СЕКЦИЯ

ЗАЩИТА ИНФОРМАЦИИ

Руководители – с.н.с. к.т.н. **ЛАВРУХИН Ю.Н.,**
д.т.н., профессор **СУХАРЕВ Е.М.**

КОМПЛЕКСНАЯ АУТЕНТИФИКАЦИЯ СООБЩЕНИЙ, ПЕРЕДАВАЕМЫХ ПО КОРПОРАТИВНЫМ КАНАЛАМ РАДИОСВЯЗИ

Саликов А.Г., Исаева Т.А., Амчиславский А.Ю.

Серпуховской военный институт ракетных войск, Серпухов

Вопросы обеспечения информационной безопасности сообщений передаваемых по различным каналам связи в силу ряда причин как технического, так и организационного характера продолжают оставаться весьма актуальными. Указанное в полной мере относится и к корпоративным сетям связи, ибо существующий арсенал технических средств перехвата, а также и навязывания ложных сообщений [1, 2] достаточно совершенен и вполне доступен для конкурентов и иных заинтересованных в получении конфиденциальной информации неавторизованных лиц (злоумышленников). Применение известных апробированных протоколов и схем аутентификации безусловно позволяет выявить ложные сообщения и ложных абонентов, но лишь при том условии, что конфиденциальные компоненты указанных протоколов и схем остались таковыми в течении всего цикла информационного обмена. В противном случае используемые в настоящее время механизмы аутентификации в значительной степени теряют свою эффективность [3, 4]. Кроме того, наличие большого количества ложных сообщений ведёт к перегрузке программно-аппаратного модуля аутентификации, что равносильно блокированию информационной подсистемы (проблема «информационного мусора»).

В качестве одного из возможных направлений повышения эффективности процедур аутентификации можно рассматривать подход связанный с введением дополнительных компонентов в общий протокол аутентификации. Указанные компоненты должны с одной стороны позволять осуществлять предварительную отбраковку ложных сообщений внедряемых в корпоративную сеть извне, тем самым снижая нагрузку на программно-аппаратный модуль осуществляющий процедуру криптографической аутентификации, а с другой стороны должны увеличивать достоверность процедуры аутентификации. Таким образом дополнительные компоненты протокола необходимо связать с конкретными техническими параметрами радиоэлектронных средств, используемых при формировании сигнально-кодовых конструкций применяемых для передачи сообщения в соответствующем радиоканале корпоративной сети с учётом текущей электромагнитной обстановкой в точке приёма.

Под комплексной аутентификацией сообщения будем понимать сложный протокол включающий в свой состав один из стандартных криптографических протоколов аутентификации [3, 4], процедуру радиомониторинга корпоративных каналов радиосвязи [5], алгоритм формирования допусков на технические параметры используемых в корпоративных каналах радиосвязи сигнально-кодовых конструкций и протокол параметрической идентификации абонента корпоративной сети связи. Один из возможных вариантов построения процедуры комплексной аутентификации для верификатора представлен на рис. 1.

Его суть заключается в следующем. Специальное радиоприёмное устройство помимо приёма сообщений осуществляет анализ помеховой обстановки на частотах выделенных для радиоканалов корпоративной сети. Результатом указанного радиоконтроля являются уровни помех. Кроме того, подсистема радиоконтроля осуществляет измерение принятого набора индивидуальных технических параметров излучений радиоэлектронных средств претендента. С помощью алгоритма формирования допусков осуществляется определение полей допусков на отклонения от усреднённых значений выделенного набора технических параметров с учётом текущего уровня помех на выделенной рабочей частоте корпоративного радиоканала. Протокол параметрической идентификации на основе сформированного поля допусков на контролируемые технические параметры излучения и результатов измерения аналогичного набора технических параметров излучений формирует признаки принадлежности сообщения на сигнальном уровне претенденту в форме «не норма», «норма», «неопределённость». В случае получения по результатам параметрической идентификации реше-

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

ния «не норма» реализуется браковка принятого сообщения. В случае получения по результатам параметрической идентификации решения «норма» для принятого сообщения, то реализуется стандартный протокол криптографической аутентификации и в случае его успешного прохождения сообщение выдаётся пользователю. Если протокол криптографической аутентификации дал отрицательный результат, то принятое сообщение бракуется. принятого сообщения. В случае получения по результатам параметрической идентификации решения «неопределённость» для принятого сообщения, то реализуется стандартный протокол криптографической аутентификации, либо усиленный (более мощный) протокол криптографической аутентификации и в случае его успешного прохождения сообщение выдаётся пользователю с признаком не полностью гарантированной аутентичности.

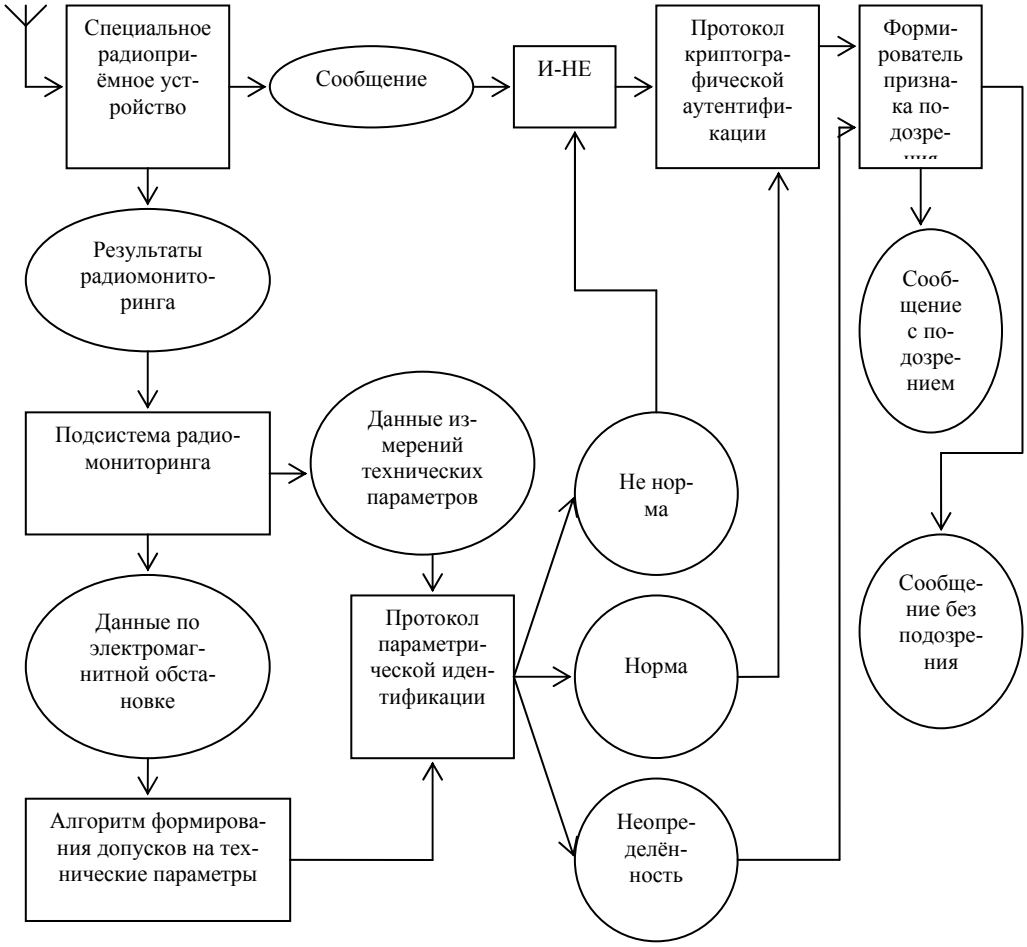


Рис. 1. Вариант протокола комплексной аутентификации сообщения

Для оценки эффективности предложенного варианта реализации комплексной аутентификации могут быть использованы подходы, изложенные в [5].

Литература

1. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь!- М.: НОУ ШО «Баярд», 2004.-432 с.
2. Торокин А.А. Основы инженерно-технической защиты информации. - М.: Издательство «Ось-89» , 1998. -336с.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия - Телеком, 2000. – 452 с.
4. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

5. Злобин В.И., Данилюк С.Г. Принципы построения сложных адаптивных систем в связи и управлении. – МО РФ, 1998. –296 с.

COMPLEX AUTHENTIFICATION OF THE MESSAGES SENT ON CORPORATIVE CHANNEL RADIO COMMUNICATION

Salickov A., Isaeva T., Amchislavskiy A.

Serpukhov Military Institute of Rocket Forces

The considered procedure to complex authentification of the messages sent on corporative channel radio communication.

ПОДХОДЫ К АВТОМАТИЗИРОВАННОЙ ОЦЕНКЕ ЭФФЕКТИВНОСТИ СРЕДСТВ ВЕРИФИКАЦИИ ИСХОДНЫХ ТЕКСТОВ ПРОГРАММ

Юдичев Р.М.

В\ч 32382

В критических областях человеческой деятельности все шире внедряются различные средства комплексной автоматизации информационного обмена. Но темпы внедрения ограничиваются необходимостью повышения степени доверия к используемому программному обеспечению. Данная проблема на практике решается как путем выбора между открытым или проприетарным программным обеспечением, так и сертификацией программного обеспечения по требованиям безопасности, включающей как функциональное тестирование исполняемых файлов в составе программных продуктов в предполагаемой операционной среде, так и логико-аналитические методы исследования их исходных текстов. В данной работе рассматривается процесс анализа исходных текстов на отсутствие в них негативных и недекларированных функциональных возможностей. Наличие широкого спектра утилит, осуществляющих различные алгоритмы проверки исходных текстов программного обеспечения, а также необходимость организовать исследование исходных текстов в промышленных масштабах ставит проблему выбора адекватных задаче средств, которые могут дать максимальную отдачу при минимуме затраченных ресурсов, то есть стоит проблема оценки эффективности процессов анализа исходных текстов с учетом принципиальной достижимости целей анализа разнородными средствами анализа.

В качестве демонстрации разнородности методов анализа можно привести следующее множество методов выявления НФВ (негативных функциональных возможностей) и НДВ (недекларированных возможностей) в исходных текстах:

- синтаксический анализ корректности исходных текстов (в основном выполняется компиляторами);
- семантический анализ;
- поиск по шаблонам уязвимостей и критических синтаксических, семантических и прагматических конструкций;
- построение/визуализация/экспорт/импорт графа управления;
- построение/визуализация/экспорт/импорт графа связей по данным;
- выделение критических маршрутов передачи управления;
- окрестностный анализ исходных текстов приложения;
- верификация моделей программ;
- построение и анализ блок-схем программ.

Особую актуальность проблема оценки эффективности приобретает также в связи с переходом процессов исследования исходных текстов программного обеспечения систем защиты информации с методов, описанных в РД Гостехкомиссии [1], на методологию Общих критериев (ОК) [2], представленную ОУД (оценочными уровнями доверия). В частности, в работе дается краткий обзор возможностей существующих инструментальных средств поддержки процесса анализа исходных текстов программного обеспечения с точки зрения соответствия реализованных в них методов подходу ОК (ОУД). Анализаторы исходных текстов ранжированы в соответствии со степенью формализованности реализованных в них методов анализа (аналогично ранжированию ОУД в ОК). Дополнительным критерием классификации служит предельный уровень автоматизации действий анализатора по сформированным экспертам шаблонам поведения. Актуальность данной функции определяется необходимостью накопления и использования опыта эксперта, а также превышением сроков оценки продуктов ИТ над периодом разработки новых их версий [3] и потребностью в повышении временной эффективности средств автоматизации процесса оценки.

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

Предлагается оценивать эффективность средств верификации исходных текстов программ с позиций качественной оценки степени достижимости целей верификации. Данный подход позволит выбирать оцененные средства верификации исходных текстов по степени соответствия цели оценки (требуемому ОУД). Решение о выборе средств верификации может приниматься также с учетом перспектив верификации на более строгие ОУД, для чего может потребоваться применение более формальных методов верификации, но, возможно, с учетом текущих невысоких требований к гарантиям, детальность верификации может быть сознательно (и обоснованно) снижена. Такой подход позволит, при инициировании работ по сертификации на более высокий ОУД, использовать в качестве опорных предыдущие результаты оценки, что снизит как материальные, так и временные затраты на сертификацию.

Неотъемлемой частью модели оценки эффективности является информационная "отрицательная обратная связь" по результатам эксплуатации верифицированных продуктов с целью скорректировать прогнозные оценки эффективности различных методов с учетом реально обнаруженных уязвимостей безопасности верифицированных программ. В настоящее время активно разрабатываются и внедряются система "bug-tracking'a" – автоматизированного сбора и обработки отчетов об ошибках от членов команды тестировщиков и конечных пользователей программных продуктов. Посильной задачей представляется встраивание в данные системы модуля сопоставления места обнаруженной ошибки в программном коде системы с картой покрытия кода тестами в процессе верификации и обнаружения коллизий между результатами тестов и работы пользователей. Системы оповещения об ошибках, встроенные в типовые системы bug-tracking'a, должны содержать в списках оповещения как членов команды разработчиков кода системы, так и членов команды верификации.

По получении качественных оценок достижимости целей верификации программ на заявленный ОУД может возникнуть ситуация выбора конкретного средства автоматизации среди элементов класса однотипных программных средств различных производителей. Данная проблема решается в предлагаемой модели оценки эффективности применением механизма специализированных тестов производительности – benchmark'ов – учитывающих конкретные показатели быстродействия (скорости анализа), совместимость форматов данных, актуальную для достижения повторяемости результатов,

Литература

1. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. М.: Гостехкомиссия России, 1999.
2. ГОСТ Р ИСО/МЭК 15408-32002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
3. Общие критерии оценки безопасности информационных технологий: Учебное пособие. Перевод с английского Е.А. Сидак / Под ред. М.Т. Кобзаря, А.А. Сидака. – М.: ЦБИ, 2001.

Questions of the automated rating of efficiency programs for verification source code of programs are considered.

СПОСОБ ПРИМЕНЕНИЯ ХАОТИЧЕСКИХ СИГНАЛОВ В УГЛОМЕРНОЙ НАВИГАЦИОННОЙ СИСТЕМЕ

Беспалов Е.С., Мусянков М.И., Родичев П.В.

Московский государственный институт радиотехники, электроники и автоматики
(технический университет)

Известно применение хаотических сигналов (например, в системах радиосвязи) для скрытной передачи информации [1,2]. В настоящее время продолжается поиск новых направлений использования таких сигналов с целью обеспечить скрытность для других радиотехнических систем, в частности, для навигационных.

