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

НАУКА И МОЛОДЕЖЬ – 2008

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

СЕКЦИЯ

ИНФОРМАЦИОННЫЕ И ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

подсекция

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТА ИНФОРМАЦИИ

Барнаул – 2008

ББК 784.584 (2 Рос 537) 638.1

V Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь – 2008". Секция «Информационные и образовательные технологии». Подсекция «Безопасность информационных технологий и защита информации». / Алт. гос. техн. ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2008. – 15 с.

В сборнике представлены работы научно-технической конференции студентов, аспирантов и молодых ученых, проходившей в апреле 2008 г.

Организационный комитет конференции:
Максименко А.А., проректор по НИР – председатель, Марков А.М., зам. проректора по НИР – зам. председателя, Стопорева Т.А. – ответственный секретарь Центра НИРС – секретарь оргкомитета, Кантор С.А., заведующий кафедрой «Прикладная математика» АлтГТУ – руководитель секции.

Научный руководитель подсекции: зав. кафедрой ЗИРСС,
д.т.н., профессор, Белов В.М.
Секретарь подсекции: к.в.н., профессор, Загинайлов Ю.Н.

СОДЕРЖАНИЕ

РАЗРАБОТКА МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ВНЕДРЕНИЮ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ НА ОСНОВЕ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 27001:2005

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

Развитие малых и средних предприятий является одним из наиболее приоритетных направлений реформирования экономики. Значимость малого бизнеса обусловлена его специфическими свойствами, ключевыми из которых являются оперативность, мобильность и способность достаточно гибко реагировать на все изменения конъюнктуры рынка. В связи с приближающимся вступлением России в ВТО и необходимостью повышения конкурентоспособности отечественной продукции перед предприятиями малого и среднего бизнеса ставится задача активного внедрения систем менеджмента качества.

При вступлении в ВТО Россия, как и многие восточноазиатские страны, может потерять до 40% предприятий малого бизнеса из-за отсутствия конкурентоспособных компаний, а одним из конкурентных преимуществ организации является действующая система менеджмента, будь то качества, экологии или информационной безопасности [1].

Арсенал международных стандартов, в которых установлены критерии оценки соответствия в различных областях системы общего менеджмента организации, в 2005 г. пополнился стандартом ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [2], определяющим требования для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения документированной системы менеджмента информационной безопасности (СМИБ) в контексте общих деловых рисков организации. Он определяет требования для реализации средств управления защитой, приспособленных к потребностям отдельных организаций или их подразделений.

СМИБ разрабатывается для того, чтобы обеспечить выбор адекватных и пропорциональных средств управления защитой, которые защищают информационные активы и придают уверенность заинтересованным сторонам.

В целом можно выделить следующие преимущества от внедрения СМИБ, соответствующей требованиям стандарта ISO/IEC 27001:2005[3]:

- повышение управляемости и надежности бизнеса компании;
- повышение защищенности ключевых бизнес-процессов компании;
- повышение доверия к компании как к партнеру, так и к клиенту;
- соответствие компании требованиям данного стандарта подчеркивает прозрачность бизнеса компании;
- наличие СМИБ и сертификата соответствия ISO/IEC 27001 упрощает процедуру выхода компании на внешние рынки;
- международное признание и повышение авторитета компании как на внутреннем, так и на внешнем рынках;
- повышение доходности и капитализации бизнеса в целом.

В настоящее время более семи тысяч организаций более чем из 70 стран стали обладателями сертификата соответствия ISO/IEC 27001. В России сертификация по ISO 27001 только набирает обороты, однако в перспективе значение стандартизации как средства экономического и научно-технологического развития национальных производителей повысится [4]. Затраты на эту деятельность в большинстве развитых стран относятся к инновационным расходам и субсидируются государством. Что касается России, то на текущий момент государство активно поддерживает предпринимательство, компенсируя расходы на сертификацию, включая консалтинг. Но проблема заключается в том, что эта поддержка касается в основном достаточно крупных компаний, а предприятиям малого и среднего бизнеса проблематично получить помощь со стороны государства в данной области.

Большинство организаций малого и среднего бизнеса не может позволить себе обратиться в консалтинговую компанию для проведения процедуры сертификации, поскольку это требует больших материальных затрат. Именно в интересах организаций малого и среднего бизнеса, желающих внедрить СМИБ и сертифицировать ее на соответствие международному стандарту ISO 27001, но не имеющих возможности, главным образом материальной, и были разработаны методические рекомендации по внедрению системы менеджмента информационной безопасности в организации на основе ISO/IEC 27001:2005.

Разработанные методические рекомендации [5] не только значительно упростят понимание данного процесса заинтересованными людьми, но и позволят внедрить СМИБ на предприятии своими силами, что в дальнейшем позволит существенно сократить затраты на сертификацию.

