не все инциденты информационной безопасности.

Второй уровень (“повторяемый”). Проведена первичная оценка рисков. Оценка рисков носит неформальный характер, не включена в план обязательных мероприятий по обеспечению информационной безопасности. Ответственность персонала за проведение мероприятий по оценке и анализу рисков документально не зафиксирована. Существуют документально зафиксированные свидетельства возможности переноса рисков на третьи стороны, но не предложены конкретные программы и стратегии переноса, не определены ответственности исполнителей.

Определены критерии принятия рисков информационной безопасности, но они не обновляются и не подвергаются всестороннему анализу, выбор критериев возложен на отдельное ответственное лицо, требования к квалификации которого также не определены. Обсуждения по вопросам снижения рисков носят ситуационный характер, бессистемны и непериодичны, отсутствует системный подход к оценке рисков.

Третий уровень (“определенный”). Существует политика организации, в которой определяется периодичность и область оценки рисков информационной безопасности. Процесс оценки рисков документирован и стандартизирован, суть процесса доводится до заинтересованного персонала посредством обучения базовым принципам безопасности, оценки и анализа рисков информационной безопасности.

Разработан план работ по оценке рисков. Методология оценки рисков с большой степенью вероятности гарантирует, что основные риски информационной безопасности

будут выявлены, поскольку результаты деятельности в рамках процесса по оценке и анализу рисков согласованы с соответствующими политиками, стандартами и (или) процедурами. Однако выбор метода сбора информации об инцидентах, угрозах и уязвимостях, а также способа оценки рисков оставлен на усмотрение ответственного персонала (реализация не скоординирована). В связи с данным фактом вероятность отклонения от стандартных процедур по оценке остается достаточно высокой.

Мероприятия по минимизации рисков не всегда оптимальны и своевременны, однако являются отражением действующей в организации практики обеспечения информационной безопасности.

Четвертый уровень (“управляемый”). Характеризует то, что обеспечиваются мониторинг и оценка соответствия используемых в организации процессов. При выявлении низкой эффективности реализуемых процессов менеджмента ИБ обеспечивается их оптимизация. Процессы менеджмента ИБ находятся в стадии непрерывного совершенствования и основываются на хорошей практике. Средства автоматизации менеджмента ИБ используются частично и в ограниченном объеме.

Разработана стратегия переноса рисков на сторонние организации.

Сотрудники обеспечены соответствующими средствами для выполнения полномочий в рамках должностных обязанностей по оценке рисков.

Пятый уровень (“оптимизированный”). Оценка рисков в организации доведена до уровня лучших практик по оценке и анализу риска. Выбранная стратегия оценки рисков непрерывно совершенствуется, ориентируясь на последние достижения в области информационной безопасности, принимаемые международные стандарты и результаты сравнения с уровнем других организаций. Привлекаются сторонние сертифицированные специалисты для консультаций по вопросам рисков, оптимизации существующей системы сбора и анализа первичной информации для анализа рисков. В рамках внутриорганизационной структуры используются совещания по принципу «мозгового штурма» с целью выявить и проанализировать причины идентифицированных рисков. Система защитных мер строго скоординирована с приоритетами рисков и зависимостью «эффективность защитных мер — стоимость», комплексно используется установленная форма отчетности об эффективности защитных мер.

Процедуры сбора, анализа, хранения, сопровождения и передачи информации для баз данных по угрозам, уязвимостям и инцидентам информационной безопасности преимущественно автоматизированы и формализованы. Установлены ответственности персонала за неинформирование об имевшем место инциденте информационной безопасности, а также за нарушение процедуры информирования заинтересованных лиц.

Руководители, а также рядовой персонал организации регулярно обучаются лучшим практикам информационной безопасности, до их сведения доводятся новейшие рекомендованные требования информационной безопасности с последующей проверкой знаний.

В компании, находящейся на самом высоком уровне развития, все процессы представляют собой единый интегрированный комплекс, обеспечивающий эффективное управление и обработку информации на всех этапах ее работы.

Модели зрелости не подсказывают как улучшить работу компании и не объясняют, как работать с персоналом, также нет готовых руководств и по применению моделей зрелости. Рекомендуется каждой конкретной компании разработать подобное руководство для своего бизнеса или пригласить сторонних консультантов для решения этого вопроса. Модели зрелости предназначены для организации эффективного управления ИБ. Они определяют ключевые действия, которые указывают, что надо сделать для достижения требуемого качества и содержат способы контроля над правильностью выполнения ключевых процессов ИБ и методы их корректировки.

Таким образом, при оценивании состояния информационной безопасности на предприятии первоочередной задачей должно стоять определение уровня зрелости

предприятия, сравнение этого уровня с требованиями мировых стандартов для предприятий в этой области и принятие решений о необходимости проведения каких-либо мероприятий для повышения уровня зрелости организации в области ИБ.

Список литературы

1. Стандарт CobiT. Управление и аудит информационных технологий. Особенности проведения внешнего аудита ИТ. //http://citforum.univ.kiev.ua/consulting/standart_cobit/article1.1.2003130.html#AEN188
2. СТО БР ИББС_1.0_2006 «Стандарт банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
3. Модель зрелости процессов менеджмента информационной безопасности организации БС РФ //http://www.budgetrf.ru/Publications/Magazines/VestnikCBR/2006/vestnikcbr20060203/vestnikcbr20060203200.htm
4. Информационная безопасность. Модель зрелости аудита безопасности информации //http://inform-bez.ru/?cat=55

К ВОПРОСУ О БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ И ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

Просветова Д.В. – студент, Пивкин Е.Н. – к.т.н, ст. преподаватель

Алтайский государственный технический университет (г. Барнаул)

Наиболее распространенными и надежными методами аутентификации и идентификации личности считаются криптографические протоколы аутентификации и комбинированные методы идентификации (требуют знание пароля и наличия специального устройства, подтверждающего подлинность субъекта). В качестве недостатков, данных методов выделяют: сложность реализации процедур безопасного хранения криптографических и личных ключей.

Методы биометрической аутентификации личности [5] решают проблему утери паролей и личных ключей. Примерами реализации данных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и т.д.

Выделяют следующий перечень проблем которые решают с использованием биометрической аутентификации и идентификации [1]:

– предотвращение проникновения злоумышленников на охраняемые территории и в помещения за счет подделки, кражи документов, карт, паролей;

– ограничение доступа к информации и обеспечение персональной ответственности за ее сохранность;

– обеспечение допуска к ответственным объектам только сертифицированных специалистов;

– избежание накладных расходов, связанных с эксплуатацией систем контроля доступа (карты, ключи);

– исключение неудобств, связанных с утерей, порчей или элементарным забыванием ключей, карт, паролей;

– организация учета доступа и посещаемости сотрудников.

Применение биометрических характеристик связано с затруднениями в реализации из-за сложности применяемых методов. Поэтому используют такие алгоритмы, которые не приводят к ошибкам системы. Этапы применения биометрической технологии [1]:

– сканирование объекта;

– извлечение индивидуальной информации;

– формирование шаблона;

– сравнение текущего шаблона с базой данных.

Выделяют следующие общие принципы биометрического распознавания человека [5]:

– преобразование исходного изображения в начальное представление (может включать в себя как предобработку, так и математические преобразования, например вычисление главных компонент);

– выделение ключевых характеристик (например, берётся первые *n* главных компонент или коэффициентов дискретного косинусного преобразования);

– механизм классификации (моделирования): кластерная модель, метрика, нейронная сеть и т.п.

Рассмотрим некоторые методы распознавания [4]:

Метод главных компонентов (Principal Component Analysis, PCA) применяется для сжатия информации без существенных потерь информативности. Процесс распознавания заключается в сравнении главных компонент неизвестного изображения с компонентами всех остальных изображений. Для этого обычно применяют какую-либо метрику (простейший случай – Евклидово расстояние). Дальнейшее совершенствование заключается в использовании метрики Махаланобиса и Гауссовского распределения для оценки близости изображений.

Линейный дискриминантный анализ (Linear Discriminant Analysis, LDA), выбирает проекцию пространства изображений на пространство признаков таким образом, чтобы минимизировать внутриклассовое и максимизировать межклассовое расстояние в пространстве признаков. Но данный метод имеет ряд невыясненных вопросов и ставит под сомнение эффективность своего использования.

Основной недостаток этих методов – высокие требования к условиям съёмки изображений. Изображения должны быть получены в близких условиях освещённости, одинаковом ракурсе и должна быть проведена качественная предварительная обработка, приводящая изображения к стандартным условиям (масштаб, поворот, центрирование, выравнивание яркости, отсечение фона).

Генетические методы являются наиболее ярким представителем эволюционных методов и представляет собой мощнейшее поисковое средство, имеющее важное значение при решении различных проблем.

Нейросетевые методы [2-3] предлагают инструменты для построения сложных разделяющих поверхностей. Они лишены распространенных недостатков и считаются наиболее эффективными. Их применение основано на самообучении, обучении без учителя, которое применяется для решения задач распознавания образов, оптимизации, управления, сжатия данных. Искусственные нейронные сети применяются в различных методах распознавания, таких как:

– гибкие контурные модели лица;

– сравнение эластичных графов;

– оптический поток.

Искусственные нейронные сети широко используются при решении самых различных задач и активно применяются в тех ситуациях, где обычные алгоритмические решения оказываются неэффективными или вовсе невозможными. Для информационной безопасности нейронные сети представляют большой интерес, как с теоретической, так и с

практической точки зрения. Наиболее интересными являются вопросы идентификации и аутентификации, задачи детектирования деятельности злоумышленника, а так же выявления различных аномалий в работе пользователя. Но использование нейронных сетей применяется не только для распознавания лица, а так, же и в других областях биометрической аутентификации.

Приведенные методы иллюстрируют неотъемлемые принципы создания систем, которые приведут к переходу на качественно новый уровень развития искусственной информации и безопасности в целом.