В данной работе исследована возможность скрытной передачи информации в угломерной навигационной радиотехнической системе – системе MLS [3].

Рассмотрен вариант системы MLS, в котором для передачи информации об угле (например, об азимуте) наземный передатчик модулируется по частоте поднесущим колебанием, а мгновенное значение частоты поднесущей- F зависит от мгновенного значения угла:

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

$$F = A + B \cdot \theta, \tag{1}$$

где: θ - мгновенное значение угла в градусах; $A = 110$ кГц; $B = 500$ Гц /градус.

Это – вариант системы MLS с плавным качанием узкого луча антенны, имеющего в плоскости качания ширину 1…2 градуса. При максимальных углах качания $\pm 60^0$ частота поднесущей изменяется в интервале от 80 до 140 кГц [3].

Скрытность передачи угломерной информации в такой системе может быть обеспечена с помощью хаотической манипуляции частотой F, причём, в случае применения для манипуляции маркированных хаотических последовательностей, удаётся сохранить возможность определения угла. При такой манипуляции система становится аналогом системы MLS с ступенчатым качанием луча [3]. При облучении объекта, решающего навигационную задачу, в приёмнике этого объекта фиксируется от 8-и до12-ти значений поднесущей частоты.

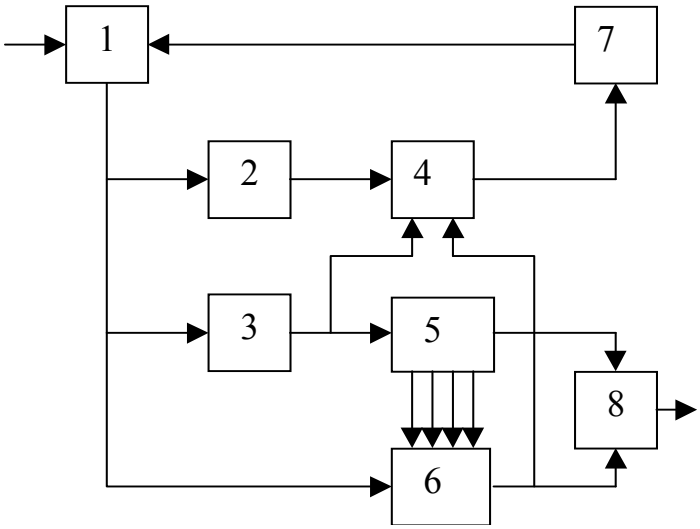


Рис.1

Структурная схема устройства фильтрации, используемого в приёмнике для выделения информации об угле, изображена на рис.1. Основой схемы устройства является схема фазовой синхронизации, синтезированная в [4] и предназначенная для оптимальной фильтрации сигнала, модулированного по частоте узкополосным процессом.

Устройство содержит: фазовый детектор – 1; низкочастотный канал фильтрации – 2; блок запуска – 3; сумматор – 4; генератор опорных поднесущих частот – 5; квадратурный фильтр поднесущих – 6; подстраиваемый генератор – 7; блок анализа и принятия решения – 8.

Известное начальное значение частоты генератора 5 устанавливается по сигналу, излучаемому широким лучом антенны наземного передатчика. Ширина диаграммы направленности этой антенны превосходит ширину сектора качания узкого луча. Сигналу запуска соответствует заранее согласованное значение поднесущей частоты, и на это значение настроен блок запуска 3. Опорные колебания для квадратурного фильтра 6 вырабатываются генератором 5. Алгоритм формирования последовательности частот этого генератора совпадает с алгоритмом формирования последовательности поднесущих частот в наземном передатчике. Номера элементов последовательности поднесущих частот принятого сигнала и соответствующие этим номерам значения углов определяются в блоке 8.

При синтезе значений поднесущих частот в рассматриваемой системе можно использовать целый ряд известных алгоритмов формирования маркированных хаотических числовых последовательностей $\{X_n\}$, в частности, алгоритм, опубликованный в [5]:

$$X_n = \left(\frac{4kn}{1+kn}\right) \cdot X_{n-1}(1 - X_{n-1}), \tag{2}$$

где: n - номер ступени угла (аналог номера ступени при ступенчатом качании луча); k - постоянная, определяемая из условий сохранения хаотического режима.

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

Сформировав в приёмнике последовательность значений поднесущих частот, после приведения этих значений к интервалу (0,1) получают последовательность чисел $\{X_n^*\}$ и рассчитывают порядковые номера принятых элементов этой последовательности. Как и в случае ступенчатого качания луча, используют связь между номером ступени и углом. Номер ступени в соответствии с (2) рассчитывают по формуле:

$$n = b/\{k[4a(1-a)-b]\}, \text{ где: } a = X_{n-1}^*; b = X_n^*. \quad (3)$$

Рассмотренный способ обепечивает возможность решения навигационной задачи и в то же время повышает скрытность передачи сигналов навигационной системы.

Литература

1. Дмитриев А.С., Панас А.И., Старков С.О. Динамический хаос как парадигма современных систем связи // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники, 1997, №10.- С.4 –26.

2. Капранов М.В., Кулешов В.Н., Ларионова М.В., Морозов А.Г., Удалов Н.Н. Свойства систем передачи информации с манипуляцией параметрами и начальными условиями генераторов хаотических колебаний // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники,2000, №11.- С.48-59.

3. СВЧ система инструментальной посадки самолётов (реферат) // Зарубежная радиоэлектроника, 1972, №11.- С.3-21.

4. Беспалов Е.С., Кулешов В.Н. Оптимальная нелинейная фильтрация сигнала, модулированного по фазе или частоте узкополосным случайным процессом // Изв. вузов – Радиоэлектроника, 1979, т.22, №7.- С.11-17.

5. Беспалов Е.С., Мусянков М.И., Родичев П.В. Маркированные хаотические последовательности на основе алгоритма Ферхюльста. В кн.: 5-ая Международная конференция и выставка “Цифровая обработка сигналов и её применение”. Доклады –2.- М.: ИПРЖР, 2003.- С. 483-485.

THE APPROACH FOR APPLICATION OF CHAOTIC SIGNALS AT ANGLE METER NAVIGATION SYSTEM

Abstract. The approach for application of chaotic signals at navigation angle meter system is proposed. The application of the marked chaotic sequences based on Verhulst’s algorithm are considered.

БЕЗОПАСНОСТЬ ПРИМЕНЕНИЯ И ВНЕДРЕНИЯ СИСТЕМ РАДИОИДЕНТИФИКАЦИИ

Дорохин В.И.

Московский технический университет связи и информатики
111024, Россия, Москва, Авиамоторная, 8а

В связи с тенденцией повсеместного внедрения технологий радиоидентификации растет угроза безопасности пользователей систем, основанных на этой технологии.

Задача радиоидентификатора – на расстоянии передать считывающему устройству некоторые данные, на основании которых может быть определена личность, баланс банковского счета, принадлежность, например, к некоторой социальной категории граждан, право на пользование услугой или право прохода, принадлежность транспортного средства или другой собственности тому или иному владельцу, цена на товар. Кроме того, радиоидентификаторы применяются в грузовых и почтовых перевозках для учета или сортировки товара, на складах, а так же для определения подлинности. Это далеко не все области применения технологии радиоидентификации, однако уже сейчас можно представить себе возможный ущерб от внедрения в систему идентификации злоумышленника.

Можно выделить несколько участков системы, через которые возможна атака. Рассмотрим сначала один из вариантов построения системы (Рис. 1). В поле действия каждого считывателя может попасть как один, так и несколько идентификаторов. Один или несколько считывателей подключаются к терминалу. Обычно такое соединение проводное, и осуществляется посредством интерфейса RS-232, RS-422, RS-485 или USB. Терминалы объединены в локальную сеть, через которую они связываются с сервером, обслуживающим базу данных (БД).

Радиометки, попадая в поле действия считывателя, по его запросу должны выдать заложенную в них информацию по радиоканалу. Считыватель может разрешать ситуации, когда несколько меток одновремен-

но попадают в поле его действия. В большинстве систем реализован протокол обнаружения и разрешения коллизий. Суть его работы заключается в перезапросах считывателя таким образом, чтобы радиометки отвечали по очереди, в соответствии с алгоритмом.

Терминал может иметь обратную связь со считывателем для блокировки доступа или выполнения других действий с носителем радиометки. Так, например электронный замок получает команду от терминала на открытие или закрытие и т.п.

Терминалы соединены в локальную сеть, в которой так же присутствует сервер базы данных (БД). В БД может храниться например необходимая информация для определения прав доступа обладателя радиометки, цены товара с такой меткой, состоянии банковского счета и т.п. Обычно это высокопроизводительный компьютер, способный обрабатывать большой поток запросов от терминалов.

Одно из уязвимых мест в системе – радиоканал между считывателем и меткой. В отличие от контактных идентификаторов, диалог между радиометкой и считывателем можно прослушать, что следует учитывать при разработке протокола обмена. Перехват диалога позволяет получить информацию, хранящуюся в памяти идентификатора.

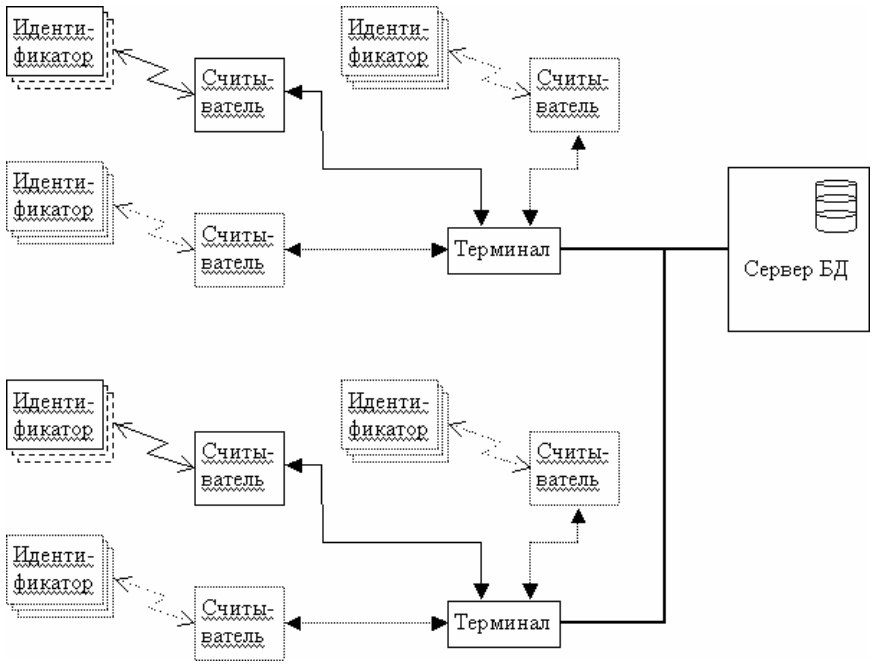


Рис. 1. Система радиочастотной идентификации.

Доступ к информации на таких радиометках может осуществляться хакером прямо в магазине - при помощи карманного компьютера, дополненного специальным модулем и программой для работы с ним. Таки образом можно менять цену товара, заменив его код кодом более дешевой вещи, а несовершеннолетние хакеры смогут покупать алкоголь или иные обычно недоступные им товары. Подобные атаки мошенников в последнее время заметно участились в крупных супермаркетах, в которых хорошо развита система радиоидентификационного контроля товаров. Так же не последнюю роль сыграло появление в сети Интернет программного обеспечения, для перепрограммирования радиоидентификаторов с карманного компьютера. То есть, фактически эту операцию может произвести любой желающий. Решить эту проблему частично помогает разработанная технология двойной идентификации. Когда метка кодируется, на нее автоматически вводится код дистрибьютора (при этом оператор не знает используемого кода). Считыватели, поставляемые перепродавцом, также обладают этим кодом, внедренным в микропроцессорное обеспечение. Когда считыватель читает метку, производится сверка кодов; если соответствия не обнаружено, считыватель не производит обработки данных, и защищенность метки сохраняется. Таким образом, держатель метки из другой системы, или злоумышленник, не знающий кода, не может получить доступа к данной системе. Радиометка «не позволит» себя перепрограммировать или считать данные без предъявления ей этого кода.

Такое решение, одновременно позволяет решить и задачу различения своих и чужих радиометок, так как без такой защиты считыватели в магазине могли бы реагировать, к примеру, на пластиковые карточки в кармане покупателей или иные распространенные радиоидентификаторы. Так же снижается возможность отслеживать перемещения товаров конкурирующими структурами.

Другая проблема - нарушение конфиденциальности рядовых пользователей: борцы за права человека настаивают на том, чтобы при выходе из магазина память радиометок очищалась. В некоторых супермарке-

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

тах внедрена система «глушения» радиометки. Специальная метка наклеивается на пакет для покупок и считыватель уже не может определить, какие именно товары попали в радиус его действия. Тем не менее, считыватель определяет их наличие. Таким образом, злоумышленнику не удастся вынести товар незамеченным.

Другой заметной уязвимостью является локальная сеть, обеспечивающая доступ терминалов к БД. Получение злоумышленником доступа к серверу БД через локальную сеть, грозит нарушением всей системы целиком, не говоря уже о больших возможностях осуществления разных манипуляций с самими объектами контроля. Как правило, при небольших масштабах радиоидентификационной системы, для нее проще использовать локальную сеть, отдельную от той, где происходит общий информационный обмен внутри организации. При объединении этих двух сетей возникает необходимость уделять гораздо большее внимание безопасности сервера БД, разграничению прав доступа, а так же архитектуре сети в целом. При обеспечении корректной работы сети не следует забывать о ее производительности. Снижение скорости доступа терминалов к серверу БД замедлит работу всей системы в целом.

Практически не подвергаются атакам злоумышленников пожалуй только линии, связывающие терминал со считывателем. Обычно длина этого соединения невелика и оно находится на виду у оператора. Если же это не так, то линии соединения следует уделить такое же внимание, как и остальным уязвимым местам системы.

Пожалуй, главным уязвимым местом системы идентификации, как и любой другой, является человеческий фактор. Ошибка оператора, или ошибка при проектировании или конфигурировании системы обслуживающим персоналом может породить различные уязвимости.

Нельзя забывать и про нестандартные способы атак на систему, различные вариации которых ограничены только фантазией злоумышленника. Так например, для получения персональных данных держателя кредитной банковской карты банкомат оборудовался злоумышленниками фальш-панелью с органами управления (клавиатура для ввода персонального кода), и устройством чтения данных с карты. Получение этих данных позволяло несанкционированно распоряжаться банковским счетом.