Методические рекомендации по внедрению СМИБ содержат подробный алгоритм не только тех действий, выполнение которых необходимо при создании и внедрении СМИБ, но также в них освещены вопросы, касающиеся эксплуатации, постоянного контроля, анализа работы СМИБ.

Особое внимание уделено вопросам документирования необходимых процедур при создании, внедрении и дальнейшей эксплуатации СМИБ, поскольку документирование является одной из главных составляющих системы менеджмента.

Важной частью менеджмента информационной безопасности является оценка уровня риска и методов снижения его до приемлемого уровня. Основу международного стандарта ISO/IEC 27001:2005 составляет система управление рисками, связанными с информацией.

В методических рекомендациях освещены основные стратегии анализа рисков и подробно изложена методика оценки рисков, предлагаемая как наиболее подходящий вариант при внедрении СМИБ.

Список литературы

1. Белобрагин В. Восхождение к вершинам качества продолжается // Стандарты и качество, 2008, №2.
2. Международный стандарт ISO/IEC 27001:2005 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования»/
3. Петросян Е. Наравне с первыми // Стандарты и качество, 2007, №4.
4. Свиткин М. На повестке дня – система менеджмента защиты информации // Методы менеджмента качества, 2008, №1.
5. Загинайлов Ю.Н., Решетицкая А.В. Методические рекомендации по внедрению системы менеджмента информационной безопасности в организации на основе международного стандарта ИСО/МЭК 27001 / Алт.гос.техн.ун-т им.И.И.Ползунова.- Барнаул: Изд-во АлтГТУ.-2008

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ВИРТУАЛЬНОГО КАНАЛА НА ОСНОВЕ АППАРАТА НЕЧЕТКИХ МНОЖЕСТВ

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

Успех деятельности организации зависит от ее способности накапливать, эффективно обрабатывать и анализировать информацию самого различного характера. Ущерб, связанный с нарушением работы системы защиты и утратой ценной информации, способен парализовать деятельность организации. Появление и осознание проблем информационной

безопасности приводит к необходимости оценки уровня безопасности информации. На основе оценки уровня безопасности определяют необходимую степень защиты, выбирают стратегию развития информационной структуры организации и поддерживают на должном уровне безопасность организации.

Одним из компонентов комплексной системы защиты информации выделяют защиту от внешних атак. Для чего используют модель идентификации атак. Факт сканирования портов локальной сети организации определяют путем анализа сетевого трафика. Для чего используют отдельные его параметры, которые применяют при определении набора нечетких величин. В модели идентификации атак вводят понятия: виртуальный канал (ВК) и возраст виртуального канала. Виртуальный канал для Интернет-протокола создает адресат в момент получения IP-пакета (по конкретному порту). Канал существует некоторое время, на момент обмена IP-пакетами.

Число виртуальных каналов зависит от аппаратных и программных возможностей компьютерной сети и имеет максимальное значение $max_{КВК}$. Виртуальные каналы характеризуют параметром «время жизни» (ВЖ), по которому определяют время существования канала.

В модели идентификации атак вводят две лингвистические переменные (ЛП) «Количество виртуальных каналов» (КВК) и «Возраст виртуального канала» (ВВК), которые задают кортежами $<КВК, T_{КВК}, X_{КВК}>$ и $<ВВК, T_{ВВК}, X_{ВВК}>$.

Эталоны определяют введенными ЛП (КВК и ВВК), для чего формируют базовое терм-множество на универсальном множестве $X_{КВК} \square \{0, max_{КВК}\}$. Базовое терм-множество задают пятью нечеткими термами $T_{КВК}$ ={«очень малое» (ОМ), «малое» (М), «среднее» (С), «большое» (Б), «очень большое» (ОБ)}.

Множество термов $T_{КВК}$ отображают нечеткими числами *ОМ, М, С, Б, ОБ*, для которых формируют функции принадлежности нечетких чисел (НЧ). Существуют различные методы построения функций принадлежности [1-6]: метод лингвистических термов (используют данные статистических исследований), методы на основе парных сравнений (основаны на обработки матрицы оценок парных сравнений, отражающих мнение эксперта об относительной принадлежности элементов множеству или степени выраженности у них оцениваемого свойства), метод назначения параметров, метод опроса (опрос эксперта или группы экспертов) и т.д. В модели идентификации атак на основе статистических данных, полученных сканером сети, для формирования функций принадлежности всех термов, используют метод лингвистических термов [1].