Список литературы

1. Татарченко Н.В., Тимошенко С.В. Биометрическая идентификация в интегрированных системах безопасности. – «Специальная Техника» №2, – 2002.
2. Борисов Е.С. Основные модели и методы теории искусственных нейронных сетей – 2005.
3. Уоссермен Ф. «Нейрокомпьтерная техника. Теория и практика» Перевод на русский язык, Ю.А. Зуев, В.А. Точенов, – 1992.
4. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. / В.В. Борисов, В.В. Круглов, А.С. Федулов. – М.: Горячая линия – Телеком, 2007. – 284 с.: ил.
5. Иванов А.И., Сапегин Л.Н., Щигунова Е.А. Контроль качества учебного материала нейросети и систем биометрической идентификации личности. /А.И.Иванов, Л.Н.Сапегин, Е.А. Щигунова //Автометрия. №4. – 2000. – с. 32-40.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АВТОМАТИЗИРОВАННОГО РАСЧЕТА ВЕЛИЧИН СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ

Соболь Д.Б. – студент, Загинайлов Ю.Н. – к.в.н., профессор

Алтайский государственный технический университет (г. Барнаул)

На сегодняшний день проблема технической защиты конфиденциальной информации является особенно актуальной в связи с тем, что значительное количество организаций решают проблему по защите персональных данных. Эта проблема обусловлена необходимостью реализации положений Федерального закона № 152 «О персональных данных», обязывающего привести в соответствие с требованиями безопасности информационные системы персональных данных (ИСПДн) [1]. Особую значимость при этом имеет вопрос определения необходимых мер по технической защите ИСПДн.

Наш век высоких технологий позволяет злоумышленнику использовать специальные технические средства для перехвата информации по техническим каналам. Так же совершенствуются средства технической защиты информации. Но как определить есть ли необходимость устанавливать средство технической защиты информации? Перекрывает ли средство технической защиты информации канал утечки информации?

Утечка конфиденциальной информации по техническим каналам осуществляются:

- за счет наводок на вспомогательные технические средства и системы и их коммуникации;
- по каналам электроакустических преобразований;
- по акустическому и виброакустическому каналам;
- за счет утечки конфиденциальной информации при передачи по линиям связи.

В настоящее время для проверки достигнутого уровня защищенности объекта информатизации проводят специальные исследования. Специальные исследования проводятся лицензиатами Федеральной службы по техническому и экспортному контролю (ФСТЭК России), имеющими специальную лабораторию. При проведении специальных исследований специальными средствами измерения получают замеры, которые необходимы для определения уровня защищенности объекта информатизации, определяемого на основе методик приведенных в нормативных документах ФСТЭК по защите конфиденциальной информации.

Полученные результаты могут сказать о состоянии защиты по тому или иному техническому каналу. Расчет величин полученных в результате специальных исследований производится вручную, при этом возникают следующие проблемы:

– затрата временных ресурсов на расчет величин специальных исследований и на проверку вычислений;

– ошибки или неточности при расчете величин и составлении протокола.

Разработанный программный продукт предназначен в помощь специалисту отдела аттестации, в автоматизации процесса вычисления величин специальных исследований и составлении протоколов специальных исследований.

Входными данными служат величины, полученные в результате специальных исследований. Данные в программный продукт поступают посредством загрузки файлов с замерами специальных исследований, а также могут быть введены с клавиатуры.

Выходными данными являются результаты вычислений величин специальных исследований. Программный продукт позволяет экспортировать результаты в формате html и OpenOffice.

На рисунке 1 представлена форма для расчета максимального расстояния, на которое распространяется информативный сигнал от объекта исследования.

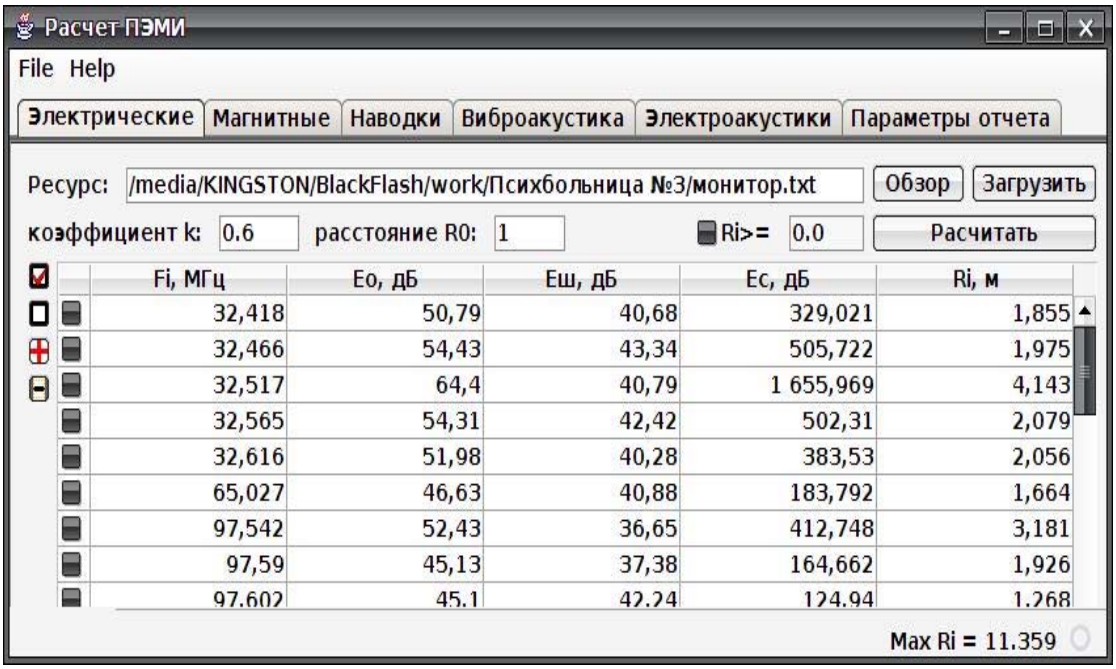

Рисунок 1 – Форма расчета расстояния ПЭМИН

Форма заполнения реквизитов объекта исследований приведена на рисунке 2.

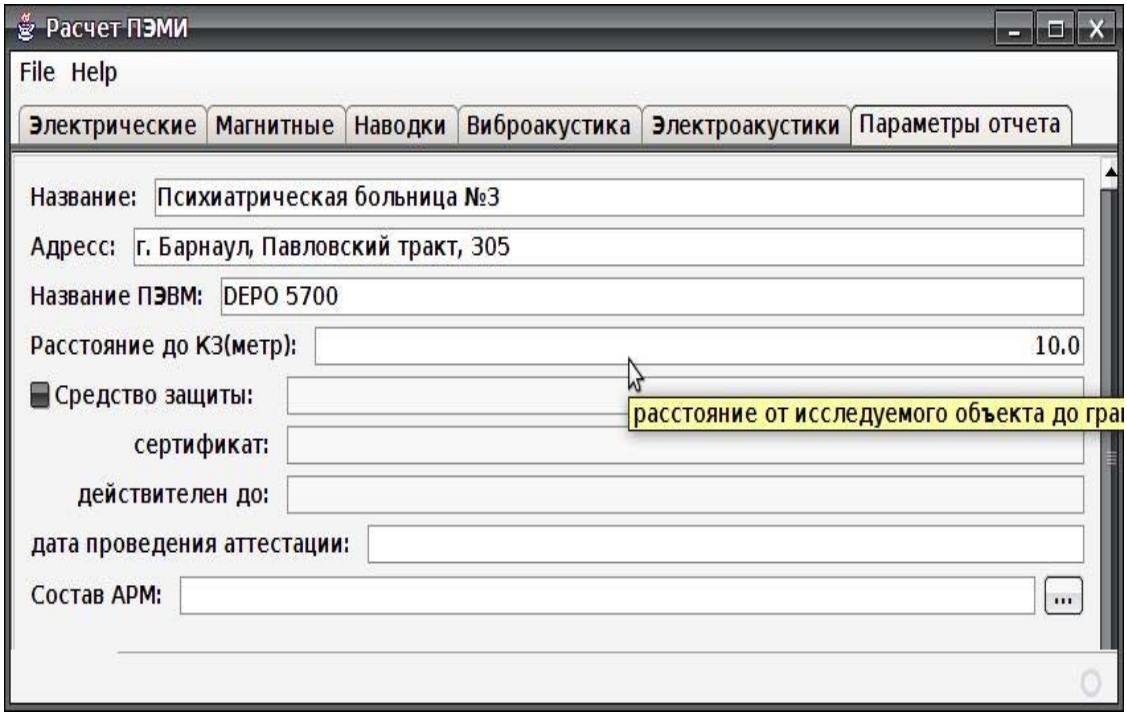

Рисунок 2 – Форма заполнения реквизитов организации

Для программного продукта разработано руководство пользователя, позволяющее в короткие сроки полностью освоить работу с программным продуктом.

Система написана и реализована для IBM – совместимых компьютеров с операционными системами Windows 2000/XP/Vista, ОС Linux, требует наличия виртуальной машины Java.

Программный продукт разработан на межплатформенном языке Java [2]. В визуальной среде программирования NetBeans IDE 6.7 и поэтому все новые изменения, исправления, а так же добавление расчета новых параметров может быть произведено за короткий период времени.

Программный продукт обладает удобным графическим интерфейсом, который обеспечивает наиболее удобную работу с ним. Для каждого пункта меню в программе имеется вспомогательная информация. Программный продукт имеет интерактивный графический интерфейс и защиту ввода от ошибок пользователя, что обеспечивает высокую отказоустойчивость системы.

Для обеспечения конфиденциальности специальных исследований предусмотрена подсистема безопасности, отвечающая требованиям руководящих документов ФСТЭК России.

Использование программного продукта позволяет существенно сэкономить время специалиста по защите информации анализа результатов специальных исследований и повысить эффективность работы ООО “Центр Информационной Безопасности”, в котором планируется его применение.

Список литературы

1. Федеральный закон № 152 «О персональных данных». [электронный ресурс]. - http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html
2. П. Ноутон, Г. Шилдт «Java2. Наиболее полное руководство», Вильямс, 2005г.

ИНФОРМАЦИОННАЯ СИСТЕМА ПОДДЕРЖКИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО СПЕЦИАЛЬНОСТИ КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Урминский Е.В. – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Тенденции развития системы непрерывного образования в глобальном плане свидетельствуют, что в будущем в учебных планах количество часов, выделяемых на самостоятельную работу, будет только увеличиваться в связи с дальнейшей качественной компьютеризацией системы образования, с развитием дистанционного обучения, с использованием Интернета, созданием электронных учебников и учебных пособий, которые позволят создать оптимальную образовательную среду в вузах и вне вузов, в домашних условиях для качественного выполнения всех запланированных образовательными программами вузов или самими обучающимися видов самостоятельной работы [1].

В ходе учебного процесса студент пользуется профильной литературой, методическими и лабораторными пособиями. Если специальность широкого профиля, то областей знания может оказаться достаточно много, а при проведении научно-исследовательской работы в любом случае возникнет необходимость оперирования терминами из двух и более областей знания, именно к таким специальностям относится специальность «Комплексная защита объектов информатизации» (КЗОИ).