SAFETY OF APPLICATION AND INTRODUCTION OF SYSTEMS OF RADIOIDENTIFICATION

Dorokhin V.

Moscow Technical University of Communication and informatics
111024, Russian Federation, Moscow, Aviamotornaya st., 8a

This report considerate the safety issues arising at introduction and use of systems of radio-frequency identification. As an example the general scheme of radio-frequency identification is considered. In this scheme the attention is given to the weak places, malefactors potentially subject to attack. Including features of the report of an exchange of the radioidentifier with the input reader are considered, one of which allow to be protected from attacks, and others on the contrary - are subject to attacks. Thus in clause the question of human rights directly connected to a problem of identification on distance, and as ways of struggle against a dishonest competition is mentioned. It is marked, that at growth of scales of system more careful approach to a question of a safety, both from the technical party is required, and on the part of the attendants.

ПСЕВДОСЛУЧАЙНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ ЦЕЛЫХ ЧИСЕЛ, ФОРМИРУЕМАЯ АЛГОРИТМОМ С ЗАПАЗДЫВАНИЕМ, КАК МАРКОВСКИЙ ПРОЦЕСС

Колесов В.В.

Институт радиотехники и электроники РАН
125009, Москва, центр, ГСП-9, ул. Моховая, д.11, корп. 7

Проблема защиты информации в открытых информационных и компьютерных сетях от несанкционированного доступа, а также задача повышения помехоустойчивости телекоммуникационных каналов связаны с применением сложных кодирующих алгоритмов и шумоподобных сигналов с большой информационной емкостью. Поэтому разработка сложных кодирующих алгоритмов и критериев объективной оценки их статистических свойств является достаточно актуальной задачей.

В качестве тестируемого алгоритма рассмотрен алгоритм с запаздыванием на основе отображения типа Фибоначчи. Для ограничения области определения алгоритма конечным замкнутым целочисленным интервалом [1, M], M>1 отображение дополнено операцией преобразования интервала [1, M] самого в себя с "отражающими границами":

$$\tilde{x}_n = x_{n-1} + (-1)^{x_{n-Kz}} \cdot x_{n-Nz}, \quad Kz \in [2,\ Nz-1], \quad x_n \in [1,\ M]$$
$$x_n = \tilde{x}_n, \quad если \quad \tilde{x}_n \in [1,\ M] \qquad (1)$$
$$x_n = \tilde{x}_n - M, \quad если \quad \tilde{x}_n > M$$
$$x_n = \tilde{x}_n + M, \quad если \quad \tilde{x}_n < 1$$

Здесь Nz - параметр запаздывания, он определяет размерность фазового пространства и радиус-вектора $R_n(x_{n-1},x_{n-2},\dots x_{n-Nz})$ состояния данной дискретной динамической системы (ДДС) в этом пространстве. Число возможных состояний в ФП конечно и равно M^{Nz}. В зависимости от начальных условий $R_0(x_{-1}, x_{-2},\dots x_{-Nz})$ ДДС (1) на каждом шаге алгоритма описывает в ФП ту или иную "траекторию", представляющую собой последовательные дискретные переходы из одной точки состояния в другое по псевдослучайному закону (Рис.1). Из-за ограниченности объема ФП эти траектории образуют замкнутые циклы, которые, вследствие однозначности преобразования (1), не пересекаются и не имеют общих точек. Все точки ФП принадлежат только одному какому-либо циклу, либо изолированной точке с координатами (M,M,… M). Так, например, при M=5, Nz=4, Kz=3 в ФП алгоритма один 562-тактный цикл, два цикла с периодом T=27, один 8-тактный цикл и одна особая точка. При Nz=5, Kz=3 и M=13 (M^{Nz}=371293) в ФП существуют циклы с периодами T=332373, 21721, 7966, 4959, 3640, а при Nz=6, Kz=4 и M=15 один "длинный" цикл с периодом T=11099897 включает в себя подавляющее большинство ($0.974 \cdot M^{Nz}$) точек ФП.

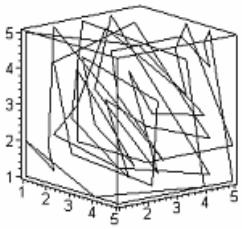


Рис.1

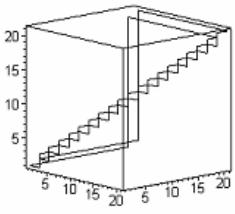


Рис.2

Циклы алгоритма (1) имеют важную отличительную особенность: поведение динамической системы на цикле до его замыкания (а нас будут интересовать процессы именно до замыкания цикла) имеет случайный, хаотический характер (Рис.1), а порождаемая при этом алгоритмом непериодическая последовательность $\{x_n\}$ – псевдослучайного типа. Множество точек состояний динамической системы в ФП, объединенных в такой цикл, назовем псевдослучайным циклом. В отличие от регулярного цикла, которому до замыкания цикла соответствует регулярное движение в фазовом пространстве. Пример простого регулярного цикла ($x_n=x_{n-3}+2$ с преобразования интервала [1,21] в себя) приведен на Рис.2. Таким образом, псевдослучайный цикл представляет собой конечное множество внешне хаотически, но строго детерминированным образом следующих одна за другой точек состояний дискретной динамической системы в фазовом пространстве алгоритма.

Для практических применений наибольший интерес представляют непериодические псевдослучайные последовательности большой длины. При надлежащем выборе параметров алгоритма (1) и начальных условий сегмент непериодической ПСП, формируемой алгоритмом на псевдослучайном цикле до выхода системы на период, может быть произвольно большой длины и, как показал анализ, по своим статистическим свойствам близок к последовательности с равномерным распределением вероятностей генерируемых чисел p(x). Так при интервале области определения алгоритма [1,63] (M=63) и запаздывании Nz=3 длина непериодической ПСП равна $N=7.8317 \cdot 10^4$, при Nz=5 $N=3.3174 \cdot 10^8$, при Nz=7 $N=1.676 \cdot 10^{12}$, при Nz=9 длина непериодической ПСП более $5 \cdot 10^{12}$.

Отметим, что дискретная ПСП с дискретными числами $\{x_n\}$ по своему виду близка к последовательности испытаний классической теории вероятностей. Каждый переход в этой последовательности от числа x_n к следующему числу x_{n+1}, равным образом, как и к числу x_{n+s} через s шагов алгоритма, полностью определен вследствие детерминированности и однозначности процесса (1). Тем не менее, для внешнего наблюдателя он ничем не отличается от процесса случайных испытаний. Абстрагируясь поэтому от детерминированности процесса (1), покажем, что формируемая им последовательность при должном выборе параметров алгоритма может быть очень близкой к случайной последовательности марковского типа и, более того, к случайной последовательности независимых равновероятных событий.

Как известно, марковский процесс - это процесс без вероятностного последействия, когда условная вероятность для всех $t>t_0$ однозначно определяется значением x_0, принятым в момент t_0 и не зависит от предшествующей истории. Для дискретной последовательности с дискретными значениями x_n – простой цепи Маркова это означает, что существует вероятность $p(x_j, n \mid x_i, k)$ перехода от любого из значений процесса x_i при k-ом испытании к любому значению x_j при n-ом испытании (n>k, i,j=1,2,…M) [1]. В частном случае последовательности независимых испытаний вероятность перехода в состояние x_j совпадает с вероятность этого состояния при n-ом испытании $p(x_j, n \mid x_i, k)=p(x_j)$ независимо от результатов других испытаний. Для

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

однородной цепи Маркова вероятности переходов зависят только от числа шагов s=n–k между испытаниями $p(x_j, n \mid x_i, k) = p(x_j, \mid x_i, s)=p_{ij}(s)$. Величины $p_{ij}(s)$ образуют матрицу $\boldsymbol{\pi}_s$ вероятностей перехода за s шагов. Для однородной цепи должно выполняться соотношение (уравнение Маркова) [1]: $\boldsymbol{\pi}_s = (\boldsymbol{\pi}_1)^s$, т.е. вероятности перехода за s шагов выражаются через вероятности перехода за один шаг.

Обратимся к алгоритму (1). На первый взгляд последовательность, формируемая этим алгоритмом с запаздыванием, не является процессом без последействия. Более того, каждое новое значение ПСП определяется предысторией из принятых на предыдущих этапах Nz значений запаздывания. С другой стороны, операция "преобразования числового интервала самого в себя" как бы разрывает эту связь (не нарушая однозначности процесса в прямом направлении, но делая его необратимым) при каждом выбросе нового числа за границы интервала [1,M]. Проверим поэтому, насколько справедливо ли соотношение $\boldsymbol{\pi}_s = (\boldsymbol{\pi}_1)^s$ для ПСП, формируемой алгоритмом (1). То есть, установим, в какой степени эта последовательность отвечает уравнению Маркова? Предположение об однородности процесса $\{x_n\}$ вполне естественно, если имеется предварительная информации о близости распределения вероятности p(x) к равномерному.

Для наглядности результатов численный эксперимент проведем для алгоритма (1) с небольшими значениями параметров, но с наличием в ФП псевдослучайного цикла с периодом, достаточным для генерации непериодической последовательности с числом членов N, обеспечивающим необходимый для статистической обработки массив. Положим M=3, Nz=9, Kz=5, т.е. у алгоритма 9-мерное фазовое пространство и область определения из трех чисел. В этом случае в ФП существует длинный цикл с периодом T=19677 при полном объеме ФП, равном M^{Nz}=19683. Распределение вероятностей чисел p(x) в последовательности, генерируемой алгоритмом, практически равномерное со среднеквадратичным отклонением от этого закона, равным $4.8\cdot10^{-5}$, и максимальным отклонением по модулю $6.8\cdot10^{-5}$.

На основе реализации сформированной алгоритмом ПСП длиной N=19677 определим вероятности P(A) генерации числа x_i (i=1,2,…M) путем подсчета осуществленных наступлений события A, равного $n(x_i)$: $P(A)= n(x_i)/N$. Следуя определению условной вероятности по Колмогорову: $P(B \mid A)=P(AB)/P(A)$, где P(AB) - вероятность одновременного осуществления событий A и B. Подсчитаем в реализации из N испытаний количество $n(x_j, x_i, s)$ одновременно наступивших событий A (генерация числа x_i) и B (переход от этого числа через s шагов алгоритма к числу x_j). Тогда вероятность $P(AB)= n(x_j, x_i, s)/(N-s)$, а условная вероятность $P(B \mid A)=[n(x_j, x_i, s)/(N-s)]/[n(x_i)/N]= p_{ij}(s)$. Матрица переходов $\boldsymbol{\pi}_s = \| p_{ij}(s) \|$. Для последовательности независимых равновероятных событий все $p_{ij}(s)=1/M$ и соответствующую матрицу вероятностей переходов обозначим через $\boldsymbol{\pi}_0$.

При анализе реализации ПСП длиной N=19677 получены следующие матрицы перехода:

$$\boldsymbol{\pi}_1=\begin{pmatrix} 0.33335 & 0.33335 & 0.33335 \\ 0.33325 & 0.33340 & 0.33340 \\ 0.33320 & 0.33350 & 0.33320 \end{pmatrix}, \boldsymbol{\pi}_2=\begin{pmatrix} 0.33321 & 0.33352 & 0.33337 \\ 0.33326 & 0.33342 & 0.33342 \\ 0.33315 & 0.33337 & 0.33321 \end{pmatrix}, \boldsymbol{\pi}_{20}=\begin{pmatrix} 0.33321 & 0.33382 & 0.33382 \\ 0.33342 & 0.33357 & 0.33372 \\ 0.33330 & 0.33367 & 0.33376 \end{pmatrix}.$$

Установление одного этого факта, что все вероятности переходов $p_{ij}(s)= p(x_j, \mid x_i, s)=p(x_j, n \mid x_i, k)$ существуют, уже достаточно, чтобы считать этот процесс марковским [1]. Кроме того, мы видим, что все элементы матриц очень близки к равновероятному значению $p_{ij}=1/M=1/3$. При этом, поскольку сумма элементов каждой строки матриц $\boldsymbol{\pi}_s$ равны единице, то эти матрицы являются стохастическими [2]. Наибольшее отличие эвклидовых норм матриц $\boldsymbol{\pi}_s$ от единицы составило величину, меньшую 10^{-5}.

Оценку справедливости равенства (2) для исследуемой ПСП проведем на основе вычисления среднеквадратичного отклонения элементов матриц $\boldsymbol{\pi}_s$ и $(\boldsymbol{\pi}_1)^s$:

$$y_S = \sqrt{(1/M^2)\sum_{i,j=1}^{M}(p_{i,j}(s) - p_{i,j}^{(s)}(1))^2} = (1/M)\cdot\|\Delta p_S\|,$$

где $\|\Delta\boldsymbol{\pi}_s\|$ - эвклидова норма матрицы $\Delta\boldsymbol{\pi}_s = \boldsymbol{\pi}_s - (\boldsymbol{\pi}_1)^s$, а $p_{ij}^{(s)}$ (1) - элементы матрицы $(\boldsymbol{\pi}_1)^s$. Полученные числовые значения σ_s построены на графике Рис.3 (кривая 1а). Мы видим, что отличия элементов матриц в левой и в правой частях (2) при всех интервалах переходов s=1,2,…20 менее $4\cdot10^{-4}$ по абсолютной величине или примерно 10^{-3} по относительному значению. Этот результат показывает, что тестируемую последовательность, формируемую алгоритмом (1) с запаздыванием, мы можем рассматривать как очень близкую к марковскому процессу. Более того, как показывает анализ близости матриц переходов $\boldsymbol{\pi}_s$ к матрице $\boldsymbol{\pi}_0 = \| p_{ij}=1/M \|$, эта последовательность при данных значениях параметров M и Nz практически не отличается от последовательности независимых равновероятных испытаний. Действительно, характеризуя отличие матриц $\boldsymbol{\pi}_s$ и $\boldsymbol{\pi}_0$ среднеквадратич-ным отклонением их элементов

$$\sigma_O = \sqrt{(1/M^2)\sum_{i,j=1}^{M}(p_{i,j}(s) - 1/M)^2} = (1/M)\cdot\|\Delta\pi_0\|,$$

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

где $\|\Delta\boldsymbol{\pi}_0\|$- норма матрицы $\Delta\boldsymbol{\pi}_0 = \boldsymbol{\pi}_s - \boldsymbol{\pi}_0$, полученные в численном эксперименте значения σ_0 для s=1,2,…20 отложим на графике Рис.3 (кривая 1б). Мы видим, что отличия элементов матриц перехода $p_{ij}(s)$ от значений 1/M при всех анализируемых переходах s не превышают уровня $5\cdot10^{-4}$ или в относительном выражении около 0.1%.