Для ЛП «Возраст виртуального канала» формируют базовое терм-множество, которое задают тремя нечетким термами $T_{ВВК}$={«молодой» (М), «средний» (СР), «старый» (СТ)}. Множество термов $T_{ВВК}$ отображают нечеткими числами *М*, *СР*, *СТ*, для которых формируют функции принадлежности.

Нечеткие эталоны $T_{КВК}$ и $T_{ВВК}$ формируют, используя логико-лингвистический подход [2]. Значения эталонных ЛП переопределяют в зависимости от условий функционирования локальной вычислительной сети.

На основе полученных КВК и ВВК с эталонными термами формируют $T=ВЖ/max_{ВВК}$, текущие значения КВК относительно ВВК для заданных моментов времени, используя статистические данные и кусочно-линейные функции [2]. Для построения модели идентификации атак применяют величины термов М («молодой»), СР («средний»), СТ («старый») и формируют текущие нечеткие числа КВК(М), КВК(СР), КВК(СТ). Полученные нечеткие числа характеризуют текущее состояние виртуального канала в данный момент времени. Для построения текущего состояния ВК используют различные методы построения функций принадлежности [1-6]. Это дает возможность использовать различные исходные данные (статистические данные, опрос, назначение параметров и т.д.).

Полученное нечеткое число с помощью функции упорядочения [2,3] сравнивают с эталонными НЧ. Эталоны и текущее НЧ представляют в $\alpha-$ уровневом виде и аппроксимируют до значений, которые имеют минимальное количество точек пересечения.

На основе результата выполнения функции упорядочения, делают вывод о возможности сканирования портов (низкая, средняя, высокая и т.д.) в данный момент времени. После чего делают вывод, каков уровень защищенности локальной вычислительной сети организации. Таким образом, логико-лингвистический подход используют для повышения эффективности технологий в системах выявления атак.

Для достижения поставленной цели исследования решены следующие задачи:

1) Разработан программный модуль, реализующий построение функций принадлежности, обладающий достоинствами:

- возможность обработки исходных данных, представленных в различной форме (статистические данные, опрос, назначение параметров и т.д.);
- построение функций принадлежности различными методами.

2) Разработано программное обеспечение, реализующая модель идентификации атак на примере виртуального канала, обладающего достоинствами:

- возможность выбора метода построения функций принадлежности при построении текущего состояния;
- возможность анализа уровня защищенности виртуального канала;
- графическое представление результатов анализа.

Список литературы

1. Сваровский С. Т. Аппроксимация функций принадлежности значений лингвистической переменной // Мат. вопр. анализа данных. - Новосибирск: ВЦ СО АН СССР - 1980. - С. 127-131.
2. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. -320с.
3. Борисов А. Н, Крумберг О. А., Федоров И. П. Принятие решений на основе нечетких моделей. Примеры использования. - Рига: Зи-натне, 1990. - 184 с.
4. А. Н. Аверкин, И. 3. Батыршин, А. Ф. Блишун и др. Нечеткие множества в моделях управления и искусственного интеллекта // Под ред. Д. А. Поспелова. - М.: Наука, 1986. - 312 с.
5. Ротштейн А. П. Интеллектуальные технологии идентификации. - Винница: "Универсум Винница ", 1999. - 320 с.
6. Ротштейн А. П., Штовба С. Д. Нечеткая надежность алгоритмических процессов. - Винница: Континент-ПРИМ, 1997. - 142 с.

МЕТОД ОПРЕДЕЛЕНИЯ УРОВНЯ ЗРЕЛОСТИ ОРГАНИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Типичной компанией, внедряющей систему управления информационной безопасностью (далее СУИБ), как правило, является та, которая либо сама имеет большие объемы информации, либо вынуждена управлять ею по поручению своих клиентов. Но есть и такие организации, где вопросам зашиты информации уделяется совсем мало внимания, а в некоторых не уделяется вообще. Поэтому очень важно для организации определить к какому уровню зрелости в области информационной безопасности (далее ИБ) оно относится, для того чтобы затем сформировать нормативно-методическую базу, необходимую для нормального функционирования СУИБ, определить состав отдела защиты информации и средства обеспечения безопасности IT-систем.

Современные методы определения уровней организационной зрелости [1] и уровней

зрелости IT-инфраструктуры предприятия [2] предусматривают пять таких уровней.

Суть предлагаемого метода определения уровня зрелости организации в области информационной безопасности в том, что для определения используются соответствующие критерии и характеристики:

1. наличие средств защиты информации;
2. наличие персонала ответственного за защиту информации;
3. наличие документов регламентирующих информационную безопасность;
4. наличие системы управления информационной безопасностью;
5. наличие системы управления качеством информационной безопасности.

В соответствии с критериями оценки организация относится к одному из пяти, предусмотренных методом, уровней.