Для решения вопросов информационного обеспечения потребностей студента разработана «Информационная система поддержки самостоятельной работы студента» (ИСПСРС), которая является средством для решения следующих задач:

- методическое обеспечение учебной деятельности студента;
- справочное обеспечение учебной деятельности по специальности КЗОИ;
- навигация по учебным ресурсам специальности.

Концептуальная модель ИСПСРС представлена на рисунке 1. Все модули системы автономны.

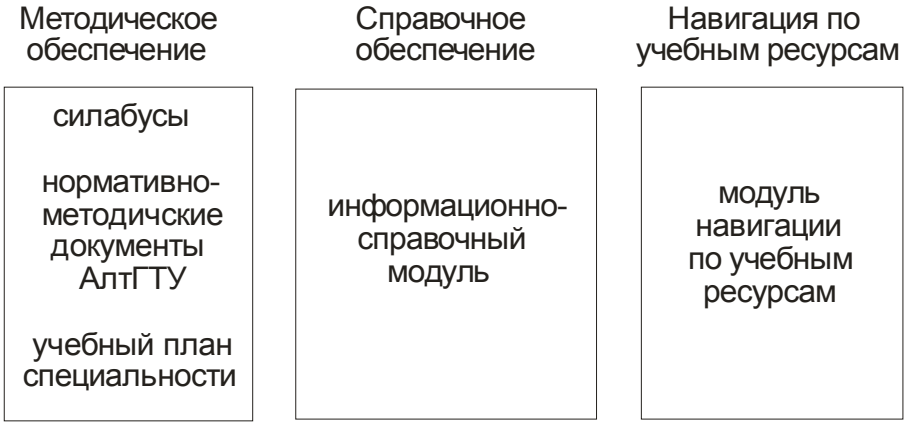

Рисунок 1 – концептуальная модель ИСПСРС по специальности КЗОИ

Модуль «Методическое обеспечение учебной деятельности» предназначен для использования студентами электронных ресурсов в части образовательной деятельности. Документы по образовательной деятельности включают в себя: силабусы, учебный план специальности и другую документацию регламентирующую образовательный процесс.

Модуль «Навигации по учебным ресурсам» - предоставляет возможности оперативного поиска нужной литературы по запросу. Литература хранится в виде профилей, структура которых основана на стандарте XML. Оглавление книги представляется в модуле навигации

как профиль, который создаётся посредством встроенного редактора, знание английского языка в котором (названия тегов) минимальны. Программа хорошо документирована и требует не более 10 минут ознакомления. С учетом динамичного развития специальности, модуль содержит функции администрирования, которые позволят развивать базу в дальнейшем в зависимости от требований образовательного процесса и контролировать изменения в ней. В функции администрирования входят: регистрация событий, менеджер профилей, функция архивирования базы и управления справочником. Элементы интерфейса модуля представлены на рисунке 2.

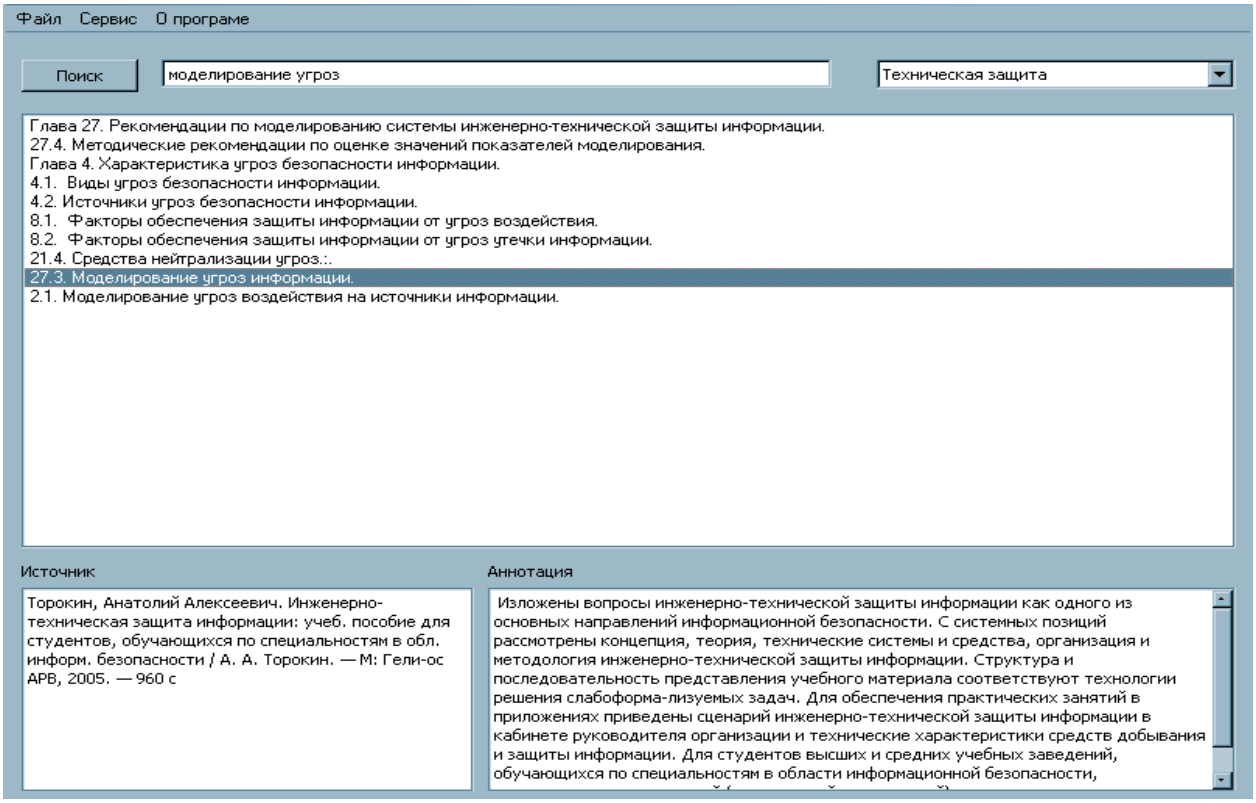

Рисунок 2 – элементы интерфейса модуля навигации по учебным ресурсам

Справочное обеспечение по специальности реализовано в виде информационно-справочного модуля и содержит понятийный аппарат из национальных стандартов, федеральных законов и других нормативных документов в области информационной безопасности.

Чтобы отразить важность модуля нужно рассмотреть многообразие образовательного процесса по специальности КЗОИ. В качестве примера рассмотрим термин «информационная безопасность», который упоминается в дисциплинах специализации и общего профессионального цикла. В дисциплинах «Правовое обеспечение информационной безопасности» и «Безопасность вычислительных сетей» термин трактуется не одинаково. В первом курсе рассматривается правовой аспект, а во втором аспект политики безопасности принятой на предприятии. Если обратиться к стандартам, то окажется, что рассматриваемый термин в них изложен по разному:

- все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки (ГОСТ Р ИСО/МЭК 13335-1-2006);
- обеспечение доступа к информации только авторизованным пользователям (ГОСТ Р ИСО/МЭК 17799-2005);

– свойство информации сохранять конфиденциальность, целостность и доступность (ГОСТ Р ИСО/МЭК 27001-2006).

В курсе «Безопасность вычислительных сетей» с термином «информационная безопасность» связано следующее определение:

Информационная безопасность — это система, позволяющая выявлять уязвимые места организации, опасности, угрожающие ей, и справляться с ними.

Если исходить из термина предложенного в дисциплине то из контекста следует использование сетевого экрана, системы отражения атак и подсистемы аудита и регистрации событий. Не ясно, на сколько эти меры поддержания необходимого уровня информационной безопасности обеспечат уровень защищённости. Кроме этого в одной из этих подсистем может быть допущена ошибка при администрировании и в итоге система окажется уязвимой.

Пример показывает, что понятие должно описывать состояние защищённости некоторой системы, а не набор абстрактных политик, которые реализуют организационные или технические мероприятия.

Анализ образовательных ресурсов и сайтов связанных с информационной безопасностью в сети Интернет показал, что полноценных словарей по информационной безопасности, состоящих из стандартов и законодательства в этой предметной области в открытом доступе (и в виде платной услуги) нет.

Доступность для студента справочного материала достигнута за счет разработки одного из компонентов ИСПСРС – информационно справочного модуля. Элементы интерфейса модуля приводятся на рисунке 3.

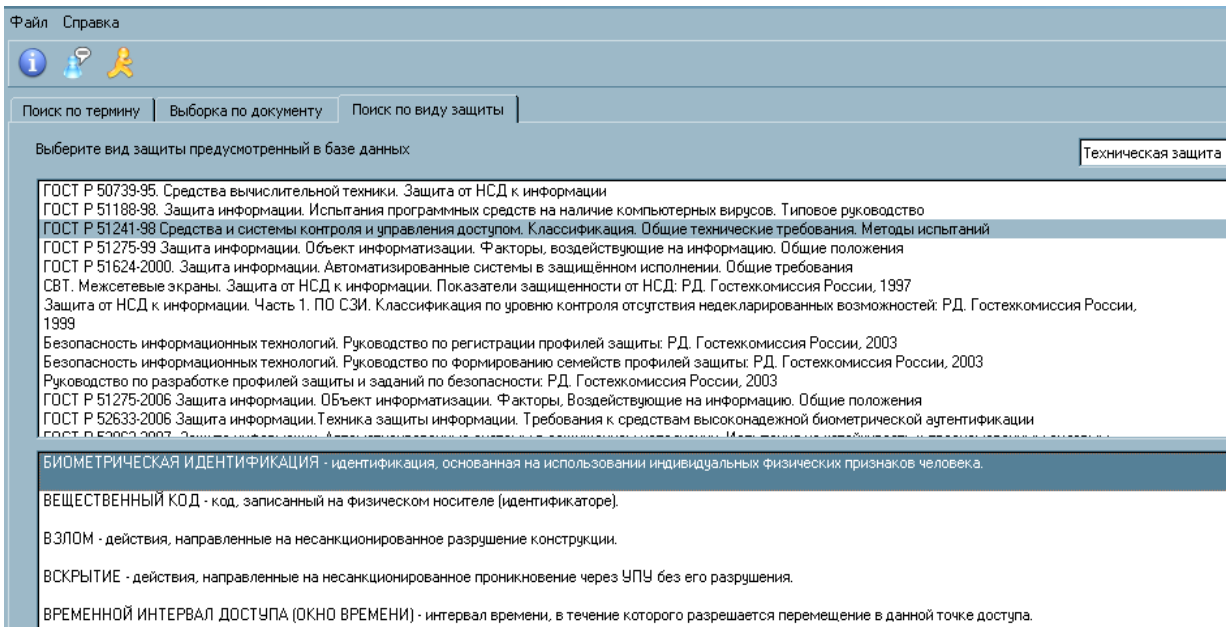

Рисунок 3 – элементы интерфейса информационно-справочного модуля

Информационно-справочный модуль позволяет выполнять выборки из базы по виду защиты согласно [2], виду документа и термину.