Аналогичные вычисления выполнены при анализе матриц переходов для ПСП алгоритма (1) с параметрами M=9, Nz=9, Kz=5, т.е. с областью определения из девяти чисел и ФП объемом 387420489 точек состояний. Длина исследуемой реализации ПСП с начальным вектором $R_0(1,1,\ldots1)$ выбиралась равной N=180000. Распределение вероятностей генерируемых чисел p(x) близко к равномерному со среднеквадратичным отклонением от этого закона, равным $6.42\cdot10^{-4}$, и максимальным отклонением по модулю $1.45\cdot10^{-3}$. Отличия элементов матриц переходов $\boldsymbol{\pi}_s$ и $(\boldsymbol{\pi}_1)^s$, а также матриц $\boldsymbol{\pi}_s$ и $\boldsymbol{\pi}_0$ демонстрируют графики 2а и 2б на Рис.3. Величины среднеквадратичного отклонения, как это следует из построенных зависимостей, находятся на уровне $\sigma=2\cdot10^{-3}$, т.е. менее 1% по относительной величине. Это свидетельствует также в пользу принятия заключения о близости сформированного псевдослучайного процесса к цепи Маркова и к последовательности независимых равновероятных испытаний.

Кривые 3а и 3 б на Рис.3 относятся к случаю ПСП, сформированной алгоритмом (1) при следующих параметрах: M=9, Nz=5, Kz=3. От предыдущего случая этот вариант отличается меньшей величиной запаздывания. В ФП алгоритма представлены циклы с периодом T=55070, 3230, 260, 130, 50. Для численного анализа взят самый длинный псевдослучайный цикл с начальным вектором $R_0(1,1,\ldots1)$. Длина исследуемой реализации ПСП равна N=55070. Распределение вероятностей генерируемых чисел p(x) близко к равномерному со среднеквадратичным отклонением от этого закона $7.3\cdot10^{-4}$, и максимальным отклонением по модулю $1.05\cdot10^{-3}$, что практически не отличается от степени близости к равномерному распределения генерируемых чисел в предыдущей тестируемой последовательности.

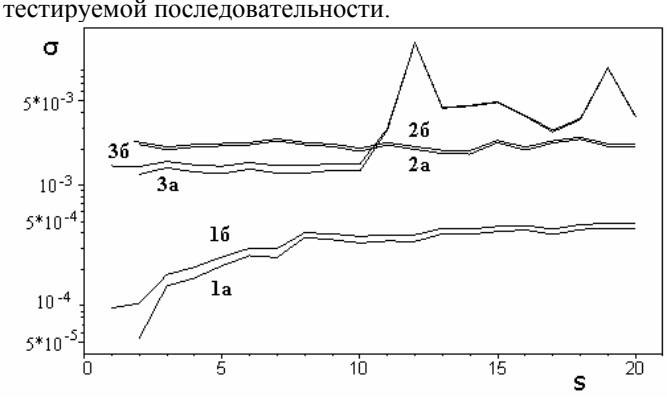


Рис.3.

Действительно, как показали исследования, функция распределения вероятностей по мере увеличения параметра запаздывания, а, значит, размерности алгоритма, имеет тенденцию к улучшению, т.е. приближению к равномерному закону, но при Nz порядка 6 и более плотность распределения p(x) практически не отличается от этого закона. Как свидетельствует ход кривых 3а и 3б матрицы переходов $\boldsymbol{\pi}_s$ и $(\boldsymbol{\pi}_1)^s$, а также матрицы $\boldsymbol{\pi}_s$ и $\boldsymbol{\pi}_0$ мало отличаются на интервалах переходов s=1,2… 10, но на больших интервалах s=12, 13… отличия в матрицах возрастают до единиц процентов. Этот компьютерный эксперимент подтверждает, что для оценки ПСП как близкой к последовательности независимых испытаний знания о равномерности распределения вероятностей появления чисел p(x) еще не достаточно. Важно, чтобы были равномерными и все распределения условных вероятностей $p(x_j, n \mid x_i, k)$. Сопоставление хода графиков 2 и 3 на Рис.3 показывает, что увеличение запаздывания от значения Nz=5 до Nz=9 приводит к улучшению статистических характеристик формируемого алгоритмом псевдослучайного процесса, приближая их к характеристикам цепи Маркова и последовательности независимых равновероятных событий.

Заметим, что определение матриц вероятностей переходов при больших значениях параметра M требует обработки больших числовых массивов, поэтому для экспресс-анализа статистического качества формируемых ПСП вполне приемлемо, как известно, построение упрощенных матриц переходов, информирующих лишь о том, отличны от нуля вероятности перехода $p_{ij}(s)$ или же нет. Построение таких матриц возможно при анализе реализаций не обязательно большой длины. При этом не все ячейки матриц могут оказаться правильно заполненными: при больших значениях M и недостаточной длине N анализируемой ПСП ($N<s\cdot M^2$) такая матрица доже для процессов со всеми $p_{ij}(s)$ отличными от нуля имеет вид "звездного неба". Тем не менее, последовательное по номеру s рассмотрение вида матриц переходов $p_{ij}(s)=,\neq0$ дает важную информацию о качестве исследуемого дискретного процесса.

Процесс с запаздыванием– это процесс с последействием. Однако введение в алгоритм операции преобразования интервала [1,M] в себя разрывает это последействие на каждом шаге, когда число x_n выходит за границы этого интервала. При этом формируемую алгоритмом (1) псевдослучайную последовательность

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

при надлежащем выборе параметров алгоритма можно рассматривать фактически как процесс без последействия, т.е. как простую однородную цепь Маркова с вероятностями переходов $p_{ij}(s) \approx 1/M$. Показано, что при соответствующем выборе параметров алгоритма и начальных условий, при которых отличие матриц переходов $\boldsymbol{\pi}_s$ и $(\boldsymbol{\pi}_1)^s$ становится заметным, статистические свойства генерируемой ПСП ухудшаются по сравнению с чисто случайным процессом, даже если при этом распределение вероятностей p(x) практически равномерное.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проекты № 03-07-90133, № 04-07-90161, № 04-07-08013.

Литература

1. Рытов С.М. Введение в статистическую радиофизику –М.: Наука. 1966.
2. Гантмахер Ф.Р. Теория матриц – М.: Наука. 1966.

The analysis of the discrete dynamic system behavior on the basis of Fibonacci- type mapping with delay and with operation of the interval transformation of the definitional domain into itself with reflecting border was carried out. It was shown that formed at that the pseudorandom integer-valued process at suitable choice of parameters was possible to consider as uniform Markov chain with probability transitions corresponding to random sequence of the independent equiprobable tests.

УЧЕТ ВЕРОЯТНОСТНЫХ ФАКТОРОВ ПРИ ПЛАНИРОВАНИИ ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАТИВНЫХ СИГНАЛОВ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

Иванов С.М., Самсонов А.А, Симанькин Ю.Н.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, Воронеж

Основным содержанием организационных мероприятий по защите информации (ЗИ) информативных сигналов радиоэлектронных средств (РЭС) является введение запретов или ограничений (энергетических, пространственных или иных) на излучения РЭС в течение периодов времени нахождения в зоне его энергетической доступности средств несанкционированного добывания информации (СНДИ) в радио – и радиотехническом диапазонах (РРД).

По своему назначению можно выделить текущее и перспективное планирование организационных мероприятий по ЗИ от СНДИ в РРД. В рамках текущего планирования (на ближайшую перспективу проводимых работ) необходимо обоснованно определить состав вводимых ограничений и границы временного интервала (интервалов), в течение которого данные ограничения должны действовать. При перспективном (долгосрочном) планировании в интересах обоснования комплекса мероприятий по ЗИ на объекте, необходимо оценить объем задач ЗИ от СНДИ в РРД, которые могут быть решены организационными мероприятиями.

В настоящее время определение границ временных интервалов проведения организационных мероприятий в процессе текущего и перспективного планирования осуществляется без учета вероятностных факторов, существенно влияющих на продолжительность безопасной работы РЭС (т.е. интервалов времени, в течение которых в зоне энергетической доступности РЭС отсутствуют СНДИ) и продолжительность выполнения работ, связанных с излучениями РЭС. В результате возрастает вероятность возникновения ситуации, когда защищаемый сигнал РЭС может вскрываться (обнаруживаться и анализироваться) СНДИ, что приводит к снижению эффективности организационных мероприятий по ЗИ.

Для исключения таких ситуаций в рамках текущего планирования моменты времени появления СНДИ в зоне энергетической доступности РЭС и выхода из данной зоны, а также продолжительность выполнения работ, связанных с излучениями РЭС, необходимо рассматривать как случайные величины с определенными средними значениями и дисперсией. В качестве одного из основных требований к организационным мероприятиям необходимо рассматривать выполнение следующего неравенства:

$$1-\left[1-P\left\{t_1^{НДИ} < t_1^{ОМ}\right\}\right]\cdot\left[1-P\left\{t_2^{НДИ} > t_2^{ОМ}\right\}\right]\cdot\left[1-P\left\{T_{техн} < T_{БР}\right\}\right] > \xi\,, \qquad (1)$$

где $t_1^{НДИ}$, $t_2^{НДИ}$ - соответственно моменты времени входа и выхода СНДИ в зону энергетической доступности РЭС;

$t_1^{ОМ}$, $t_2^{ОМ}$ - соответственно моменты времени начала и окончания организационных мероприятий;

$T_{техн}$, $T_{БР}$ - соответственно продолжительность интервала времени, необходимого для проведения работ, связанных с излучением РЭС и продолжительность интервала времени безопасной работы РЭС (с момента начала работ, связанных с излучением РЭС);

$P\left\{t_1^{НДИ} < t_1^{ОМ}\right\}$ - вероятность того, что СНДИ войдут в зону энергетической доступности РЭС до начала проведения организационных мероприятий;

$P\left\{t_2^{НДИ} > t_2^{ОМ}\right\}$ - вероятность того, что СНДИ не выйдут из зоны энергетической доступности РЭС к моменту окончания проведения организационных мероприятий;

$P\left\{T_{техн} > T_{БР}\right\}$ - вероятность того, что потребная продолжительность работ, связанных излучением РЭС, превысит продолжительность интервала времени безопасной работы РЭС;

ξ - пороговое значение вероятности невыполнения условий, обеспечивающих эффективность организационных мероприятий по ЗИ от СНДИ в РРД, принимающее значение в диапазоне $\xi = 0{,}05 - 0{,}1$.

Входящие в выражение (1) вероятности определяются по следующим выражениям:

$$P\left\{t_1^{НДИ} < t_1^{ОМ}\right\} = \int_{\left(m_1^{НДИ} - 4\sigma_1^{НДИ}\right)}^{t_1^{ОМ}} \omega_1^{НДИ}(\tau)d\tau,$$

$$P\left\{t_2^{НДИ} > t_2^{ОМ}\right\} = \int_{t_2^{ОМ}}^{\left(m_1^{НДИ} + 4\sigma_1^{НДИ}\right)} \omega_2^{НДИ}(\tau)d\tau, \qquad (2)$$

$$P\left\{T_{техн} > T_{БР}\right\} = \int_{T_{БР}}^{(m_{техн} + 4\sigma_{техн})} \omega_{техн}(\tau)d\tau,$$

где $\omega_1^{НДИ}(\tau)$ - нормальная плотность распределения вероятности (ПРВ) момента времени входа СНДИ в зону энергетической доступности РЭС с математическим ожиданием и среднеквадратическим отклонением (СКО) соответственно $m_1^{НДИ}$ и $\sigma_1^{НДИ}$;

$\omega_2^{НДИ}(\tau)$ - нормальная ПРВ момента времени выхода СНДИ из зоны энергетической доступности РЭС с математическим ожиданием и СКО соответственно $m_2^{НДИ}$ и $\sigma_2^{НДИ}$;

$\omega_{техн}(\tau)$ - нормальная ПРВ продолжительности работ, связанных с излучением РЭС, с математическим ожиданием и СКО соответственно $m_{техн}$ и $\sigma_{техн}$.

Математические ожидания и СКО входа СНДИ в зону энергетической доступности РЭС и выхода из данной зоны должны определяться по результатам обработки статистических данных по функционированию различных видов СНДИ в районе размещения РЭС. Математическое ожидание и дисперсия продолжительности интервала времени, необходимого для проведения работ, связанных с излучением РЭС, должны определяться с учетом количества отдельных выполняемых в рамках данных работ этапов (технологических операций) по следующим выражениям:

$$m_{техн} = \sum_{f=1}^{F} m_f \;,\; \sigma_{техн} = \sqrt{\sum_{f=1}^{F} \sigma_f^2} \;, \qquad (3)$$

где F - количество отдельных этапов (технологических операций);

m_f, σ_f - соответственно математическое ожидание и СКО продолжительности отдельных этапов, определяемые по результатам обработки статистических данных по времени выполнения данных операций.

Использование выражений (1) … (3) позволит свести к минимуму вероятность возникновения ситуаций, когда защищаемый сигнал РЭС может вскрываться (обнаруживаться и/или анализироваться) СНДИ.

При перспективном (долгосрочном) планировании в рамках оценки объема задач по ЗИ от СНДИ в РРД, которые могут быть решены организационными мероприятиями, необходимо корректно оценить вероятность решения задач ЗИ с учетом следующих основных условий реализуемости организационных мероприятий:

- график появления СНДИ в зоне энергетической доступности РЭС должен быть известен;
- продолжительность периодов времени отсутствия средств СНДИ в зоне энергетической доступности РЭС должна превышать требуемую длительность излучения РЭС в соответствии с содержанием и объемом проводимых работ;

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

- предельно – допустимое значение паузы между излучениями РЭС, определяемое с учетом интенсивности проведения работ, должно превышать значение паузы между интервалами безопасной работы РЭС.

При проведении долгосрочных оценок детерминированные процессы появления СНДИ в зоне энергетической доступности РЭС, а также излучений РЭС трансформируются в случайные процессы с определенными вероятностно - временными характеристиками. Вследствие этого выполнение второго и третьего условий реализуемости организационных мероприятий необходимо рассматривать как вероятностные. Совместное их выполнение определяет возможность решения задач ЗИ от СНДИ в РРД за счет введения временных ограничений, а вероятность их совместного выполнения P^{vr} является выходным показателем оценки объема задач по ЗИ от СНДИ в РРД, которые могут быть решены организационными мероприятиями.