Уровень первый (хаос). Этот уровень присущ большинству начинающих и малых компаний. Ведение бизнеса здесь носит хаотичный характер, что напрямую связано с борьбой за выживание. В компании, как правило, отсутствует стратегия развития: основное внимание уделяется решению сиюминутных тактических задач.

Одной из характерных черт начального уровня организационной зрелости являются спонтанные информационные связи в компании, которые аккумулируются в руководящем звене и носят в основном справочный характер. Через этот уровень проходят все предприятия и организации — кто быстрее, кто медленнее — но в конечном итоге они подступают вплотную к следующему уровню.

Необходимо отметить, что средств защиты информации нет, работы с персоналом в области информационной безопасности не ведутся, документы, регламентирующие защиту, отсутствуют. СУИБ и система менеджмента качества также отсутствуют.

Второй уровень (фрагментарная защита). На этом уровне зрелости в компании уже возможна успешная реализация задуманных проектов, что достигается благодаря жесткому управлению, оперативному планированию и контролю. Основные бизнес-процессы становятся повторяемыми и управляемыми, они приобретают устойчивый характер. Для организаций, находящихся на этом уровне, характерна автоматизация базовых составляющих, таких как кадры, бухгалтерия, зарплата.

В компании начинают формироваться корпоративные традиции и культура, однако по-прежнему отсутствует интеграция информации, а сами информационные потоки остаются неформализованными. Уже фрагментарно используются средства защиты информации, назначены ответственные за защиту, формируются отдельные документы, регламентирующие информационную безопасность предприятия. СУИБ и система менеджмента качества отсутствуют.

Третий уровень (системная защита). На этом уровне процессы (как в управлении, так и в производстве) становятся формализованными и настолько повторяемыми, что их можно описать и задокументировать. В компаниях появляются описания ролевых функций сотрудников внутри организации или список задач, которые должен выполнять сотрудник внутри того или иного подразделения.

Все процессы стандартизированы, документированы и объединены в общий информационный поток. Благодаря этому в организации появляется возможность анализа информации по всем аспектам управленческой деятельности, а также получения оперативной информации о степени использования ресурсов. Сформирована служба защиты информации. Используются сертифицированные средства защиты, объединенные в систему. Деятельность по защите регламентирована нормативными документами. СУИБ и система менеджмента качества отсутствуют.

Для предприятий, находящихся на этом уровне, характерно формирование стратегии развития. Как только такие решения начинают приниматься на основе анализа, это означает, что предприятие переходит на следующий этап зрелости.

Четвертый уровень (управляемая защита). Здесь приоритетным направлением становится повышение качества продукции или предоставляемых услуг, а целью —

достижение рыночной привлекательности и увеличение доли рынка, т. е. именно то, к чему стремится любая компания, добивающаяся успеха в том сегменте рынка, где она работает. В организации формируются внутрикорпоративные стандарты качества, касающиеся не только собственной продукции или процессов производства, но и всей цепочки поставки — от партнеров (контрагентов) до клиентов.

Наличие и сохранение постоянных клиентов дает возможность долгосрочного планирования бизнеса и прогнозирования будущих продаж. В компании налажены стратегические и оперативные взаимосвязи, а для принятия решений активно используются обратные связи, в частности данные от клиентов. Попытки принимать решения не только на основе анализа предыдущего опыта, но и на основе прогнозов будущего развития, стратегическое планирование с учетом тенденций (для чего необходимы корпоративные базы знаний) обуславливают постепенный переход организации на последний, высший уровень организационного развития.

На данном этапе средства защиты функционируют полноценно, а именно – построена на предприятии комплексная система защиты информации, которая создает условия надежной и безопасной работы посредством применения комплекса мер защиты, которые отвечают главным требованиям:

- успешно отражать большую часть вероятных атак;
- при существенных нарушениях нормального функционирования, которые могут возникать при внешних воздействиях разного рода (в том числе, и в результате реализованных атак) система должна иметь способность либо к полному самовосстановлению, либо к восстановлению за нормативные сроки и с минимальными потерями;
- при построении системы должно соблюдаться оптимальное соотношение (цена системы)/вероятные потери.

Персонал, ответственный за защиту информации, имеет специальную подготовку, образование и/или переподготовку. Очень важно отметить тот факт, что внедрена СУИБ на основе ISO/МЭК 17799 [3].

Пятый уровень (управление качеством). Достичь этого уровня чрезвычайно трудно, и удается это лишь немногим компаниям, лидирующим в индустрии. Здесь управление качеством по количественным показателям происходит по всей цепи взаимосвязанных процессов. Для организации характерно не только построение стратегических планов, но и оптимизация путей их достижения. Стратегия компании направлена на достижение организационного, финансового, технологического преимущества.