ИСПСРС планируется внедряться в 2010-2011 году.

Список литературы

1. Морозова Н.А. Роль информационно-технологической компетентности в продуктивности самостоятельной работы современного студента. [электронный ресурс – 09.04.2010г.]. - http://www.pedlib.ru/Books/3/0269/3_0269-41.shtml
2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2006. - 12с.

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

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

Совершенствование систем менеджмента информационной безопасности организации привело к тому, что в ней выделена самостоятельная часть — менеджмент инцидентов информационной безопасности. Для этого международным сообществом в области стандартизации и информационных технологий подготовлено и издано в форме специального стандарта руководство по менеджменту инцидентов информационной безопасности. В России этот стандарт принят в качестве национального[1].

Не смотря на то, что в этом стандарте указаны основные процедуры и этапы управления инцидентами информационной безопасности организации, вопросы решения задач а также нормативного регулирования и методического обеспечения рассмотрены поверхностно, что обуславливает необходимость разработки дополнительных практических и методических рекомендаций специалистам, разрабатывающим и внедряющим системы менеджмента информационной безопасности.

Для обеспечения максимальной эффективности системы обеспечения информационной безопасности организации необходимо иметь структурированный, хорошо продуманный метод управления инцидентами информационной безопасности. Такой метод должен предусматривать:

– обнаружение и обработка событий информационной безопасности;

– оценка инцидентов и их разрешение на информационной безопасности более эффективным способом;

– снижение до минимума отрицательного воздействия инцидентов на организацию соответствующими защитными мерами, являющимися частью процесса реагирования на инцидент;

возможность быстрого извлечения уроков из инцидента информационной безопасности для повышения шансов предотвращения подобных инцидентов в будущем.[1]

Недостаточная подготовка организации к обработке инцидентов информационной безопасности делает практическую реакцию на инциденты малоэффективной, и это увеличивает риск отрицательного воздействия на бизнес.

С учётом рассмотренных проблемных вопросов разработаны практические рекомендации по управлению инцидентами информационной безопасности, которые содержат:

− классификацию инцидентов информационной безопасности и их характерные признаки;

− рекомендации и методы по обнаружению и обработке инцидентов информационной безопасности;

− рекомендации по принятию мер, предотвращающих повторение инцидентов и извлечению уроков из инцидентов;

− рекомендации по документированию процесса управления инцидентами информационной безопасности (инструкции, отчёты, журналы);

В основу рекомендаций взяты положения ГОСТ Р ИСО/МЭК 18044 «Менеджмент инцидентов информационной безопасности» и ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

Система менеджмента инцидентов информационной безопасности является частью политики безопасности организации. Ключевые вопросы обеспечения эффективного управления изложены в [2].

Наиболее проблемными вопросами в системе управления инцидентами

информационной безопасности, требующими дополнений, разъяснений и примеров, являются: оповещение, ответственность и процедуры, извлечение уроков из инцидентов информационной безопасности, сбор доказательств.

Рассматривая вопрос оповещения, следует добавить, что лицо, непосредственно обратившее внимание на нечто необычное или оповещенное автоматическими средствами, несет ответственность за инициирование процесса обнаружения и оповещения. Этим лицом может быть любой представитель персонала организации, работающий постоянно или по контракту. Этот представитель должен следовать процедурам и использовать форму отчета о событиях информационной безопасности, определенную системой менеджмента инцидентов информационной безопасности, с целью привлечения внимания, прежде всего, группы обеспечения эксплуатации и менеджмента. Следовательно, важно, чтобы весь персонал был ознакомлен с рекомендациями, относящимися к вопросу оповещения о возможных событиях информационной безопасности, включая формы отчета, имел доступ к ним и знал сотрудников, которых необходимо оповещать о каждом случае появления события информационной безопасности. Необходимо, чтобы весь персонал организации был, по крайней мере, осведомлен о форме отчета, что способствовало бы его пониманию системы менеджмента инцидентов информационной безопасности.[1]

Ответственность предполагает разработку документации, содержащей информацию об ответственности не только руководства организации, но и лиц из числа персонала, которые непосредственно или косвенно связаны с системой управления инцидентами информационной безопасности. Эти документы должны информировать сотрудников об ответственности на всех этапах реализации системы: начиная с обнаружения и заканчивая реагированием и принятием мер, предотвращающих повторное возникновение инцидента. Также инструкции должны предусматривать ответственность виновных в совершении инцидента. Данная мера необходима для предостережения сотрудников от создания угроз информационной безопасности и совершения событий информационной безопасности, которые потенциально могут нанести ущерб организации и, следовательно, перейти в разряд инцидентов информационной безопасности.

В процессе извлечения уроков следует учитывать, что после завершения инцидента информационной безопасности важно быстро идентифицировать уроки, извлеченные из его обработки, и предпринять соответствующие действия, которые могут рассматриваться с точки зрения:

– новых или изменившихся требований к мерам защиты информационной безопасности. Это могут быть технические или нетехнические (включая физические) меры защиты. В зависимости от извлеченных уроков требования могут включать в себя необходимость быстрого обновления материалов и проведения инструктажа с целью обеспечения осведомленности в вопросах безопасности (для пользователей, а также для другого персонала) и выпуска руководств и (или) стандартов по безопасности;

– изменений в системе менеджмента инцидентов информационной безопасности и ее процессах, формах отчета и базе данных событий/инцидентов информационной безопасности.

Кроме того при изучении урока по инциденту информационной безопасности необходимо рассматривать полученный опыт не только в рамках отдельного инцидента информационной безопасности, но и проводить проверку наличия тенденций (закономерностей) появления предпосылок к инцидентам информационной безопасности, которые могут быть использованы в интересах определения потребности в защитных мерах или изменениях подходов к устранению инцидента информационной безопасности. Целесообразно также проведение тестирования информационной безопасности, в особенности оценки уязвимостей, после ориентированного на ИТ инцидента информационной безопасности.

Поэтому необходимо регулярно анализировать базы данных событий/инцидентов информационной безопасности для определения:

– тенденций/образцов;

– проблемных областей;

– областей деятельности, где можно предпринять предупредительные меры для снижения вероятности появления инцидентов в будущем.

Существенная информация, получаемая в процессе обработки инцидента информационной безопасности, должна направляться для анализа тенденций (закономерностей), что может в значительной мере способствовать ранней идентификации инцидентов информационной безопасности и обеспечивать предупреждение о том, какие следующие инциденты информационной безопасности могут возникнуть на основе предшествующего опыта и документов.

Необходимо также использовать информацию об инцидентах информационной безопасности и соответствующих им уязвимостях, полученную от государственных и коммерческих поставщиков.

Итоговый анализ инцидентов информационной безопасности представляется для обсуждения его на каждом совещании руководства организации по вопросам обеспечения информационной безопасности и (или) на других совещаниях, касающихся вопросов по общей организационной политике информационной безопасности[1].

При сборе доказательств для ускорения процесса расследования в организации может быть проведена первичная идентификация нарушителя. Попытка идентификация нарушителя в процессе расследования инцидента не всегда может завершиться удачей. Не смотря на успех процедуры противодействия распространению инцидента, для определения “личности” злоумышленника может потребоваться расследование нескольких инцидентов, сопоставление фактов, анализ “почерка” атакующего. В любом случае, если угроза не исходит от внутреннего нарушителя и инцидент не является сложной цепочкой событий, которая, возможно, приведёт к сговору сотрудников организации, действия экспертов команды реагирования должны быть направлены на реализацию мер, которые являются предметом данного регламента. В противном случае, к расследованию инциденты должны быть подключены соответствующие службы внутренней безопасности. Важным является сбор и анализ свидетельств инцидента.[3]

Следует подчеркнуть, что сбор доказательств всегда должен проводиться в соответствии с правилами судопроизводства или слушания дела, для которых возможно представление данного доказательства. Для правовой оценки инцидентов информационной безопасности сформирована соответствующая база позволяющая оценить принадлежность инцидента к преступлению в соответствии с законодательством Российской Федерации или преступлению по классификатору Интерпола.

Разработанные авторами практические рекомендации планируется использовать в учебном процессе АлтГТУ, при подготовке специалистов по защите информации, а также на курсах повышения квалификации по программам в области защиты конфиденциальной информации.

Список литературы

1. ГОСТ Р ИСО/МЭК 27001 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2008.- 48с.
2. ГОСТ Р ИСО/МЭК 18044 -2007 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М.: Стандартинформ, 2007. -47с.
3. Романовский С. Обработка инцидентов информационной безопасности, "Искусство управления информационной безопасностью". [Электронный ресурс] - http://www.iso27000.ru

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ТРАНСПОРТНЫХ ПОТОКОВ В РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ СБОРА И ОБРАБОТКИ ДАННЫХ

Бочкарева Е.В. – аспирант, Харламов А.И. – аспирант
Алтайский государственный технический университет (г. Барнаул)

Перспективным направлением в области разработки распределенных вычислительных систем является предварительное моделирование их работы, которое позволяет снизить риски и удешевить проектирование аппаратной части, структуры и размещения данных.

Поскольку события носят случайный характер, то предлагается организовать работу имитационной системы по принципу одноканальной СМО без отказов – G\G\1. В качестве требования в построенной имитационной системе рассматривается событие, а в качестве обслуживающего прибора - диспетчер. Тогда вся система имитационного моделирования представляет набор взаимодействующих СМО.

Для моделирования работы гетерогенной распределенной системы разработана событийно-ориентированная имитационная система. Для каждого компонента имитационной системы (сетевое оборудование, вычислительные узлы, дисковые хранилища) определяется список событий, вводится **диспетчер** и **очередь**. При этом при обработке события могут формироваться новые события или управляющие воздействия. Предусмотрены очереди событий для диспетчера каждого устройства и для диспетчера всей имитационной системы. Событие характеризуется: типом (например: возникновение нештатной ситуации, отправка запроса на данные, получение данных, остановка работы процесса и т.д.); статусом (обработано или нет); идеальным временем для обработки (при необходимости обработки события по расписанию в некоторый момент модельного времени); реальным временем обработки (тот момент модельного времени, когда диспетчер закончил обработку события). Заявки, относящиеся к логике работы отдельного устройства, обрабатываются его диспетчером. Запросы, необходимые для организации взаимодействия потоков, для моделирования аппаратного взаимодействия, для обработки информации, имеющей отношение к среде в целом, обрабатываются в очереди диспетчера среды моделирования.