Для разработки методики оценки данной вероятности периодическую последовательность интервалов безопасной работы РЭС целесообразно представить в виде случайного импульсного потока [1], рассматриваемого как совокупный результат независимого функционирования нескольких СНДИ. При этом импульсы суммарного потока, соответствующие интервалам времени безопасного излучения РЭС, укорачиваются и дробятся по сравнению с импульсами суммируемых потоков, а паузы между импульсами наоборот – суммируются и увеличиваются. В соответствии с [2, 3], можно сделать следующие допущения относительно вероятностно - временных характеристик (ВВХ) данного потока:

- интервалы времени безопасной работы РЭС распределены следующим образом: при функционировании одного СНДИ – по нормальному закону; при функционировании 2 ... 4 СНДИ – по обобщенному распределению Эрланга вида *k(1)*; при функционировании от пяти и более СНДИ – по экспоненциальному закону;
- длительности пауз между интервалами времени безопасной работы РЭС распределены по нормальному закону;
- требуемая продолжительность излучения РЭС и максимально – допустимая длительность интервала времени между излучениями РЭС распределены по нормальному закону.

Вероятность превышения длительности интервала времени безопасной работы РЭС над требуемым временем его излучения в соответствии с [6] определяется по следующему выражению:

$$P_{t_{br}>t_i} = P\{t_{br} > t_i\} = \int_0^{\infty} \omega_{t_i}(\tau)\left[1 - W_{t_{br}}(\tau)\right] d\tau \,, \tag{4}$$

где $\omega_{t_i}(\tau)$ - ПРВ времени излучения РЭС;

$W_{t_{br}}(\tau)$ - функция распределения вероятности (ФРВ) длительности интервала времени безопасной работы РЭС.

В соответствии с обоснованными выше допущениями, ПРВ $\omega_{t_i}(\tau)$ является нормальной и определяется по следующему выражению:

$$\omega_{t_i}(\tau) = \frac{1}{\sqrt{2\pi}\cdot\sigma_{t_i}} \cdot \exp\left(-\frac{1}{2}\left(\frac{\tau - m_{t_i}}{\sigma_{t_i}}\right)^2\right), \tag{5}$$

где m_{t_i} и σ_{t_i} - математическое ожидание и СКО времени проведения работ, связанных с излучениями РЭС.

Вид ФРВ $W_{br}(\tau)$ зависит от количества функционирующих СНДИ (т.е. от количества суммируемых случайных импульсных потоков):

- при функционировании одного СНДИ:

$$W_{br}(\tau) = \frac{1}{\sqrt{2\pi}\cdot\sigma_{t_{br}}} \cdot \int_0^{\tau} \exp\left(-\frac{1}{2}\left(\frac{\tau_1 - m_{t_{br}}}{\sigma_{t_{br}}}\right)^2\right) d\tau_1 \,, \tag{6}$$

где $m_{t_{br}}$ и $\sigma_{t_{br}}$ - математическое ожидание и СКО интервала времени безопасной работы РЭС;

- при функционировании 2 … 4 СНДИ [7]:

$$W_{br}(\tau) = \frac{\lambda_1 \lambda_0^{k-1}}{(\lambda_0 - \lambda_1)^{k-1}} \int_0^{\tau} \exp(-\lambda_0 \tau) \sum_{i=k-1}^{\infty} \frac{\left[(\lambda_0 - \lambda_1)\tau\right]^i}{i!} d\tau \,, \tag{7}$$

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

где λ_0, λ_1, k - параметры обобщенного распределения Эрланга вида *k(1)*, связанные с математическим ожиданием и дисперсией интервала времени безопасной работы РЭС следующими соотношениями:

$$k = \left\langle \frac{m_r^2}{\sigma_r^2} \right\rangle, \tag{8}$$

$$\lambda_0 = \frac{m_r(k-1) + \sqrt{(k-1)^2 m_r^2 + k(k-1)(m_r^2 - \sigma_r^2)}}{(m_r^2 - \sigma_r^2)}, \tag{9}$$

$$\lambda_1 = \frac{\lambda_0}{(1 - k + \lambda_0 m_r)}, \tag{10}$$

где $\langle \bullet \rangle$ – операция округления в сторону наибольшего целого;

- при функционировании от 5 и более СНДИ :

$$W_{br}(\tau) = 1 - \exp\left(-\frac{\tau}{m_{t_{br}}}\right). \tag{11}$$

Путем подстановки получаем следующие выражения для вычисления вероятности превышения длительности интервала времени безопасной работы РЭС над требуемым временем его излучения:

- для одного СНДИ (подстановка (5) и (6) в (4)):

$$P_{t_{br}>t_i} = \frac{1}{2\pi\sigma_{t_i}\sigma_{t_{br}}} \int_0^\infty \exp\left(-\frac{1}{2}\left(\frac{\tau - m_{t_i}}{\sigma_{t_i}}\right)^2\right) \int_\tau^\infty \exp\left(-\frac{1}{2}\left(\frac{\tau_1 - m_{t_{br}}}{\sigma_{t_{br}}}\right)^2\right) d\tau_1 d\tau; \tag{12}$$

- для 2 … 4 СНДИ (подстановка (5) и (7) в (4)):

$$P_{t_{br}>t_i} = 1 - \frac{\lambda_1 \lambda_0^{k-1}}{\sqrt{2\pi}\sigma_{t_i}(\lambda_0 - \lambda_1)^{k-1}} \int_0^\infty \exp\left(-\left[\frac{1}{2}\left(\frac{\tau - m_{t_i}}{\sigma_{t_i}}\right)^2 + \tau\lambda_0\right]\right) \sum_{i=k-1}^\infty \frac{[(\lambda_0 - \lambda_1)\tau]^i}{i!} d\tau, \tag{13}$$

где λ_0, λ_1, k - параметры обобщенного распределения Эрланга вида *k(1)*, определяемые из заданных $m_{t_{br}}$ и $\sigma_{t_{br}}$ по выражениям (8) … (10);

- для 5 и более СНДИ (подстановка (5) и (11) в (1)):

$$P_{t_{br}>t_i} = \frac{1}{\sqrt{2\pi}\cdot\sigma_{t_i}} \int_0^\infty \exp\left(-\left[\frac{1}{2}\left(\frac{\tau - m_{t_i}}{\sigma_{t_i}}\right)^2 + \frac{\tau}{\bar{t}_{br}}\right]\right) d\tau \cdot \tag{14}$$

Вероятность превышения предельно – допустимого значения паузы между излучениями РЭС (определяется в зависимости от интенсивности проведения работ в рамках технологической схемы разработки образцов ВВТ) над паузой между интервалами безопасной работы РЭС определяется по следующему соотношению:

$$P_{Ti>Tbr} = P\{T_i > T_{br}\} = \int_0^\infty \text{ɑ}_{Tbr}(\tau)[1 - W_{Ti}(\tau)] d\tau, \tag{15}$$

где $P_{Ti>Tbr} = P\{T_i > T_{br}\}$ - вероятность превышения предельно – допустимого значения паузы между излучениями РЭС над паузой между интервалами безопасного излучения РЭС;

$\text{ɑ}_{Tbr}(\tau)$ - ПРВ длительности паузы между интервалами безопасного излучения РЭС, определяемая с учетом вероятностного прореживания суммарного потока функционирования СНДИ;

$W_{Ti}(\tau)$ - ФРВ предельно – допустимого значения паузы между излучениями РЭС.

В соответствии с обоснованными выше допущениями, $W_{Ti}(\tau)$ определяется по следующему выражению:

$$W_{Ti}(\tau) = \frac{1}{\sqrt{2\pi}\cdot\sigma_{Ti}} \cdot \int_0^\infty \exp\left(-\frac{1}{2}\left(\frac{\tau - m_{Ti}}{\sigma_{Ti}}\right)^2\right) d\tau, \tag{16}$$

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

где m_{Ti} и σ_{Ti} - математическое ожидание и СКО предельно – допустимого значения паузы между излучениями РЭС.

Плотность распределения вероятности появления интервалов безопасной работы РЭС $\omega_{Tbr}(\tau)$ по существу является характеристикой прореженного импульсного случайного потока функционирования совокупности СНДИ. В качестве вероятности прореживания импульсного потока в нашем случае выступает вероятность $P_{pr} = 1 - P_{t_{br} > t_i}$. Обобщив результаты, полученные в [2], на случай случайных импульсных потоков получаем следующее выражение для расчета $\omega_{Tbr}(\tau)$:

$$\omega_{Tbr}(\tau) = P_{t_{br} > t_i}\omega_{Tbr}(\tau) + \\ + \sum_{n=2}^{\infty}\left\{P_{t_{br} > t_i}\left[1 - P_{t_{br} > t_i}\right]^{n-1}\left[\omega_{Tbr}(\tau) \overset{n-1}{\oplus} \omega_{t_{br}}(\tau)\right]\right\}, \quad (17)$$

где $\omega_{Tbr}(\tau)$ - ПРВ длительности паузы между интервалами безопасной работы РЭС в исходном суммарном импульсном потоке функционирования СНДИ (т.е. до вероятностного прореживания данного потока);

$\left[\omega_{Tbr}(\tau) \overset{n-1}{\oplus} \omega_{t_{br}}(\tau)\right]$ - *(n-1)*- кратная свертка $\omega_{Tbr}(\tau)$ и $\omega_{t_{br}}(\tau)$.

В соответствии с обоснованными выше допущениями относительно ВВХ случайных величин, используемых в разрабатываемой методике, $\omega_{Tbr}(\tau)$ определяется по следующему выражению:

$$\omega_{Tbr}(\tau) = \frac{1}{\sqrt{2\pi}\cdot\sigma_{Tbr}}\cdot\exp\left(-\frac{1}{2}\left(\frac{\tau - m_{Tbr}}{\sigma_{Tbr}}\right)^2\right), \quad (18)$$

где m_{Ti} и σ_{Ti} - математическое ожидание и СКО длительности паузы между интервалами безопасной работы РЭС в исходном суммарном импульсном потоке функционирования СНДИ.

Для случая функционирования от 1 до 4 СНДИ *(n-1)*- кратная свертка ПРВ $\omega_{Tbr}(\tau)$ и $\omega_{t_{br}}(\tau)$, входящая в выражение (17), определяется как:

$$\left[\omega_{Tbr}(\tau) \overset{n-1}{\oplus} \omega_{t_{br}}(\tau)\right] = \\ = \frac{1}{2\pi(n-1)\sigma_{Tbr}\sigma_{t_{br}}}\int_0^{\tau}\exp\left(-\frac{1}{2}\left[\left(\frac{\tau_1 - (n-1)m_{Tbr}}{\sqrt{(n-1)\sigma_{Tbr}^2}}\right)^2 + \left(\frac{(\tau-\tau_1) - (n-1)m_{t_{br}}}{\sqrt{(n-1)\sigma_{t_{br}}^2}}\right)^2\right]\right)d\tau_1. \quad (19)$$

Для случая функционирования от 5 и более СНДИ *(n-1)*- кратная свертка ПРВ $\omega_{Tbr}(\tau)$ и $\omega_{t_{br}}(\tau)$ определяется следующим образом:

$$\left[\omega_{Tbr}(\tau) \overset{n-1}{\oplus} \omega_{t_{br}}(\tau)\right] = \\ = \frac{1}{\sqrt{2\pi(n-1)\sigma_{Tbr}^2}\cdot m_{t_{br}}^n\cdot(n-1)!}\int_0^{\tau}(\tau-\tau_1)^{n-1}\exp\left(-\left[\frac{1}{2}\left(\frac{\tau_1 - (n-1)m_{Tbr}}{\sqrt{(n-1)\sigma_{Tbr}^2}}\right)^2 + \frac{\tau-\tau_1}{m_{t_{br}}}\right]\right)d\tau_1. \quad (20)$$

В результате, получены все соотношения, необходимые для расчета вероятности выполнения задач ЗИ за счет введения временных ограничений на излучение защищаемых РЭС:

$$P^{vr} = P_{t_{br} > t_i}\cdot P_{Ti > Tbr}. \quad (21)$$

Таким образом, приведена методика учета вероятностных факторов при текущем и перспективном планировании организационных мероприятий по ЗИ от СНДИ в РРД, обеспечивающая требуемую эффективность ЗИ и обоснованное определение объема задач ЗИ, которые могут быть решены организационными мероприятиями.

Литература

1. Седякин Н.М. Элементы теории случайных импульсных потоков. - М: Сов. радио, 1965. - 260 с.
2. Вентцель Е.С., Овчаров Л.А. Задачи и упражнения по теории вероятностей. - М.: Высш. шк., 2000. - 366 с.
3. Тараканов К.В., Овчаров А.А., Тырышкин А.Н. – Аналитические методы исследования систем. – М.: Сов. радио, 1974. – 240 с.
4. Левин Б.Р. Теоретические основы статистической радиотехники. Книга первая. - М.:"Сов. радио", 1969. - 752 с.
5. Розанов Ю.А. Теория вероятностей, случайные процессы и математическая статистика: учебник для вузов. – М.: Наука, 1985. – 320 с.
6. Дружинин В.В., Конторов Д.С., Конторов М.Д. Введение в теорию конфликта. – М.: Радио и связь, 1974. – 240 с.
7. Иванов С.М., Язов Ю.К. Расчет распределения времени выявления сигналов средствами объективного контроля в изменяющихся внешних условиях. - Радиотехника, 1996, №6, с. 69-73.

ПРОЕКТИРОВАНИЕ СПЕЦИАЛИЗИРОВАННОЙ РАСПРЕДЕЛЕННОЙ БАЗЫ ДАННЫХ ДЛЯ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ СИСТЕМЫ ОРГАНОВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Бурушкин А.А., Головин С.А., Жилинский С.В., Затока И.В.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, Воронеж

Эффективность функционирования системы органов технической защиты информации (ТЗИ) существенно зависит от качества информационного обеспечения принятия решений по организации и проведению мероприятий по ТЗИ, что в значительной мере определяется своевременностью и полнотой сбора и обработки необходимой информации о функционировании элементов системы и условиях (обстановке), в которых решаются задачи ТЗИ. Одним из основных направлений работ по повышению качества информационного обеспечения является внедрение в деятельность органов ТЗИ современных информационных технологий, которые позволят обеспечить соответствие информационного обеспечения современному уровню развития науки и техники.

В рамках проведения работ по внедрению информационных технологий с учетом того, что формирование информационных ресурсов системы органов ТЗИ, производится территориально удаленными структурными элементами системы, а функциональные механизмы по поддержанию в актуальном состоянии данных ресурсов и обеспечению высоких требований по достоверности и безопасности их хранения и обработки в настоящее время отсутствуют, необходимо решение задачи совершенствования информационного обеспечения деятельности органов ТЗИ с использованием технологии распределенных баз данных (РБД). Все это обуславливает необходимость и целесообразность проектирования распределенной базы данных в качестве информационной основы (ядра) информационно-аналитической системы (ИАС) обеспечения деятельности системы органов ТЗИ, создание которой возможно уже в ближайшее время.