Современный этап развития управленческой культуры характеризуется развитием коллективной обработки и анализа информации и переходом:

- от анализа количественных показателей к качественному анализу;
- от оперативного анализа к стратегическому планированию;
- от единоличного анализа и принятия решений к коллегиальной работе.

Это означает, что чем выше требования к эффективности бизнеса компании, тем выше должны быть требования к используемым в ней информационным технологиям и сложнее системы, построенные на их основе. Помимо того, что функционирует комплексная система защиты информации на предприятии, персонал, ответственный за защиту информации, имеет специальную подготовку, внедрена система управления информационной безопасности на основе ISO/МЭК 17799, обязательно должна быть построена система менеджмента качества информационной безопасности на основе ISO/МЭК 27001. Это будет говорит о том, что предприятие в своем развитии достигло высокого уровня.

Таким образом, для трех последних уровней зрелости компании — такие бизнес-задачи, как достижение успеха, увеличение доли на рынке, улучшение отношений с заказчиками, контроль затрат, являются первоочередными. Для того чтобы компания могла успешно решать эти задачи и добиваться успеха в своем бизнесе, она должна правильно и эффективно использовать информацию о протекающих процессах и внешней среде.

Все функции управления в организации осуществляются путем анализа, обработки и передачи информации. Поэтому информация становится таким же производственным ресурсом, как капиталовложения, человеческие ресурсы, основные фонды и пр. От того, насколько хорошо обрабатывается и используется информация, зависит успех компании.

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

Наивысший этап развития является идеалом, который доступен лишь лидерам, поэтому в современных условиях предприятие (и это особенно важно для российских компаний) должно стремиться обеспечить условия для функционирования на четвертом уровне.

Таким образом, определение степени зрелости организации – это первый шаг на пути развития организации. Появляется так называемая «прозрачность» процессов, происходящих в компании, что намного облегчает деятельность в области обеспечения информационной безопасности. А это очень важно для любой организации, которая стремится соответствовать международному уровню!

Список литературы

1. Пять уровней организационной зрелости предприятий по классификации Capability Maturity Model //http://www.microsoft.com/Rus/Business/Vision/Strategy/Levels.mspx
2. Уровни зрелости IT-инфраструктуры предприятия // http://www.iteam.ru/publications/it/section_91/article_3182/
3. ISO/IEC 17799:2005 «Информационные технологии – Методы и средства обеспечения безопасности – Практические правила управления информационной безопасностью».

РАЗРАБОТКА СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КРИПТОСТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ

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

В распределенных системах передачи информации одной из важнейших является задача обеспечения конфиденциальности информации. Для решения этой задачи, как правило, используют различные методы криптографической защиты. Однако криптографическая защита сама по себе не является достаточной для обеспечения секретности информации, поскольку зашифрованное сообщение будет легко обнаружено. Необходимо не только зашифровать, но и сокрыть зашифрованную информацию, для чего можно использовать методологию компьютерной стеганографии, представляющую собой технику сокрытия некоторой секретной информации в больших информационных массивах таким образом, чтобы непосвященный наблюдатель не мог заметить существование этой информации.

Методология компьютерной стеганографии основана на замене несущественных или неиспользуемых массивов данных компьютерных файлов необходимой конфиденциальной информацией. В результате обработки файла-оригинала методами стеганографии получают файл, сохраняющий свое функциональное назначение, практически не отличимый от оригинала, но содержащий секретную информацию, что позволяет идентифицировать принадлежность этого файла или передать секретную информацию.

Анализ тенденций развития компьютерной стеганографии показывает, что в ближайшие годы интерес к ее использованию будет усиливаться. Предпосылки к этому уже сформировались сегодня. В частности, общеизвестно, что актуальность проблемы

информационной безопасности постоянно растет и стимулирует поиск новых методов защиты. Объединение методов компьютерной стеганографии и криптографии позволяет устранить их слабые стороны и разработать более эффективные новые нетрадиционные методы обеспечения информационной безопасности.

В данной работе рассматривается криптостеганографическая система, которая представляет собой сложный комплекс, общая стойкость которого намного выше, чем стойкость составляющих его криптографической и стеганографической подсистем. Большую роль для надежности всей системы играет правильное согласование всех компонентов и точное следование всем заданным ограничениям.

Криптографический модуль позволяет обезопасить информацию пользователя от раскрытия ее содержания в случае извлечения сообщения. Также при шифровании изменяются статистические характеристики сообщения, повышается его энтропия. Сообщение становиться более похожим на случайные данные с распределением близким к распределению в пустом контейнере, и что наиболее важно именно шифрование не позволяет противнику однозначно установить факт передачи информации.