Заметим, что поток заявок является неравномерным, поэтому предлагается выделить фиксированное количество видов событий, с заданными законами распределения интервалов между поступлениями и распределения времени обслуживания таких заявок. Для событий предусмотрена их реализация в виде функций с разной вычислительной сложностью, зависящей от типа событий и предыдущих выполненных заявок. Порядок сложности определяет, какую зависимость имеет сложность вычисления данной функции от объема обрабатываемых данных: зависимость может быть линейной, полиномиальной, экспоненциальной, логарифмической; что определяет количество операций, необходимых для вычисления функции, а, как следствие, и время, необходимое для обработки соответствующего события. Вставка событий в очередь возможна в произвольное место очереди в соответствии с расписанием событий.

В построенной системе моделирования используется метод коррекции таймера модельного времени с переменным шагом. То есть приращение времени равно интервалу между двумя последовательными событиями. При такой организации таймера модельного времени события обрабатываются одновременно только тогда, когда эти события действительно произошли (или запланированы) в один и тот же момент модельного времени

Разработанная модель позволяет исследовать характеристики системы в стационарном и критических режимах (среднее время задержек, длины очередей, пропускную способность системы и т.д.) в зависимости от ее размера и архитектуры, а также зависимость характеристик сети от выбранного для реализации вида СМО диспетчеров системы и устройств.

РАЗРАБОТКА КОНЦЕПТУАЛЬНОЙ МОДЕЛИ 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 [1], 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 нем бесплатных продуктов программного обеспечения(Oracle 10g Express Edition) 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:

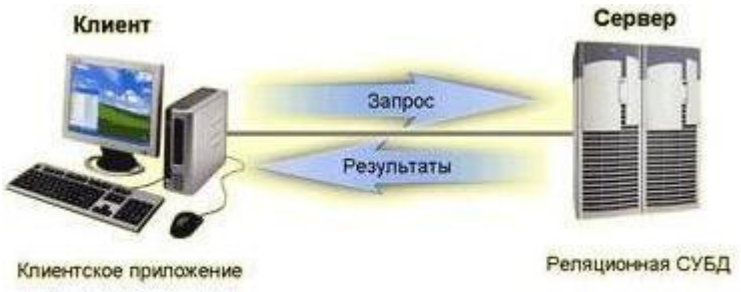

Рисунок 1. Архитектура клиент-сервер

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.

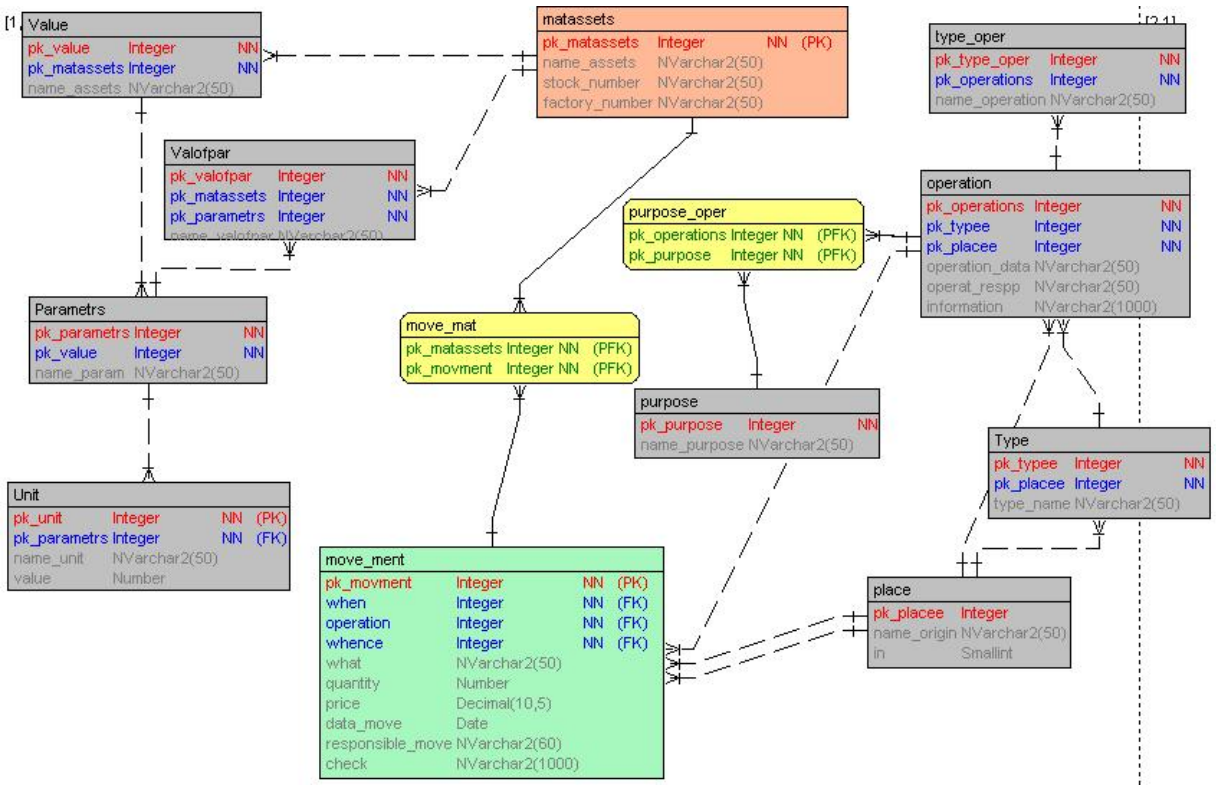

Рисунок 2. Концептуальная модель

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 и 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

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ РОБОТА НА ОСНОВЕ АНАЛИЗА ВНЕШНИХ КОМАНД И СИГНАЛОВ ДАТЧИКОВ СЕНСОРНОЙ СИСТЕМЫ

Матвеев В.В. – студент, Сучкова Л.И. – к.т.н, профессор

Алтайский государственный технический университет (г. Барнаул)

Требования научно-технического прогресса обусловливают широкое внедрение в производственный процесс и даже в офисную и домашнюю работу человека роботов, оборудованных широким спектром разнообразных датчиков. Объективными предпосылками возникновения такой потребности являются развитие информационных технологий и средств коммуникации. Преимущества такого подхода заключаются в исключении человеческого фактора, росте скорости выполнения технологических операций и действий. Однако недостатком использования роботов является ограниченность возможностей датчиков и необходимость тщательной проверки реакции робота на команды при различных факторах

внешней среды.

Функциональная схема робота, приведенная на рисунке 1, включает следующие блоки:

- Исполнительная система. Состоит из всевозможных манипуляторов и транспортного модуля. Отвечает за любые движения робота, а также за его передвижения в пространстве.
- Сенсорная система. Осуществляет взаимодействие с внешней средой при помощи датчиков.
- Информационно-управляющая система. Выполняет контроль получаемых от сенсорной системы данных и на основе них управляет исполнительной системой.
- Система связи. Реализует связь робота с оператором.

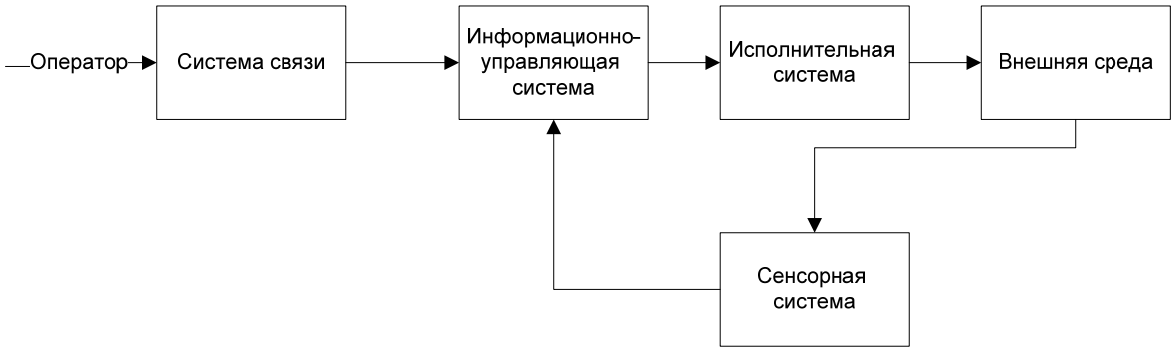

Рисунок 1

При разработке информационно-управляющей системы необходимо исследовать полноту системы команд с точки зрения адекватной реакции робота на постоянно меняющиеся внешние воздействия. В связи с этим актуальна разработка имитационных систем для моделирования реакции робота в зависимости от текущего состояния робота, текущей команды и сигналов с сенсорной системы. Такое моделирование при задании команд на некотором входном языке может быть основано на синтаксически управляемом (СУ) переводе. Язык команд описывается формальной грамматикой. Можно считать, что последовательность команд должна быть переведена в последовательность действий робота, которая в дальнейшем может быть оценена на адекватность. В процессе СУ-перевода правила исходной грамматики дополняются функциями, описывающими анализ сигналов сенсорной системы..

Программа для имитационного моделирования была написана на языке C#, среда разработки - Microsoft Visual Studio 2008. Программа имеет графический, интуитивно понятный интерфейс. Пользователю предоставляется возможность пошагового моделирования. Все выполняемые действия подробно комментируются.

ПРИМЕНЕНИЕ ИНТЕРНЕТ-ТЕХНОЛОГИЙ ДЛЯ ВИЗУАЛИЗАЦИИ ОДНОМЕРНЫХ ДИНАМИЧЕСКИХ ПРОЦЕССОВ

Матяс А.Ю. – студент, Якунин А.Г. – д.т.н, профессор

Алтайский государственный технический университет (г. Барнаул)

В наше время все большее распространение получают системы диспетчерского контроля и сбора данных (SCADA). Их задача – сбор и обработка информации, получаемой от различных датчиков и контроллеров, управление устройствами.