Первоочередной задачей проектирования РБД [2] является синтез логической структуры РБД (состав логических записей и структура их размещения по узлам информационно-телекоммуникационной сети (ИТКС) ИАС, структура взаимосвязей между типами логических записей, структура запросов пользователей) и обоснование ее рационального варианта.

Анализ известного методического обеспечения проектирования оптимальных структур РБД различного назначения показал, что имеющийся математический аппарат не в полной мере удовлетворяет особенностям задачи проектирования специализированной РБД в интересах совершенствования информационного обеспечения деятельности органов ТЗИ:

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

1) известные подходы к решению задач обоснования рациональных структур РБД в основном ориентированы на использование временных показателей оценки эффективности РБД. Имеются отдельные попытки рассмотрения в качестве не основных показателей таких, как достоверность и безопасность информации при ее хранении и обработке в РБД, но без учета их взаимосвязи и взаимозависимости, что неприемлемо в нашем случае, так как в процессе информационного обеспечения деятельности органов ТЗИ вопросы обеспечения достоверности информации, используемой при поддержке принятия решений по организации и проведению мероприятий по ТЗИ, а также вопросы обеспечения безопасности информации играют определяющую роль;

2) отсутствуют методы решения задач при совместном рассмотрении (с учетом взаимного влияния) временных характеристик РБД, характеристик достоверности и безопасности информации при ее хранении и обработке в РБД, которые требуют формулирования задачи обоснования рационального варианта построения РБД в многокритериальной постановке;

3) известный математический аппарат обоснования требований к логической структуре РБД не рассматривает особенности проектирования РБД на ранних стадиях создания автоматизированных информационных (информационно-аналитических) систем при неполноте исходной информации, необходимой для задания большого количества системных, сетевых и структурных ограничений. Упомянутый аппарат применим фактически только в случае, когда имеется достаточно полная информация о составе и структуре ИТКС, о характеристиках используемых технических и программных средств (сеть развернута и функционирует).

В связи с вышеизложенным актуальными являются исследования, направленные на разработку методического обеспечения обоснования эффективных решений по выбору рационального варианта построения РБД и формированию требований к основным характеристикам логической структуры РБД в условиях неполноты исходных данных о предметной области и необходимости рассмотрения множества показателей (временных, достоверности и безопасности информации), определяющих качество вариантов РБД.

В общем случае задача синтеза специализированной РБД может быть сформулирована следующим образом.

Пусть информация, добываемая и используемая должностными лицами органов ТЗИ различного уровня, структурирована и представлена в виде единого концептуального описания множества предметных областей потенциальных пользователей РБД, включающего минимально необходимый набор информационных элементов и взаимосвязей между ними, обеспечивающих полноту реализации информационных процессов в ИАС - канонической структуры РБД, которая является инвариантной к аппаратным и программных средствам ее реализации.

В интересах построения логической структуры РБД содержащиеся в канонической структуре данные (терминальные и групповые информационные элементы) отображаются в данные логического уровня РБД (логические записи). Варианты отображения канонической структуры в логическую определяют множество допустимых вариантов построения РБД [2].

Тогда логическая структура РБД представляет собой совокупность логических записей, распределенных по узлам ИТКС, топология которой задана иерархией системы органов ТЗИ и которая состоит из множества Q узлов.

Пусть имеется множество потенциальных пользователей РБД (должностных лиц органов ТЗИ), "прикрепленных" к узлам ИТКС и реализующих свои информационные потребности посредством реализации с помощью РБД множества N запросов.

Пусть имеется множество M вариантов построения (логической структуры) РБД $X=\{X_1, X_2, \ldots, X_m\}$, каждый из которых определяется некоторым планом распределения групп данных по узлам ИТКС и задается матрицей

$$X_m = \left\| x_{inj} \right\|_m, \; m = \overline{1, M},$$

где $x_{inj} = \begin{cases} 1, & \text{если } i-\text{я группа данных для реализации } n-\text{го запроса} \\ & \text{размещается на } j-\text{м узле ИТКС,} \\ 0, & \text{в противном случае,} \end{cases}$,

$n = 1, 2, \ldots, N$, $i = 1, 2, \ldots, I_N$, $j = 1, 2, \ldots, J_Q$;

n, i, j - номера запросов, групп данных и узлов ИТКС соответственно.

С учетом необходимости принятия решения по выбору рационального варианта построения РБД в нечеткой многокритериальной среде целесообразно включить в состав системы показателей эффективности вариантов построения РБД следующие показатели, сформулированные с использованием понятий и терминологии теории нечетких множеств [1]:

1) степень реализации информационных потребностей пользователей РБД с учетом общего времени обработки множества запросов пользователей РБД;

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

2) степень реализации информационных потребностей пользователей РБД с учетом достоверности информации;

3) степень реализации информационных потребностей пользователей РБД с учетом обеспечения безопасности информации.

Каждый из указанных показателей представляет собой функцию принадлежности $\mu_{\Pi_r}(X)$, r=1, 2, 3, нечеткого множества Π_r на множестве X (X={X_m}, $m = \overline{1, M}$) альтернативных вариантов построения РБД для каждого частного показателя эффективности РБД Π_1, либо Π_2, либо Π_3. В соответствии с [1] каждое нечеткое множество Π_r, r=1, 2, 3, может быть представлено с помощью совокупности пар Π_i={$\langle \mu_{\Pi_r}(X) \rangle$, X}, где $\mu_{\Pi_r}(X) : X \to [0, 1]$ - отображение множества X в единичный отрезок [0, 1] (далее функции принадлежности вида $\mu_{\Pi_r}(X)$ называются нечеткими частными показателями эффективности варианта построения РБД).

Тогда на основе введенных показателей для достижения наибольшей степени реализации информационных потребностей пользователей главный (основной) критерий выбора варианта построения РБД должен одновременно обеспечивать минимизацию общего времени обработки множества запросов пользователей (критерий C_1) и максимизацию достоверности (критерий C_2) и безопасности (критерий C_3) хранения и обработки информации в РБД (далее критерии C_1, C_2 и C_3 называются нечеткими частными критериями оптимизации варианта построения РБД).

Необходимость рассмотрения совокупности сформулированных выше частных критериев при обосновании варианта построения специализированной РБД требует выбора в качестве главного (основного) нечеткого векторного критерия оптимизации - критерия максимума степени реализации информационных потребностей пользователей РБД C(X). Этот критерий является оценкой вариантов построения РБД по совокупности нечетких частных критериев, характеризующих степень соответствия варианта X_m, ($X_m \in X$, $m = \overline{1, M}$) требованиям реализации информационных потребностей пользователей РБД с учетом общего времени обработки множества запросов пользователей, достоверности и безопасности информации (соответствие понятию, смысл которого формализуется нечетким множеством «степень реализации информационных потребностей пользователей РБД»):

$$C(X_m)=(C_1(X_m), C_2(X_m), C_3(X_m)) \to \max_{X_m}, \quad (1)$$

где $C(X_m)$ - нечеткий векторный критерий оптимизации варианта РБД, представляющий собой отображение $C(X_m)$: $X_m \to R$, R - множество действительных чисел единичного отрезка [0, 1].

В соответствии с требованиями ко времени обработки запросов пользователей, достоверности и безопасности информации из множества допустимых вариантов построения РБД X могут быть выделены соответственно множества X_T, X_D, X_B, каждому элементу которых соответствуют возможные значения общего времени обработки множества запросов пользователей (t), показателей достоверности (d) и безопасности (b) информации соответственно.

Тогда запись (1) эквивалентна следующей записи:

$$C(X_m)=(C_1(X_m), C_2(X_m), C_3(X_m)) \to \max_{X_m \in (X_T \cap X_D \cap X_B)} \quad (2)$$

а функции принадлежности $\mu_{\Pi_1}(X)$, $\mu_{\Pi_2}(X)$, $\mu_{\Pi_3}(X)$ эквивалентны функциям принадлежности $\mu_{\Pi_1}(X_T), \mu_{\Pi_2}(X_D), \mu_{\Pi_3}(X_B)$ соответственно.

Тогда с учетом вышеизложенного каждому элементу множества вариантов построения РБД X_m ($X_m \in X$, $m = \overline{1, M}$) может быть поставлена в соответствие следующая тройка:

$$X_m \leftrightarrow (t(X_m), d(X_m), b(X_m)),$$
$$t(X_m) \in T, d(X_m) \in D, b(X_m) \in B,$$

где $t(X_m)$, $d(X_m)$, $b(X_m)$ – параметры, характеризующие в совокупности m-й вариант построения РБД и определяющие для него значение общего времени обработки множества запросов пользователей, значение показателя, характеризующего достоверность информации, и значение показателя, характеризующего безопасность информации, соответственно; T, D, B - множества значений параметров $t(X_m)$, $d(X_m)$, $b(X_m)$ соответственно, характеризующие в совокупности множество доступных вариантов построения РБД.

Тогда каждой функции принадлежности $\mu_{\Pi_1}(X_m)$, $\mu_{\Pi_2}(X_m)$, $\mu_{\Pi_3}(X_m)$ можно поставить в соответствие эквивалентную функцию принадлежности $\mu_{\Pi_1}(t(X_m)), \mu_{\Pi_2}(d(X_m)), \mu_{\Pi_3}(b(X_m))$ соответственно. С учетом этого критерий (2) может быть представлен в виде:

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

$$C(X_m) \leftrightarrow (\mu_{\Pi_1}(t(X_m)), \mu_{\Pi_2}(d(X_m)), \mu_{\Pi_3}(b(X_m))) \rightarrow \max_{X_m}. \quad (3)$$

Таким образом, выбор варианта построения РБД может осуществляться на основе критерия (3), базирующегося на введенных функциях принадлежности $\mu_{\Pi_1}(t(X_m)), \mu_{\Pi_2}(d(X_m)), \mu_{\Pi_3}(b(X_m))$.

Тогда, в соответствии с [1], правило выбора рационального варианта построения РБД записывается в виде пересечения G компонентов критерия C:

$$G=C_1 \cap C_2 \cap C_3.$$

Операции пересечения нечетких множеств соответствует операция min, выполняемая над их функциями принадлежности [1]: $\mu_G(X_m) = \mu_{\Pi_1}(t(X_m)) \wedge \mu_{\Pi_2}(d(X_m)) \wedge \mu_{\Pi_3}(b(X_m))$.

Тогда в качестве рационального выбирается вариант построения РБД X_m^* ($X_m^* \in X$, $m = \overline{1, M}$), которому соответствует наибольшее значение функции принадлежности μ_G:

$$\mu_G(X_m^*) = \max_{m=\overline{1, M}} \mu_G(X_m). \quad (4)$$

С учетом вышеизложенного выбор рационального варианта построения специализированной РБД состоит в решении следующей научной задачи.

На исходном множестве X ($X=\{X_m\}$, $m = \overline{1, M}$) допустимых вариантов построения РБД найти такой вариант построения РБД X_m^* ($X_m^* \in X$, $m = \overline{1, M}$), для которого показатель степени реализации информационных потребностей пользователей РБД $\mu_G(X_m^*)$ достигает максимума, то есть найти

$$X_m^* = \arg \max_{X_m \in X \;\; 1 \le m \le M} \{\mu_G(X_m)\}. \quad (5)$$

В общем случае для решения сформулированной задачи необходимо осуществить генерацию допустимых вариантов построения специализированной РБД (вариантов отображения канонической структуры в логическую в соответствии с [2]) с последующей их количественной оценкой и выбором рационального варианта построения (логической структуры) РБД в соответствии с критерием оптимизации (5).

Литература

1. Модели принятия решений на основе лингвистической переменной. / А.Н. Борисов, А.В. Алексеев, О.А. Крумберг и др. - Рига: Зинатне, 1982. - 256 с.

2. Кульба В.В., Ковалевский С.С., Косяченко С.А., Сиротюк В.О. Теоретические основы проектирования оптимальных структур распределенных баз данных. - М.: Синтег, 1999. - 660 с.

ПОИСК ВЕСОВЫХ КОЭФФИЦИЕНТОВ ДЛЯ ЛИНЕЙНОЙ ФУНКЦИИ ПОКАЗАТЕЛЕЙ, ХАРАКТЕРИЗУЮЩИХ СОСТОЯНИЕ СЛОЖНОЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМЫ

Бурушкин А.А., Донцов Г.Ю., Жилинский С.В.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, Воронеж,

При проведении оценки функционирования сложных организационно-технических систем возникает потребность в показателях, характеризующих их состояние. При этом основной особенностью таких систем является наличие большого числа предъявляемых к ним требований, степень выполнения которых необходимо учитывать при проведении таких оценок.

В тоже время, анализ основных требований, предъявляемых к сложным организационно-техническим системам, показывает, что эти требования в общем случае могут быть сведены к пяти основным группам:

- наличие и полнота отработки системы документов, регламентирующих деятельность данных систем;
- полнота планирования и выполнения мероприятий, в интересах реализации возложенных на данные системы задач;
- полнота формирования технической базы, предназначенной для решения возложенных на данные системы задач;
- полнота формирования организационной структуры системы;
- эффективность выполнения возложенных на систему задач.

Таким образом, данные группы по своей сути представляют собой частные показатели ($П_j$), характеризующие полноту выполнения предъявляемых к системе требований. Иными словами значение каждого из показателей определяется по совокупности выполнения отдельных требований и рассматривается в виде функции количества выполненных требований [1, 2]:

$$П_j = F(x_1, x_2, ..., x_z) \quad (1)$$

где x_z – предъявляемое к системе z-е требование; j – номер оцениваемого показателя.

В теории систем, в качестве одного из методов оценки показателей, характеризующих функционирование сложных систем, используется замена функции показателя, если неизвестно ее аналитическое выражение, линейной функцией, включающей все основные предъявляемые к системе требования соответствующие оцениваемому показателю [1, 2]:

$$П_j = \sum_{z=1}^{Z} d_z x_z , \quad (2)$$

где d_z – весовой коэффициент предъявляемого к системе z-го требования.

Самостоятельной задачей при использовании линейной функции (1) является поиск весовых коэффициентов d_z.

Однако, в виду того, что требования, предъявляемые к сложным организационно-техническим системам, обладают большой размерностью даже в рамках одного из частных показателей, поиск их весовых коэффициентов существенно затруднен.