В ходе выполнения работы был проведен анализ современных симметричных криптографических алгоритмов, что позволило принять оптимальное решение по выбору алгоритмов шифрования. В данной системе используются стандарты шифрования ГОСТ 28147-89 и AES(Rijndael). Проведенное сопоставление параметров этих алгоритмов показало, что, несмотря на существенное различие в архитектурных принципах, их основные рабочие параметры сопоставимы. По ключевым, для алгоритмов такого рода, параметрам криптостойкости ни один из алгоритмов не обладает существенным преимуществом. Из сказанного можно сделать вывод, что оба алгоритма шифрования соответствует требованиям, предъявляемым к современным шифрам, и будут использоваться еще достаточно долгое время.

В качестве стеганографического алгоритма в работе используется адаптивный алгоритм минимизации ошибки замены наименее значащих битов (A– MELSBR), который реализует наиболее прогрессивную модель встраивания информации в изображения.

Данный алгоритм позволяет, встраивать максимальный объем данных, но при этом не изменяет статистических характеристик изображения. Он является модификацией о алгоритма минимизации ошибки замены наименее значащих битов (MELSBR).

Цвет пикселя в 24-битном цветном изображении представляется интенсивностью каждого из цветовых компонентов, которая имеет 256 уровней. Поэтому далее будет рассматриваться 8-битное изображение, имеющее 256 уровней интенсивности оттенков серого.

Под ошибкой замены понимается — расхождение значения интенсивности пикселя до замены и после замены наименее значащих битов.

При встраивании k битов $(k<8)$ сообщения в пиксель, непосредственно заменяющих k наименее значащих битов пикселя, максимальная ошибка замены будет иметь величину – 2^k-1.

Из 256 уровней интенсивности серого, есть $2^{(8-k)}$ уровней с тем же значением наименее значащих k битов, как и значение очередных k битов сообщения. Чтобы снизить ошибку заменяемых битов, нужно модифицировать пиксели, для минимизации различий со встраиваемыми битами. Для этого нужно изменить $k+1$-й наименее значащий бит, и проверить ошибки замены до и после изменения. После этого для замены пикселя изображения выбирается, вариант с наименьшим расхождением с оригиналом. Рисунок 2, иллюстрирует два шага реализации алгоритма минимизации ошибки замены наименее значащих битов. Применение этого алгоритма, ограничивает максимальное расхождение с оригинальным пикселем значением до 2^{k-1}.

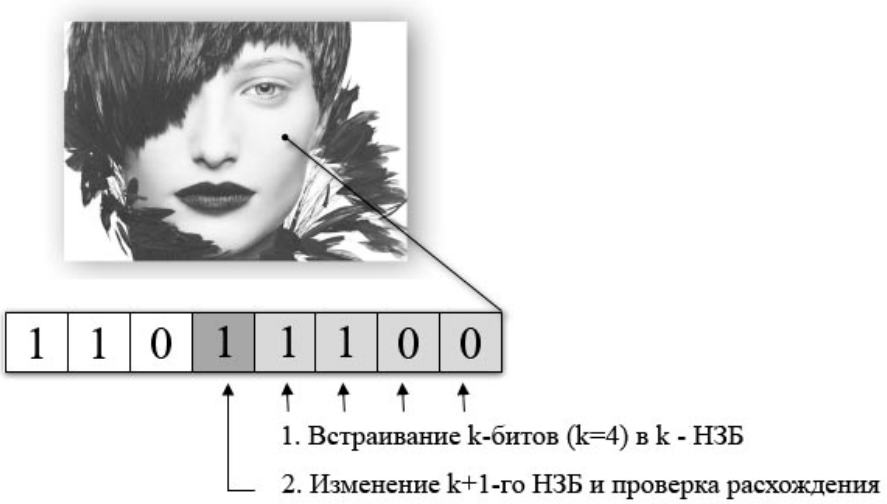

Рисунок 2 – Реализации алгоритма MELSBR.

Чтобы избежать изменения статистических характеристик изображения, сообщение должно встраиваться в определенные области каждой битовой плоскости. Данный адаптивный алгоритм, основанный на алгоритме MELSBR.

Перед встраиванием битов сообщения определяется емкость пикселя, как максимальный объем встраиваемой информации в пиксель, который не изменит статистические характеристики изображения. В пиксель встраивается определенное количество битов сообщения, которое не может превышать емкость пикселя. Такой подход позволяет избежать встраивания всего сообщения в локальную область битовой плоскости.

Данный алгоритм построен на особенности человеческого зрения, которые ранее были использованы в алгоритмах сжатия изображений с потерями, таких как JPEG.