Как правило, в состав SCADA входит программное обеспечение для визуализации процессов, дающее возможность конечному пользователю осуществлять мониторинг событий, протекающих в системе. В большинстве своем интерфейс реализован как desktop-приложение. Однако такое решение не всегда удобно: оно обладает низкими возможностями развертывания, так как требует установки на каждый операторский компьютер. С ростом SCADA системы увеличивается необходимое количество персонала для ее обслуживания, следовательно, растет и требуемое число компьютеров. Ввод каждой новой машины связан с единовременными трудовыми и временными затратами на развертывание ПО и с затратами на его обслуживание в дальнейшем. Поэтому требуются новые подходы к созданию интерфейсной части SCADA систем.

Возможное решение указанной проблемы – реализация интерфейса как web-приложения. Потенциально такой подход имеет следующие преимущества:

1. кроссплатформенность (сегодня любая пользовательская операционная система имеет встроенные средства для просмотра web-страниц);
2. доступность практически из любой точки планеты (достаточно скорости, обеспечиваемой GPRS модулем мобильного телефона, чтобы запустить интерфейс, например, на ноутбуке);
3. отсутствие необходимости в многократной установке и настройке ПО.

Разрабатываемое ПО для мониторинга одномерных динамических процессов состоит из серверной и клиентской частей. Серверная часть реализована как сценарий на языке PHP. Ее роль – выборка информации из базы данных SCADA путем отправки SQL запросов и передача полученных данных клиенту. В качестве транспортного формата (для обмена между сервером и клиентом) ввиду компактности выбран JSON.

Разработка клиентской части ведется на основе технологии Adobe Flash с использованием сценарного языка ActionScript 3.0. Ее задача – периодический запрос обновленной информации с сервера и наглядное ее отображение в виде графиков пользователю. Пример формы клиентской части представлен на рисунке 1.

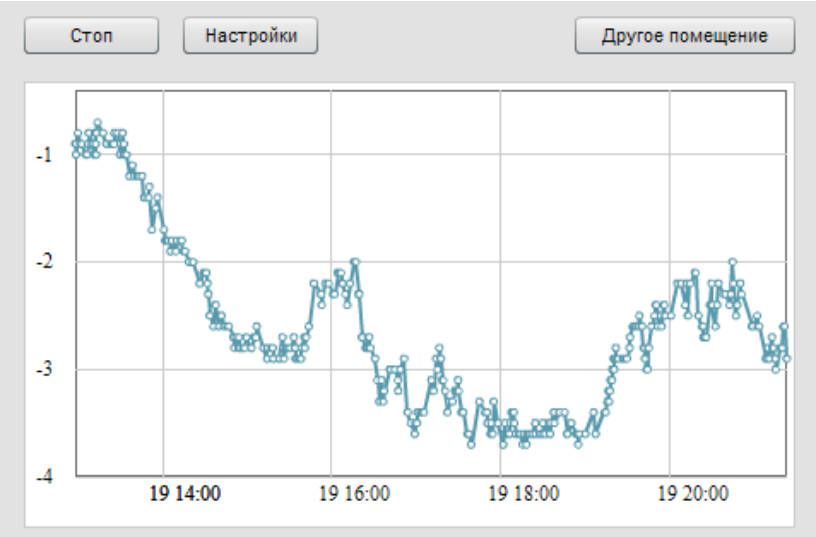

Рисунок 1

В целях тестирования и отладки ПО для мониторинга одномерных динамических процессов создан программно-аппаратный комплекс сбора температурных данных, структура которого представлена на рисунке 2:

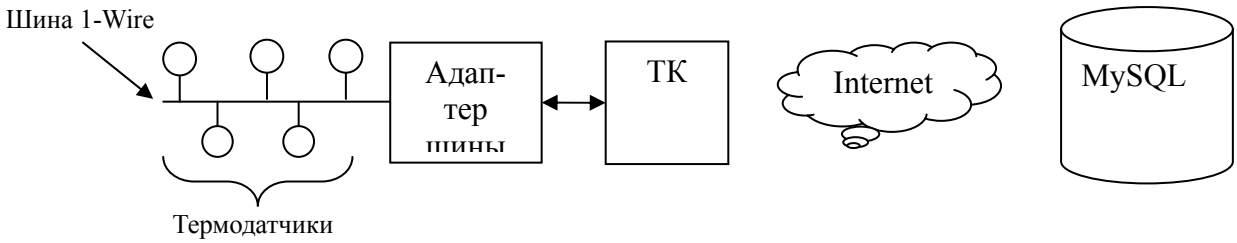

Рисунок 2

С помощью специального адаптера шина 1-Wire подключена к технологическому компьютеру (ТК), который осуществляет сбор информации о температуре с подключенных к ней датчиков. ТК имеет доступ к сети Интернет и сохраняет полученную информацию на удаленном сервере баз данных MySQL. Программа для работы с шиной, установленная на ТК, использует драйверы адаптера и специальный программный интерфейс (API) OW.NET, поставляемые компанией-разработчиком устройств 1-Wire – фирмой MAXIM. API для удаленной работы с БД MySQL поставляется SUN Microsystems.

Архитектура программного обеспечения для мониторинга одномерных динамических процессов и используемые для его создания web-технологии обеспечивают высокий комфорт работы оператора, простоту установки и настройки ПО. При этом возможное количество одновременно подключенных пользователей ограничивается лишь производительностью web-сервера и сервера БД.

МОДИФИКАЦИЯ ГРАДИЕНТНОГО МЕТОДА ОПРЕДЕЛЕНИЯ КОНТУРОВ ОБЪЕКТА ИЗОБРАЖЕНИЯ

Ненашев А.Л. – аспирант

Алтайский государственный технический университет (г. Барнаул)

Повышение интенсивности человеческой жизнедеятельности влечет за собой необходимость упрощения процедур контроля, автоматизации и идентификации для экономии человеческих ресурсов и времени. На сегодняшний день, в связи с интенсивным развитием интеллектуальных систем, появляется возможность решения многих задач путем создания прикладных систем интеллектуального анализа данных.

Одной из таких задач является задача распознавания различных псевдорегулярных объектов. Прежде чем распознать объект, необходимо получить контур объекта - получить границы объекта. Для этой цели была выполнено программное средство, в котором предусмотрены опции предварительной фильтрации и предобработки изображения. В качестве тествого образца взято изображение, отснятое с печной конвейерной линии на предприятии ОАО «Русский хлеб»[1], на котором изображены объекты – хлеб (рис.1).

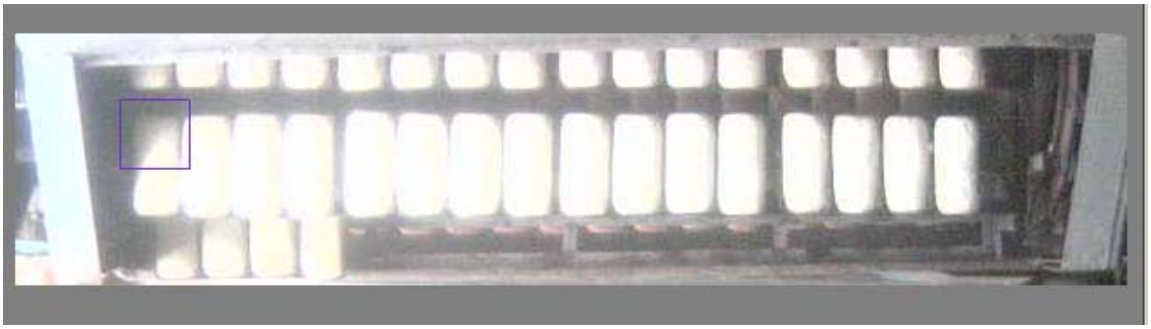

Рисунок 1 – Образец изображения конвейерной линии

Для детального исследования алгоритма определения контуров был взят фрагмент этой печной линии, выделенный на рисунке 1. Фрагмент представлен на рисунке 2.

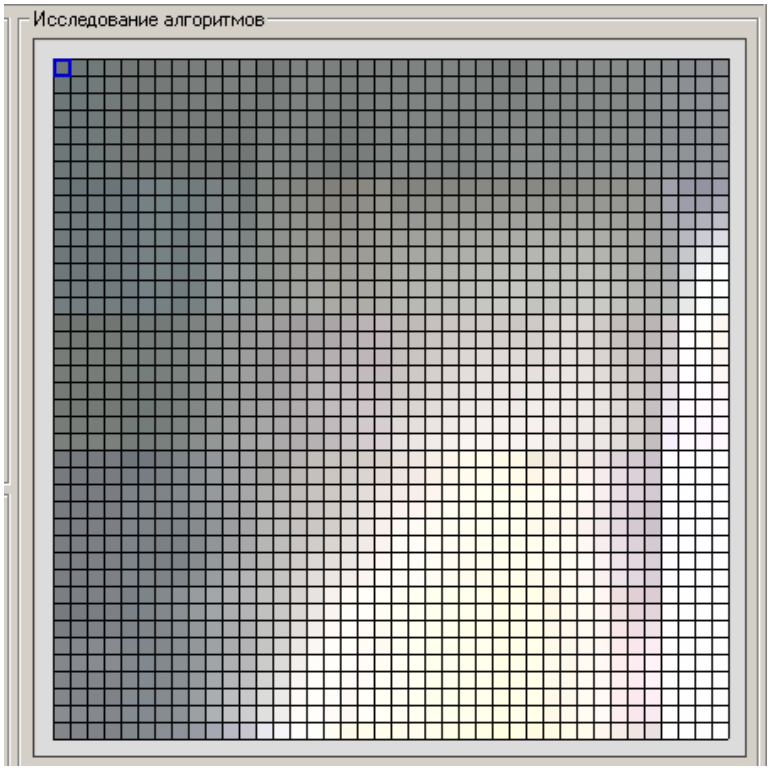

Рисунок 2 – Фрагмент изображения конвейерной линии

Граница – это контрастная область изображения, содержащая резкое различие яркости между двумя соседними пикселями. Существует множество различных методов выделения границ. На рисунке 2 представлен объект с искажающимися границами контура – перепады яркости мало различаются. Для того чтобы выделить границу объекта при незначительных передах, можно воспользоваться градиентным методом [2]. Суть градиентного метода состоит в нахождении производных цифрового изображения по X и по Y с последующим их суммированием.

При использовании градиентного метода необходимо задать константу (порог) определяющую минимальное значение перепада яркости, которое будет «отбрасывать» пиксели, значения перепадов яркости которых будет меньше чем заданное минимальное значение. Результат работы градиентного метода с использованием порога (равным 5) представлен на рисунке 3.