В интересах решения данной задачи предложено при вычислении значений частных показателей, характеризующих состояние сложных организационно-технических систем, рассматривать их не как линейную функцию количества выполненных требований, а как линейную функцию количества нарушений по их выполнению. При этом в общем случае, предложено невыполнение каждого отдельного требования классифицировать исходя из следующих положений:

- нарушение первого типа – невыполнение требований приводит к срыву эффективного функционирования системы, либо существует реальная возможность такого срыва;
- нарушение второго типа – невыполнение требований создает предпосылки к срыву эффективного функционирования системы;
- нарушение третьего типа – не выполнены другие требования предъявляемые к оцениваемой системе;
- нарушение четвертого типа – формально требования выполнены, но имеются рекомендации по улучшению состояния дел.

Тогда, значение каждого из показателей определяется по совокупности выполнения отдельных требований и рассматривается как линейная функция количества нарушений различных типов, для которых устанавливаются соответствующие весовые коэффициенты:

$$П_j = F(y_1, y_2, ..., y_i) = \sum_{i=1}^{I} a_i y_i \quad (3)$$

где y_i – количество выявленных нарушений i-го типа; a_i – весовые коэффициенты нарушений i-го типа.

Поиск весовых коэффициентов установленных типов нарушений предложено осуществлять путем формирования и решения системы нормальных уравнений Гаусса [3-7]. Однако данный метод, для решения рассматриваемой задачи, в его классической постановке не применим в следствие того, что при его применении в качестве исходных данных должны использоваться как входные данные - количество выявленных нарушений i-го типа, так и выходные данные – значения оцениваемых показателей, которые также как и искомые весовые коэффициенты a_i являются неизвестными величинами.

Для преодоления данного противоречия предложено поиск весовых коэффициентов осуществлять в два этапа. На первом этапе формируются комбинации количества выявленных нарушений различных типов, для которых с использованием экспертных методов [8] проводится вычисление значений оцениваемых показателей. На втором этапе непосредственно осуществляется формирование и решение системы нормальных уравнений с использованием полученных на первом этапе исходных данных. При этом будут найдены значения, среднеквадратичные отклонения которых от действительных значений минимальны.

В ходе решения задач первого этапа необходимо учитывать то, что количество комбинаций нарушений различных типов (y_i) должно составлять не менее $N=10^S$ раз (где S – число членов уравнения и соответственно S=I), причем данные комбинации не должны повторять друг друга. В противном случае матрица коэффициентов нормальных уравнений будет плохо обусловленной и решение уравнений затрудняется.

Таким образом, задаваемые в произвольном порядке, количество и качественный состав выявленных нарушений являются входными данными функции показателя $П_j$, по которым с использованием экспертных методов [8] формируются выходные данные – предварительные оценки значений показателей $П_j$.

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

Для учета качественного состава выявленных нарушений введены следующие основные правила:

- значения показателей находятся в интервале от 0 до 1;
- при наличии хотя бы одного нарушения первого типа значение показателя принимается равным нулю;
- нарушения второго типа оказывают более существенное влияние на состояние оцениваемой системы, чем нарушения третьего и четвертого типов вместе взятые, т.е. $a_1>(a_2+a_3)$;
- нарушения третьего типа оказывают большее влияние на состояние оцениваемой системы, чем нарушения четвертого типа, т.е. $a_2>a_3$.

При наличии нарушений верхняя граница возможных значений показателей определяется в соответствии со следующими правилами:

- при наличии хотя бы одного нарушения первого типа, значения оцениваемых показателей принимаются равными нулю;
- при наличии хотя бы одного нарушения второго типа, значения оцениваемых показателей находятся в интервале возможных значений $0 \le П_j < (1-\frac{1}{\ln 10})$;
- при наличии хотя бы одного нарушения третьего типа и отсутствии нарушений второго типа, значения оцениваемых показателей находятся в интервале возможных значений $0 \le П_j < (1-\frac{1}{(\ln 10)^3})$.

Общая зависимость возможных значений оцениваемых показателей $П_j$ от количества нарушений различных типов проиллюстрирована на рис. 1.

С учетом вышеизложенного можно составить N условных уравнений [5]:

$$\begin{aligned} a_1y_{11} + a_2y_{12} + a_3y_{13} &= П_{j1}, \\ a_1y_{21} + a_2y_{22} + a_3y_{23} &= П_{j2}, \\ a_1y_{31} + a_2y_{32} + a_3y_{33} &= П_{j3}, \\ &\dots \\ a_1y_{n1} + a_2y_{n2} + a_3y_{n3} &= П_{jn}, \end{aligned} \qquad (4)$$

где y_1, y_2, y_3 - количество нарушений второго, третьего и четвертого типов соответственно;

a_1, a_2, a_3 – весовые коэффициенты нарушений второго, третьего и четвертого типов соответственно (учитывая то, что при наличии нарушений первого типа значение оцениваемого показателя принимается равным нулю, поиск весового коэффициента для данного типа нарушений не проводится);

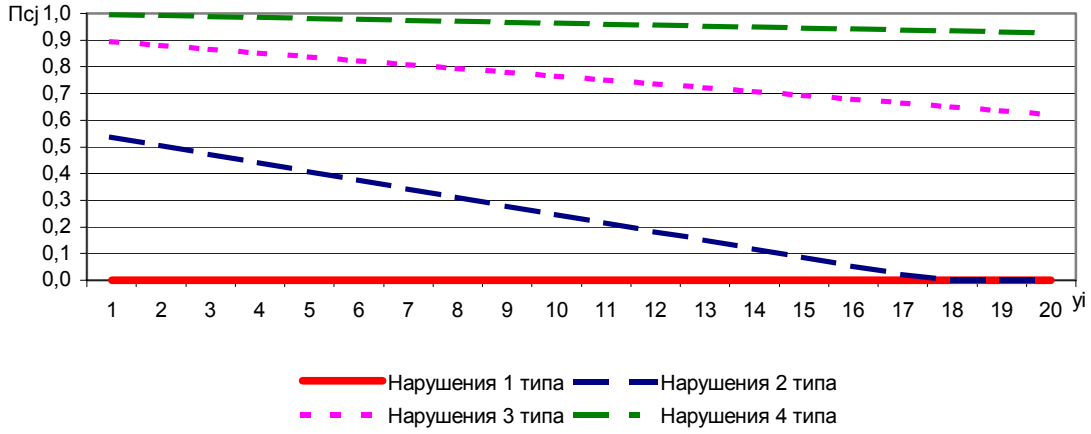


Рис. 1. Общая зависимость возможных значений оцениваемых показателей $П_j$ от количества нарушений различных типов

Кроме того, при формировании системы условных уравнений (4) учитывалось следующее:

- для правомерного использования при определении значений оцениваемых показателей линейной функции (3) выходные данные должны находиться в пределах одного из интервалов возможных значений, представляющего собой линейную функцию типа:

$$\Pi_j = a_0 - \sum_{i=1}^{I} a_i y_i , \quad (5)$$

где a_0 – верхняя граница интервала возможных значений;

- значения входных данных по второму типу нарушений не должны быть равны 0.

Система условных уравнений (4) несовместна, так как уравнений больше чем неизвестных.

Для получения первого уравнения системы совместных нормальных уравнений каждое условное уравнение умножается на коэффициент при первом неизвестном, и все условные уравнения суммируются.

Для получения второго уравнения системы совместных нормальных уравнений каждое условное уравнение умножается на коэффициент при втором неизвестном, и все условные уравнения суммируются.

Для получения третьего уравнения системы совместных нормальных уравнений каждое условное уравнение умножается на коэффициент при третьем неизвестном, и все условные уравнения суммируются.

Число нормальных уравнений равно числу неизвестных коэффициентов.

В нашем случае получим:

$$\begin{aligned}
&a_1y_{11}y_{11}+a_2y_{12}y_{11}+a_3y_{13}y_{11}=\Pi_{j1}y_{11};\\
&a_1y_{21}y_{11}+a_2y_{22}y_{11}+a_3y_{23}y_{11}=\Pi_{j2}y_{11};\\
&a_1y_{31}y_{11}+a_2y_{32}y_{11}+a_3y_{33}y_{11}=\Pi_{j3}y_{11};\\
&\ldots\\
&a_1y_{n1}y_{11}+a_2y_{n2}y_{11}+a_3y_{n3}y_{11}=\Pi_{jn}y_{11}\\
\hline
&a_1\sum_{n=1}^{N} y_{n1}y_{11}+a_2\sum_{n=1}^{N} y_{n2}y_{11}+a_3\sum_{n=1}^{N} y_{n3}y_{11}=\sum_{n=1}^{N}\Pi_{jn}y_{11}\\
&a_1y_{11}y_{12}+a_2y_{12}y_{12}+a_3y_{13}y_{12}=\Pi_{j1}y_{12};\\
&a_1y_{21}y_{12}+a_2y_{22}y_{12}+a_3y_{23}y_{12}=\Pi_{j2}y_{12};\\
&a_1y_{31}y_{12}+a_2y_{32}y_{12}+a_3y_{33}y_{12}=\Pi_{j3}y_{12};\\
&\ldots\\
&a_1y_{n1}y_{12}+a_2y_{n2}y_{12}+a_3y_{n3}y_{12}=\Pi_{jn}y_{12}\\
\hline
&a_1\sum_{n=1}^{N} y_{n1}y_{12}+a_2\sum_{n=1}^{N} y_{n2}y_{12}+a_3\sum_{n=1}^{N} y_{n3}y_{12}=\sum_{n=1}^{N}\Pi_{jn}y_{12}\\
&a_1y_{11}y_{13}+a_2y_{12}y_{13}+a_3y_{13}y_{13}=\Pi_{j1}y_{13};\\
&a_1y_{21}y_{13}+a_2y_{22}y_{13}+a_3y_{23}y_{13}=\Pi_{j2}y_{13};\\
&a_1y_{31}y_{13}+a_2y_{32}y_{13}+a_3y_{33}y_{13}=\Pi_{j3}y_{13};\\
&\ldots\\
&a_1y_{n1}y_{13}+a_2y_{n2}y_{13}+a_3y_{n3}y_{13}=\Pi_{jn}y_{13}\\
\hline
&a_1\sum_{n=1}^{N} y_{n1}y_{13}+a_2\sum_{n=1}^{N} y_{n2}y_{13}+a_3\sum_{n=1}^{N} y_{n3}y_{13}=\sum_{n=1}^{N}\Pi_{jn}y_{13}
\end{aligned} \quad (6)$$

Решая систему из трех нормальных уравнений находим весовые коэффициенты a_i для нарушений i-го типа.

Проведенные с использованием изложенного подхода расчеты применительно к системе обеспечения безопасности информации позволили получить следующие весовые коэффициенты:

- для нарушений второго типа – a_1=0,0323;
- для нарушений третьего типа – a_2=0,0144;
- для нарушений четвертого типа – a_3=0,0036.

Примеры зависимости состояния безопасности информации от количества нарушений различных типов, а также от их комбинаций (при одинаковом количестве нарушений различных типов) приведены на рис. 2.

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

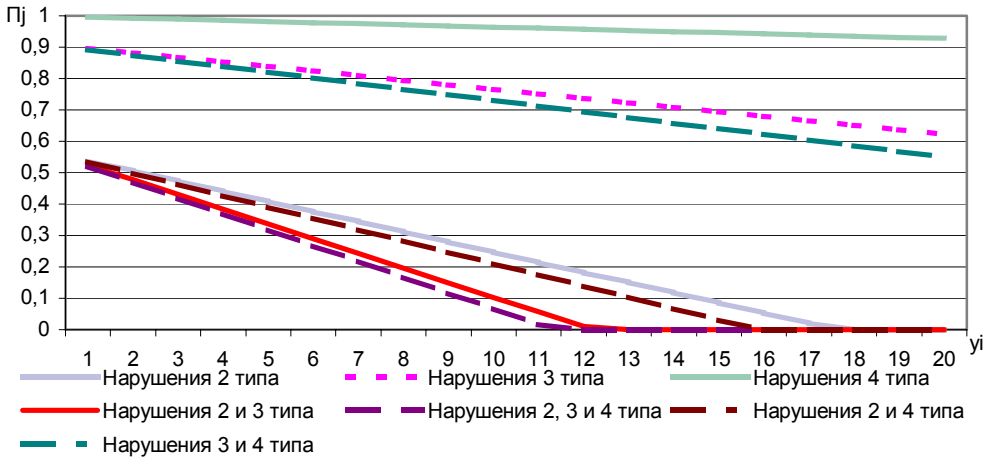


Рис. 2 – Зависимость состояния безопасности информации от количества нарушений различных типов

Литература

1. Дружинин В.В., Конторов Д.С. Системотехника. М.: Радио и связь, 1985. – 200 с.
2. Чумаков Н.М., Серебряный Е.И. Оценка эффективности сложных технических устройств. – М.: Сов. радио, 1980. - 192 с.
3. Ивахненко А.Г. Системы эвристической самоорганизации в технической кибернентике. Киев. "Техника", 1971, - 372 с.
4. Ивахненко А.Г. Самообучающиеся системы распознавания и автоматического управления. Киев. "Техника", 1969.
5. Введение в численные методы анализа и линейной алгебры. Учебное пособие. Горно-Алтайск, 2000, - 48 с.
6. Боглаев Ю.П. Вычислительная математика и программирование. М., Высшая школа, 1990, 544с.
7. Копченова Н.В., Марон И.А. Вычислительная математика в примерах и задачах. М., Наука, 1972, 367с.
8. Методы экспертных оценок. - М.: ВНИИПИ, 1987, - 28 с.

АДАПТАЦИЯ МАТЕМАТИЧЕСКОГО АППАРАТА СЕТЕЙ ПЕТРИ ДЛЯ РЕШЕНИЯ ЗАДАЧ МОДЕЛИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Бурмин В.А., Мирошников В.В.
Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, Воронеж

Системы защиты информации (СЗИ) в локальных вычислительных сетях (ЛВС) с математической точки зрения являются сложными синхронными последовательно-параллельными структурами. Моделирование указанных систем является важнейшей задачей комплексной оценки их эффективности.

Модель СЗИ как синхронной последовательно-параллельной структуры предполагает оценку ее состояния в каждой ветви моделируемых параллельных процессов по шкале модельного времени. Причем, количество состояний, определяющих поведение СЗИ, может быть достаточно большим, а алгоритм перехода из одного состояния в другое – соизмерим по сложности с алгоритмом функционирования ЛВС. Возникает необходимость разработки многомерной модели, отображающей во времени поведение и состояние моделируемой СЗИ. При этом влияние поведения моделируемой системы на ее дальнейшее состояние и влияние текущего состояния на дальнейшее поведение обоюдное. Многомерность модели не только увеличивает сложность ее реализации, но кратно увеличивает время разработки, требуемые вычислительные ресурсы, уменьшает гибкость модели.