Человеческое зрение не в состоянии определить изменение высокочастотных компонентов цвета в изображении, особенно контуров с резкими переходами цвета в изображении. Из этого свойства следует, что емкость пикселя зависит от изменения уровня интенсивности соседних с ним пикселей. На рисунке 3, показана, пространственная матрица для оценки изменения уровня интенсивности *(D)* на соседних пикселях с пикселем – *(x)*.

Рисунок 3 – Пространственная матрица для оценки изменения уровня интенсивности *(D)* на соседних пикселях с пикселем *(x)*.

Для каждого пикселя *(x)*, определяем *(D)* по формуле 1

$$D = max\{a, b, c, d\} - min\{a, b, c, d\}, \quad (1)$$

где *a, b, c* и *d* – значения интенсивностей соседних с *(x)* пикселей, их относительное расположение показано на рисунке 3.

Емкость *(K)* пикселя *(x)* определим, как минимальное количество битов, необходимое для хранения величины *(D – 1)*.

Таким образом *(K)* определяется по формуле 2:

$$K = | log2D |, \quad (2)$$

Из особенности человеческого зрения следует, что чем больше интенсивность цвета, тем меньше заметна ошибка замены. Основываясь на этом, была установлена верхняя граница емкости *(U)* для каждого пикселя, которая определяется по формуле 3:

$$U = | log2X | - 1, \quad (3)$$

где *(X)* – величина интенсивности пикселя *(x)*.

Реализация алгоритма включает следующие шаги:

1. Осуществляется проход всех пикселей изображения. Для каждого пикселя *(x)* во встраиваемой части сообщения, выполняются шаги 2-4;
2. Используя формулы (2) и (3), определяется емкость *(K)* и граница емкости *(U)* пикселя *(x)*;
3. Определяется оптимальная емкость пикселя *(x)*, как минимальное из *(K)* и *(U)*;
4. В пиксель *(x)* встраивается по алгоритму MELSBR, такое количество битов сообщения, которое не превышает оптимальной емкости пикселя.

Список литературы

1. Lee Y. K., Chen L. H., 2004, "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement", Proceedings of the Ninth National Conference on Information Security, Taiwan, 8-15 // http://debut.cis.nctu.edu.tw/Publications/

ОЦЕНКА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ НА ОСНОВЕ АППАРАТА НЕЧЕТКИХ МНОЖЕСТВ

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

Важнейшим условием эффективного и бесперебойного функционирования платежной системы Российской Федерации является обеспечение необходимого и достаточного уровня информационной безопасности (ИБ) организаций банковской системы (БС).

Особенности банковских систем таковы, что негативные последствия сбоев в работе отдельных организаций приводят к развитию системного кризиса платежной системы РФ, наносят ущерб интересам собственников и клиентов. Поэтому для организаций БС РФ угрозы ИБ, представляют реальную опасность.

Для противостояния угрозам ИБ и обеспечения эффективности мероприятий по ликвидации их влияния на операционные, кредитные и иные риски в организациях БС РФ обеспечивают и поддерживают достаточный уровень ИБ.

В настоящее время оценка уровня ИБ организации, его сопоставление с объективно необходимым уровнем, а в случае их несоответствия – подбор оптимального комплекса средств и мероприятий по повышению информационной безопасности – представляет собой сложную научно-практическую задачу.

Анализ работ [1-5] позволяет выделить четыре группы моделей оценки уровня ИБ:

1) модели, основанные на определении вероятности реализации угроз, а также уровней их ущерба;

2) имитационные и ситуационные модели;

3) вербальные модели;

4) модели, основанные на нечетких множествах.

Первую группу моделей оценки уровня информационной безопасности базируют на определении вероятности реализации угроз, а также уровней их ущерба. В данном случае значение риска вычисляют отдельно для каждой угрозы и в общем случае представляют как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяет собственник информационного ресурса, а вероятность атаки вычисляет группа экспертов.

При расчете значений вероятности проведения атаки, а также уровня возможного ущерба используют статистические методы, методы экспертных оценок или элементы теории принятия решений.

Применение статистических методов не всегда возможно из-за отсутствия в полном объёме статистических данных о ранее проведённых атаках на информационные ресурсы объекта информатизации, аналогичных тем, которые выступают в качестве объекта оценки [1,2]. Методы экспертных оценок и теории принятия решений отличает не всегда оправданный субъективизм оценок и сложность алгоритмов обработки результатов группы экспертов [3].

Вторую группу моделей базируют на организации процесса определения уровня информационной безопасности путем попыток преодоления защитных механизмов системы специалистами, выступающими в роли злоумышленников (специалисты в области ИБ наивысшей квалификации). Данный подход к оценке эффективности позволяет получать объективные данные о возможностях существующих механизмов защиты, но требует высокой квалификации исполнителей и больших материальных и временных затрат.