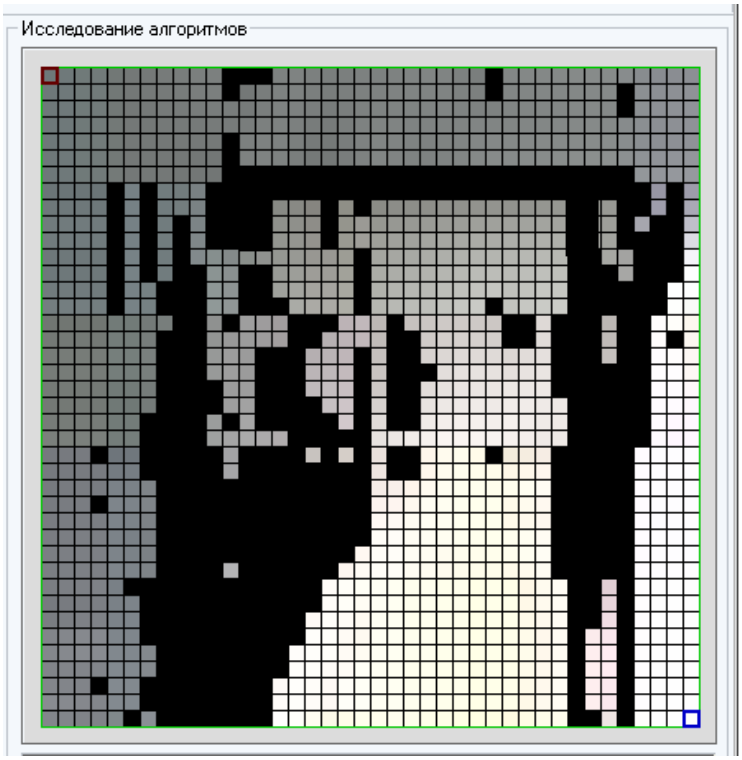

Рисунок 3 – Результат работы алгоритма определения контура объекта с использованием градиентного метода.

Как видно из результата работы вышеописанного алгоритма, градиентный метод не дает хороших результатов. Поэтому предлагается новый метод 3D обработки отдельных пикселей на основе градиентного метода. Суть предлагаемого метода заключается в обходе вершин контура представляющий собой «хребет» в 3D проекции. Самые пиковые(экстремумы) значения вершин «хребта» считаются как точками границ контура объекта. На рисунке 4 представлен результат такого алгоритма. Как видно из рисунка, однако остаются лишние пиксели, принадлежащие к псевдо контурам.

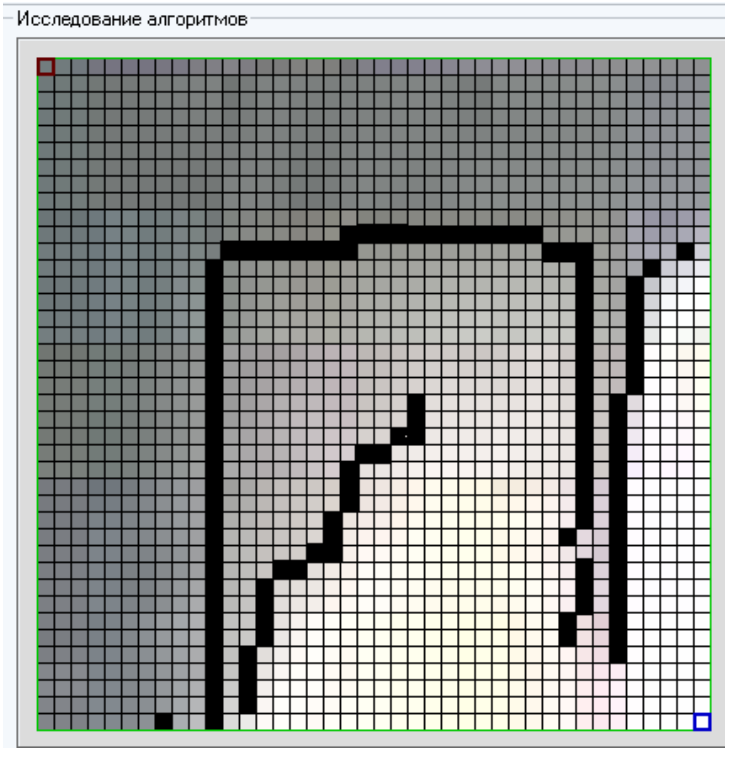

Рисунок 4 – Результат работы метода 3D обработки на основе градиентного метода

Выводы

Предложенный алгоритм определения контура объекта показывает хорошие результаты. На данном этапе разрабатывается дополнение к алгоритму для «уничтожения» псевдо контуров.

Список литературы

1. Жихарев И.М., Хомутов О.И., Якунин А.Г. Особенности обработки сцены изображения в системе технического зрения контроля и подсчета изделий на конвейерах жарочных печей. Материалы международной научной конференции «Информационные технологии в современном мире», ч.4. – Таганрог: Изд-во «Антон», ТРТУ, 2006. с.27-29.
2. Гонсалес Р., Вудс Р. Цифровая обработка изображений. Перевод с англ. под редакцией П.А. Чочиа. – М.:«Техносфера», 2005. – 1072 с.

КОНСТРУИРОВАНИЕ И ИССЛЕДОВАНИЕ РАБОТЫ СТРУКТУРНЫХ АВТОМАТОВ-ПРЕОБРАЗОВАТЕЛЕЙ И СЕТЕЙ ПЕТРИ

Перелыгин А.С. – студент, Сучкова Л.И. – к.т.н., профессор

Алтайский государственный технический университет (г. Барнаул)

Автоматы-преобразователи являются средством моделирования и исследования логики работы широкого круга устройств, используемых в различных сферах человеческой деятельности. Известные программные продукты, автоматизирующие процесс синтеза структурных автоматов и сетей Петри, либо не имеют достаточной функциональности и удобства использования, либо являются коммерческими, и отсутствуют возможности их доработки.

Была поставлена задача разработать программный комплекс, позволяющий производить синтез структурных автоматов, а также моделировать работу произвольно заданной сети Петри.

Термин "автомат" используется в двух аспектах. С одной стороны, автомат – устройство, выполняющее некоторые функции без участия человека (например, ЭВМ). С другой стороны, термин "автомат" – математическое понятие и обозначает математическую модель реальных технических процессов. Цифровые автоматы делят на два класса. В синхронных автоматах моменты времени, в которые фиксируются состояния автомата, задаются специальным устройством – генератором синхроимпульсов. В асинхронных автоматах моменты перехода автомата из одного состояния в другое заранее не определены и зависят от каких-то событий.

Взаимодействие событий в больших асинхронных системах имеет, как правило, сложную динамическую структуру. Эти взаимодействия описываются более просто, если указывать не непосредственные связи между событиями, а те ситуации, при которых данное событие может реализоваться. При этом глобальные ситуации в системе формируются с помощью локальных операций, называемых условиями реализации событий. Таким образом, предполагается, что для решения указанных задач достаточно представлять дискретные системы как структуры, образованные из элементов двух типов — событий и условий. В сетях Петри события и условия представлены абстрактными символами из двух непересекающихся алфавитов, называемых соответственно множеством переходов и множеством мест. В графическом представлении сетей переходы изображаются "барьерами", а места — кружками. Условия-места и события-переходы связаны отношением непосредственной зависимости (непосредственной причинно-следственной связи), которое изображается с помощью направленных дуг, ведущих из мест в переходы и из переходов в

места. Программа для моделирования работы сетей Петри была написана на языке C#, среда разработки - Microsoft Visual Studio 2008. Программа имеет графический интерфейс, главное окно программы представлено на рисунке 1:

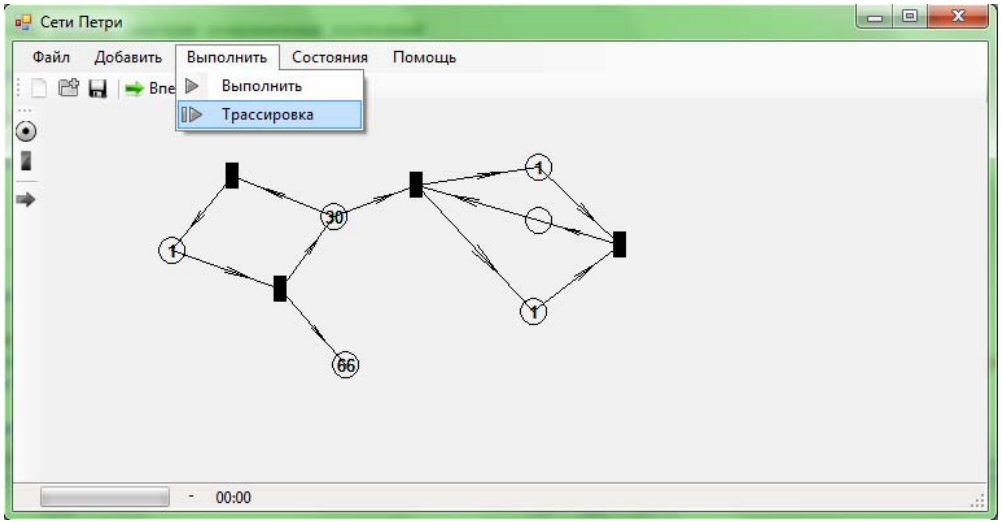

Рисунок 1

Программа предоставляет возможность создания новой сети, или открытия из файла ранее сохраненной. Пользователю предоставляется возможность редактировать сеть методом добавления ее элементов в рабочую область, указывать емкости условий и строить линии связи между объектами. После построения сети пользователь может запустить ее в трех режимах –в режиме трассировки (остановка через указанное количество времени или шагов) и в режиме пошагового выполнения. В любой момент времени состояние сети можно запомнить или указать интервал во времени или в шагах, через которые состояния будут запоминаться автоматически. В дальнейшем сеть может быть возвращена к сохраненному состоянию.

Для синтеза структурных автоматов разработано приложение, требующее задания абстрактного автомата-преобразователя путем заполнения таблицы переходов и таблицы выходов. Структурный синтез требует выбора конкретного триггера в качестве элемента памяти. В процессе расчета программа кодирует состояния, используя зеркальный метод, строит таблицу функций возбуждения, карты Карно и формирует структурную схему автомата-преобразователя.

В результате получен комплекс программ, позволяющий в интерактивном режиме создать сеть Петри и проанализировать, как эта сеть будет функционировать, а также осуществить синтез абстрактного автомата. Разработанный комплекс программ предназначен для использования в учебном процессе студентами специальности «Вычислительные машины, комплексы, системы и сети».