Третья группа моделей позволяет установить уровень ИБ путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности. Основным недостатком моделей данной группы является невозможность определения эффективности конкретного механизма защиты, так как констатируют лишь факт его наличия или отсутствия. Этот недостаток в какой-то мере компенсируют заданием достаточно подробных требований к механизмам защиты.

Четвертую группу моделей базируют на использовании аппарата нечетких множеств [4].

Банком России разработана методика оценки уровня ИБ организаций БС РФ [6], основанная на определении степени соответствия организации требованиям стандарта Банка России [7]. Анализ данной методики показывает, что ее применение имеет ряд ограничений:

1. Жесткая привязка к оцениваемым показателям (требованиям ИБ), т.е. изменение проверяемых требований приводит к необходимости модификации методики оценки.

2. Получаемые исходные данные (ИД) для оценки представляют в качественной, нечеткой форме и, следовательно, используемые в методике жесткие критерии оценки показателей ИБ приводят к сокращению информативности результата оценки.

3. Важность выполнения конкретных требований определяют использованием коэффициентов значимости, которые приведены в приложении методики. Данный аспект ограничивает возможность учета особенностей функционирования организаций БС.

Целью исследования является анализ возможностей использования нечетких моделей оценки уровня ИБ [4] в качестве альтернативы методики Банка России.

Нечеткие модели основаны на логико-лингвистическом подходе и операциях нечеткой арифметики. При данном подходе решение основывают на знаниях экспертов и связывают с высокой трудоемкостью процедур анализа и зависимостью конечного результата от субъективных факторов.

В зависимости от способа представления ИД, формата ИД и необходимого быстродействия выбирают нечеткую модель с лингвистической (НМЛШ) или бальной

шкалой (НМБШ). НМЛШ позволяет строить отношения между оцениваемыми параметрами в лингвистическом измерении, а НМБШ реализует непосредственно количественную оценку на непрерывной, вариативной балльной шкале. Модель с балльной шкалой менее наглядная и точная, но более быстродействующая.

В результате применения нечетких моделей получают лингвистическую форму уровня безопасности, которая соответствует эталонным значениям, принятым в зависимости от характеристик оцениваемой комплексной системы защиты информации (КСЗИ). Эксперты определяют эталонные значения и изменяют их в целях получения необходимой точности оценки уровня ИБ или в зависимости от условий функционирования организации БС РФ.

Методы нечеткой математики позволяют качественно оценивать эффективность существующих механизмов защиты. Среди основных недостатков в применении этих методов считают следующий: решение задач на нечетких множествах есть также нечеткое решение (множество) [5].

Для достижения поставленной цели исследования были решены следующие задачи:

1) Разработан программный модуль, осуществляющий выполнение нечетких арифметических операций, обладающий следующими достоинствами:

– возможность обработки различных классов нечетких чисел;

– выбор определенных методов обработки нечетких чисел, позволяющий регулировать информативность результата и скорость выполнения нечетких арифметических операций.

2) Разработано программное обеспечение, реализующее нечеткую модель с лингвистической шкалой, обладающее следующими достоинствами:

– возможность редактирования базы требований по обеспечению ИБ;

– определение коэффициентов важности выполнения конкретных требований (в зависимости от вероятности реализации потенциальных угроз) используя метод относительного ранжирования;

– возможность выбора контрмер для повышения текущего уровня ИБ.

Анализ результатов позволил сделать следующие выводы:

– изменение проверяемых требований не приводит к необходимости модификации модели оценки;

– экспертное определение важности выполнения конкретных требований дает возможность учета особенностей функционирования организаций БС РФ;

– возможность модификации параметров, на основании которых производят оценку уровня ИБ, а также методов осуществления операций нечеткой арифметики позволяет регулировать точность оценки уровня ИБ и адаптировать ее к изменяющимся условиям функционирования банка.

Список литературы

1. Герасименко В.А. Проблемы зашиты данных в системах их обработки //Зарубежная радиоэлектроника. 1989. N12. С. 15-20.
2. Мельников В. В. Защита информации в компьютерных системах. -М.: Финансы и статистика; Электроинформ, 1997. - 368 с.
3. Хоффман Л. Дж. Современные методы защиты информации: Пер. с англ. / Под ред. В. А. Герасименко. - М.: Сов. радио, 1980. – 264 с.
4. А.Г. Корченко. Построение систем защиты на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. – 320 с., ил.
5. Методы робастного, нейро-нечеткого и адаптивного управления: Учебник/Под ред. Н.Д. Егупова; издание 2-ое, стереотипное. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – 744 с., ил.
6. Стандарт Банка России СТО БР ИББС-1.0-2006.
7. Стандарт Банка России СТО БР ИББС-1.2-2007.