.

ИЗМЕРЕНИЕ СКОРОСТИ И НАПРАВЛЕНИЯ ВОЗДУШНОГО ПОТОКА В ТРЕХ ИЗМЕРЕНИЯХ С ИСПОЛЬЗОВАНИЕМ АКУСТИЧЕСКОГО МЕТОДА

Плотников А.Д. – студент

Алтайский государственный технический университет (г. Барнаул)

Проблема измерения скоростей (анемометрия) воздушных потоков и направления их перемещения в промышленности, в медицине, в системах экологического мониторинга, в системах автоматического управления диктует всё более высокие требования к

метрологическим и эксплуатационным характеристикам измерительных приборов. Эти требования уже не могут быть выполнены путём улучшения приборов, основанных на традиционных принципах, таких как тепловые и тахометрические. Потребность обеспечения безынерционности измерений, достаточно широкого динамического диапазона, высокой чувствительности, приемлемой точности в начале диапазона и достаточной надёжности привела к необходимости обратиться к другим физическим идеям, в частности, к акустическим методам измерения. Основными достоинствами акустических анемометров является то, что они не имеют подвижных частей, а значит - не имеют физического износа; не вносят аэродинамического сопротивления в контролируемый поток; не нарушают аэродинамической эпюры скоростей; практически безынерционны. Среди акустических расходомеров в основном распространение получили приборы, в которых измеряется разность времен прохождения акустических колебаний по потоку и против него [1].

Существующие на сегодняшний день анемометры, основанные на акустическом методе, измеряющие скорость и направление потока в трех направлениях, имеют в своей конструкции шесть ультразвуковых датчиков/излучателей [2]. В данной работе предлагается упрощение конструкции – использование четырех датчиков/излучателей. Измерение производится поочередно для трех разных пар датчиков. Полученные данные представляют собой составляющие проекции вектора скорости потока, по которым можно определить истинное значение скорости и направление воздушного потока. Для определения каждой проекции используется формула:

$$v = \frac{x \cdot (t_2 - t_1)}{2 \cdot t_1 \cdot t_2}$$

где x – расстояние между излучателем и приемником, t_1 – время прохождения звуковой волны в прямом направлении, t_2 – время прохождения звуковой волны в обратном направлении.

Данная формула позволяет избавиться в расчетах от скорости распространения звуковой волны, зависящей, в свою очередь, от таких факторов, как температура воздуха, влажность, давление, наличие газовых примесей и др. На рис. 1 представлены графики относительной погрешности вычисления скорости потока при различных расстояниях L между ультразвуковыми датчиками (при этом абсолютная погрешность измерения расстояния составляла 5e-3 м, абсолютная погрешность измерения времени – 5e-6 с).

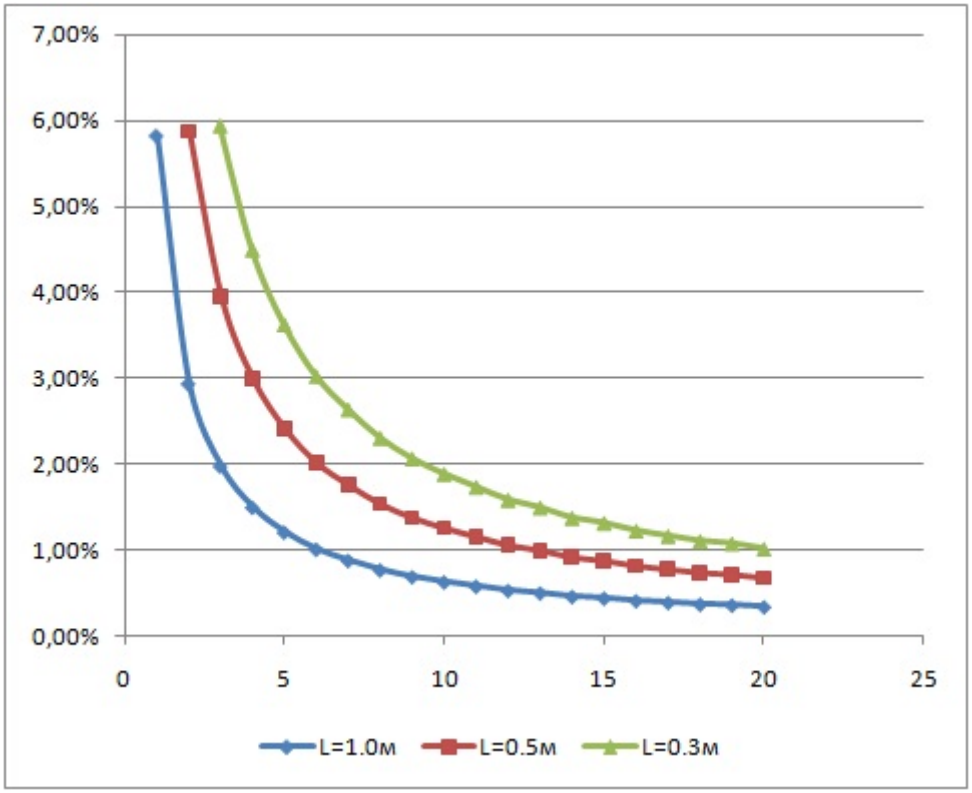

Рисунок 1 – Относительная погрешность вычисления скорости воздушного потока

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.html
2. Акустические анемометры. [Электронный ресурс] // Режим доступа: http://typhoon-tower.obninsk.org/ru/akan.html

ВЫБОР АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБРАБОТКИ ЭКГ-СИГНАЛА

Таныгин А.А. – студент

Алтайский государственный технический университет (г. Барнаул)

Компьютерная диагностика здоровья человека известна и используется уже не первый год. Она позволяет более полно оценить картину состояния организма, определить дисфункции органов даже в том случае, когда они ещё не успели развиться, что часто представляется невозможным при использовании традиционных методов диагностики. Функционал, который предоставляют высокоточные электронные устройства и компьютерная обработка информации, поражает своей широтой, непревзойдённой точностью, объёмом обрабатываемых данных и скоростью их обработки. В связи с этим не остаётся никаких сомнений в том, что компьютерная диагностика — это предсказуемое и оправданное развитие технологий, используемых ранее.

Алгоритм разрабатываемой программы содержит в себе следующие шаги:

1. Подготовка входных данных (фильтрация сигнала).
2. Распознавание характерных участков ЭКГ, имеющих диагностическое значение, с дальнейшим вычислением и анализом параметров распознанных участков.

Фильтрация сигнала осуществляется при помощи адаптивных алгоритмов и не представляет особого интереса.

Для распознавания полученного сигнала могут быть использованы разные подходы. Например, хороших результатов можно достичь, используя одновременно синтаксический и корреляционный методы [1]. Синтаксический метод начинается с простого поиска экстремума (зубец R), затем создаётся параметрическое описание QRS-комплекса и производится анализ всего сигнала на предмет локализации похожих участков, являющихся другими QRS-комплексами. Данный метод имеет хорошую устойчивость к колебаниям изолинии. Корреляционный метод основан на измерении степени подобия эталонного образца фрагмента ЭКГ и фрагмента исследуемой ЭКГ той же размерности при сканировании вдоль временной оси с шагом в один отсчет. В результате получаем массив коэффициентов корреляции, распределенных по временной оси сигнала ЭКГ, которые максимально приближаются к единичному значению в участках максимального сходства образца и фрагмента ЭКГ. Корреляционный метод показывает высокую чувствительность даже на зашумленных участках ЭКГ и позволяет достаточно точно локализовывать характерные участки электрокардиосигнала.

Ещё одним способом распознавания сигнала является метод, в основе которого лежит предположение о том, что QRS-комплекс представляет собой участок кардиограммы с наиболее высоким уровнем мощности сигнала. Исходя из этого, для обнаружения комплексов вычисляют текущие значения мощности сигнала и сравнивают с некоторым пороговым значением. Для повышения надежности обнаружения QRS-комплексов порог мощности не задают постоянной величиной, а вычисляют по адаптивному алгоритму, учитывающему изменение мощности сигнала от комплекса к комплексу.

Мощность ЭКГ-сигнала вычисляют как сумму абсолютных значений производной

сигнала в области вокруг данного отсчета ЭКГ. При этом мощность очень мало зависит от уровня сигнала и смещения изолинии. Ширина области выбирается приблизительно равной ширине типичного QRS-комплекса. Полученные значения мощности $P_x(i)$ последовательно сравнивают с некоторым пороговым значением P_t. Конкретное значение порога P_t не влияет на точность способа и выбирается равным примерно половине максимальной мощности P_x. Результаты сравнения используют лишь для первого, грубого определения момента появления QRS-комплекса. Далее, приняв, что характерной точкой комплекса является точка с наибольшей скоростью изменения сигнала (точка экстремума производной сигнала), ищут экстремум производной сигнала на интервалах, где $P_x(i)>P_t$. Этой точке и соответствует момент появления QRS-комплекса. Определение момента времени по производной сигнала позволяет найти его более точно, так как производная сигнала изменяется во времени довольно быстро. Погрешность же определения момента времени равна интервалу времени, за который сигнал изменяется на величину, равную погрешности его измерения, а поскольку производная изменяется достаточно быстро, то и точность определения момента времени по производной будет достаточно высокой.

Дополнительно повышающим точность способа фактором является то, что момент максимума производной определяют с точностью, более высокой, чем дискретность отсчетов исходного сигнала. Для этого после вычисления производной dx(i) в дискретные моменты времени и нахождения максимального значения $d_{max}=dx(i_{max})$ в некотором интервале вокруг i_{max} выполняют аппроксимацию значений производной параболой (или другой функцией) и вычисляют момент времени T_{max}, равный моменту максимума параболы. Точность определения T_{max} при этом не ограничивается дискретностью отсчетов, а определяется лишь погрешностью аппроксимации.

Преимущество описанного способа состоит в существенно более высокой точности определения момента появления QRS-комплекса. Другим преимуществом способа является его нечувствительность к медленным изменениям сигнала (к дрейфу изолинии), связанная с использованием производной, не содержащей постоянной составляющей исходного сигнала, что позволяет уменьшить число ошибок при его применении.

Список литературы

1. Богатов Н.М., Гук В.Ф. Сравнительный анализ методов распознавания электрокардиограмм. [Электронный ресурс] / Н.М. Богатов, В.Ф. Гук // Режим доступа: www.econf.rae.ru/article/1267