Использование для моделирования СЗИ аппарата сетей Петри имеет ряд неоспоримых преимуществ: гибкость модели, минимальные системные требования к средствам реализации модели, возможность управления уровнем адекватности модели, неограниченная свобода задания аспектов оценки в интересах исследования их влияния на показатели защищенности информации в ЛВС.

Авторами предлагается, во-первых, вариант решения проблемы многомерности модели, возникающей при моделировании СЗИ ЛВС. При этом предлагается совершенствование семафоров, разработанных Дейкстрой [1], обеспечивающее моделирование сложных последовательно-параллельных структур со множеством взаимозависимых состояний в одной плоскости сети Петри. Во-вторых, предлагаются методы усовершенствования способа синхронизации моделей, использующих аппарат асинхронных по определению сетей Петри.

Классический семафор представляет собой переменную на области целых неотрицательных чисел. Его применение подразумевает использование двух операций V и P, аргументами которых являются текущее значение семафора, а значениями – новое. Операция V используется для инкрементирования значения семафора, а операция P – для декрементирования. Причем, если при вызове операции P текущее значение семафора нулевое, то указанная операция будет завершена только при изменении значения семафора операцией V, инициализированной другой ветвью. Таким образом, по принципу управления классический семафор является алгебраическим абстрактным компонентом сети Петри, используемым для диспетчеризации исполнения критических интервалов. При моделировании сложных последовательно-параллельных структур со множеством взаимозависимых состояний предлагается "окрасить" семафор палитрой состояний, свойственных моделируемой системе. К примеру, при моделировании сетевого обмена семафор должен отражать текущее состояние моделируемого стека протоколов.

В общем случае предлагаемый семафор Ξ представляет собой n-разрядную двоичную переменную, область значений которой ограничивается рядом целых положительных чисел, удовлетворяющих следующим условиям:

$$\Xi = \sum_{i=1}^{n} (\xi_i \times 2^{i-1}) \text{ , причем } \sum_{i=1}^{n} \xi_i = A \text{ ,} \quad (1)$$

где A – количество одновременно допустимых значений состояний системы (обычно система в текущий момент времени может находиться только в одном состоянии, A=1);

ξ_i – булево отражение i-го состояния моделируемой системы (1 = “true” – система находится в состоянии i, 0 = “false” – система находится в состоянии, отличном от i).

Для диспетчеризации событий с учетом состояния семафора каждому переходу t_i от одного события ветви к другому устанавливаются в соответствие две семафорные константы, имеющие ту же размерность, что и семафор. Первая константа – Q_i – определяет перечень состояний семафора, при которых допустимо срабатывание перехода. Необходимое (но не достаточное) условие срабатывания перехода t_i от одного события ветви к другому:

$$(\Xi \oplus Q_i > 0) \Leftrightarrow (\bigvee_{j=1}^{n} (\xi_j \wedge q_{ij}) = 1) \,. \quad (2)$$

Вторая константа – S_i – используется для вычисления значения семафора в случае срабатывания перехода t_i по следующей формуле:

$$\Xi = (S_i \wedge \Xi) \vee ((\neg(S_i \wedge \Xi)) \vee S_i) \,. \quad (3)$$

Срабатывание перехода t_i от одного события ветви к другому будет происходить при одновременном удовлетворении условия (2) и классического условия срабатывания перехода, определенного математическим аппаратом сетей Петри:

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

$$\begin{cases} \forall p \in {}^{*}t : M(p) \geq F(p,t) \\ \bigvee_{j=1}^{n} (\xi_j \wedge q_{ij}) = 1 \end{cases}, \quad (4)$$

где *M (p)* – разметка сети – функция *M:P6N*, которая используется в сетях Петри для сопоставления каждому месту *p 0 P* некоторого числа *M (p) 0 N*, соответствующего количеству фишек в данном месте;

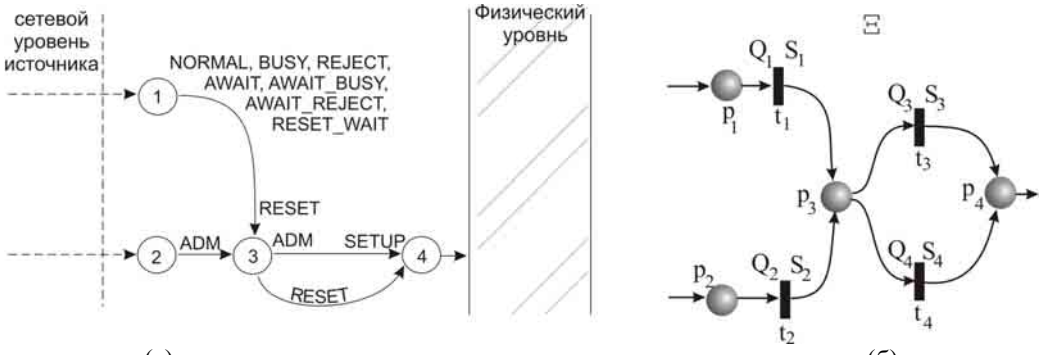
F(p,t) – входная по отношению к переходам сети Петри функция инцидентности.

Если условий для срабатывания перехода недостаточно, то процесс текущей ветви приостанавливается до момента формирования всех необходимых условий. При срабатывании перехода t_i в соответствии с (3) устанавливается новое значение семафора.

В связи с тем, что диспетчеризация посредством семафора исполнения критических интервалов сети соответствует логике моделируемых процессов, а управление семафором осуществляется выражениями булевой алгебры, предложенный авторами семафор следует считать логическим.

В качестве примера использования логического семафора рассмотрим представление одной из функций протокола LLC, являющегося обязательным компонентом распределенных вычислительных систем, связанных по стекам протоколов TCP/IP, Novell, IBM/Microsoft, и в определенной степени определяющим интегральное состояние целостности и доступности информации, циркулирующей в вычислительной сети.

На рис.1 представлен фрагмент графа функционирования протокола LLC, интерпретирующий начало установления соединения по инициативе стека передающей станции, и его интерпретация сетью Петри.



(а) (б)

Рис. 1. Фрагмент графа протокола LLC (а) и его интерпретация сетью Петри (б)

Узлы 1, 2, 3 и 4 графа LLC соответствуют следующим событиям протокола: “локальный сетевой уровень (ЛСУ) затребовал выполнение операции сброса в установленном логическом соединении”, “ ЛСУ запрашивает установление логического соединения”, “Сформирован запрос на установку сбалансированного асинхронного расширенного режима”, “Отправлен запрос на установку сбалансированного асинхронного расширенного режима”.

Дуги, соединяющие узлы графа протокола LLC, маркированы состояниями протокола. Протокол LLC в соответствии со стандартом [2] может находиться в одном из четырнадцати состояний, прокомментированных в таблице 1.

Таблица 1 – Соответствие состояний системы значениям семафора

№ п/п	Состояние системы		Значение семафора	
	обозначение	значение	$\xi_{14}\xi_{13}\ldots\xi_1$ (2_{cc})	Ξ (16_{cc})
1	ADM	исходное	..00 0000 0000 0001	0001
2	CONN	установление соединения	..00 0000 0000 0010	0002
3	D_CONN	разрыв соединения	..00 0000 0000 0100	0004
4	NORMAL	обмен кадрами	..00 0000 0000 1000	0008
5	SETUP	установка	..00 0000 0001 0000	0010
6	RESET	сброс	..00 0000 0010 0000	0020
7	AWAIT	ожидание	..00 0000 0100 0000	0040
8	ERROR	ошибка	..00 0000 1000 0000	0080
9	REJECT	отказ	..00 0001 0000 0000	0100
10	BUSY	занято	..00 0010 0000 0000	0200
11	RESET_WAIT	ожидание сброса	..00 0100 0000 0000	0400
12	RESET_CHECK	проверка сброса	..00 1000 0000 0000	0800
13	AWAIT_BUSY	ожидание освобождения	..01 0000 0000 0000	1000

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

№ п/п	Состояние системы		Значение семафора	
	обозначение	значение	$\xi_{14}\xi_{13}...\xi_1$ (2_{cc})	Ξ (16_{cc})
14	AWAIT_REJECT	ожидание восстановления	..10 0000 0000 0000	2000

Семафор в соответствии с (1) представляет собой 14-разрядную двоичную переменную, область значений которой ограничивается рядом целых положительных чисел, удовлетворяющих следующим условиям:

$$\begin{cases} \Xi = \sum_{i=1}^{14} (\xi_i \times 2^{i-1}) \\ \sum_{i=1}^{14} \xi_i = 1 \end{cases}.$$

Указанным условиям соответствуют значения семафора, представленные в таблице 1.

Для диспетчеризации моделирования событий с учетом состояния семафора каждому переходу t_i устанавливаются в соответствие две семафорные константы.

Первая константа – Q_i – определяет перечень состояний семафора, при которых допустимо срабатывание перехода в соответствии с (2):

$$(\Xi \oplus Q_i > 0) \Leftrightarrow (\bigvee_{j=1}^{14} (\xi_j \wedge q_{ij}) = 1).$$

Вторая константа – S_i – используется для вычисления значения семафора в случае срабатывания перехода t_i в соответствии с (3).

Множество переходов T сети Π_S включает 4 элемента (рис.1.б). В связи с использованием логического семафора в сети Π_S , каждый переход, помимо отношений инцидентности, описывается парой семафорных констант Q_i и S_i .

В соответствии с графом функционирования подуровня LLC (рис.1.а) и установленным упорядочиванием состояний протокола LLC (табл.1) для переходов t_i сети Π_S должны быть установлены значения семафорных констант, представленные в таблице 2.

Таблица 2 – Значения семафорных констант переходов t_i

i	Значения Q_i		Значения S_i	
	2_{cc}	16_{cc}	2_{cc}	16_{cc}
1	..11 0111 0100 1000	3748	..00 0000 0010 0000	0020
2	..00 0000 0000 0001	0001	..00 0000 0000 0001	0001
3	..00 0000 0000 0001	0001	..00 0000 0001 0000	0010
4	..00 0000 0010 0000	0020	..00 0000 0010 0000	0020

Программная реализации функционирования логического семафора проста и не отягощает в значительной мере программный код модели.

Важной особенностью сетей Петри является их асинхронность [1,3]. Сеть Петри не предполагает зависимость событий/переходов от текущих моментов времени (как реального, так и модельного). Тем не менее, для оценки эффективности моделируемых СЗИ и ЛВС в понятиях сетей Петри этого недостаточно. В данных случаях необходимы синхронные модели, обеспечивающие оценку эффективности моделируемой системы по шкале модельного времени.

Способ синхронизации сети Петри, описанный Котовым В.Е.[1], предусматривает функционирование сети по тактам. При этом, в начале каждого такта по установленным для сети правилам срабатывания переходов определяется перечень переходов, готовых к срабатыванию. Из полученного перечня исключаются переходы, срабатывание которых связано с конфликтом. Таким образом, формируется множество $T' \subset T$ неконфликтующих переходов, для которых справедливо:

$$\begin{cases} \forall p_a \in {}^*t_i, p_a \subset `P : M(p_a) \geq F(p_a, t_i) \\ \forall p_b \in {}^*t_j : M(p_b) \geq F(p_b, t_j) : p_b \not\subset `P \end{cases},$$

где выражение первой строки представляет правило срабатывания асинхронного перехода: переход t_i может сработать при некоторой разметке M сети N, если каждое входное место p_a перехода t_i имеет разметку, не меньшую, чем кратность дуги, соединяющей p_a и t_i, а выражение второй строки – условие того, что срабатывание перехода t_i не связано с конфликтом: ни одно место p_b , обеспечивающее условие срабатывания перехода t_j , не является входным по отношению к переходу t_i .

Далее все переходы $t \subset T'$ срабатывают в любом порядке, изменяя текущую разметку сети M на новую разметку M' по следующему правилу:

$$\forall p \in P, \forall t \in T' : M'(p) = M(p) - F(p,t) + F(t,p) \quad ,$$

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

где $F(p,t)$ и $F(t,p)$ – соответственно входная и выходная по отношению к множеству мест функции инцидентности переходов.

На этом такт заканчивается, после чего начинается новый такт при новой разметке.

Отличительной особенностью способа является то, что в течение такта перечень переходов, готовых к срабатыванию (Ť), не пересматривается, несмотря на меняющуюся в ходе выполнения такта разметку. То есть, в течение такта переходы $t \subset$ Ť не мешают друг другу и не оказывают влияния на ситуацию других переходов.

Очевидно, что рассмотренный способ синхронизации сети Петри, предложенный Котовым, в большей степени направлен на решение проблемы конфликтов в сети. Как способ синхронизации, рассмотренный подход, учитывая возможность привязки каждого такта к дискретной шкале модельного времени, может быть использован только в моделях с непрерывным изменением состояния, использующих метод задания времени фиксированного шага [4]. При этом данный способ, наряду с неоспоримыми достоинствами (простотой представления, универсальностью), имеет существенный недостаток, угрожающий в определенных ситуациях уровню адекватности представления моделируемой системы сетью Петри.

Недостаток способа следующий. Возможна ситуация, когда конфликт сети не будет исчерпан для определенных переходов ни в первом такте, ни в последующем. При этом фактически из сети будут выброшены фрагменты, включающие окрестности готовых к срабатыванию, но исключенных из списка обработки по причине участия в конфликте, переходов.

Решение проблемы видится в том, чтобы принципиально исключить возможность возникновения конфликтов. Для этого авторами предлагается два метода: использование многоуровневой системы приоритетов и введение в аппарат сетей Петри дополнительных элементов логического управления.

Метод использования многоуровневой системы приоритетов предполагает определение необходимого числа уровней системы приоритетов сети Петри, определение для каждого уровня приоритета подмножества переходов сети, которые будут участвовать в работе на соответствующем уровне, и выполнение такта в последовательности аналогичных действий по каждому уровню, начиная с высшего (первого) и заканчивая низшим уровнем приоритета. Причем, определение подмножеств переходов сети, участвующих в работе уровня, должно полностью исключить потенциальные конфликты сети на каждом уровне приоритетов.

Для определения числа уровней системы приоритетов (глубины конфликтов сети) в сеть Петри, являющуюся набором $N = (P, T, F, W, M_0)$, где

P – непустое множество элементов сети – мест;

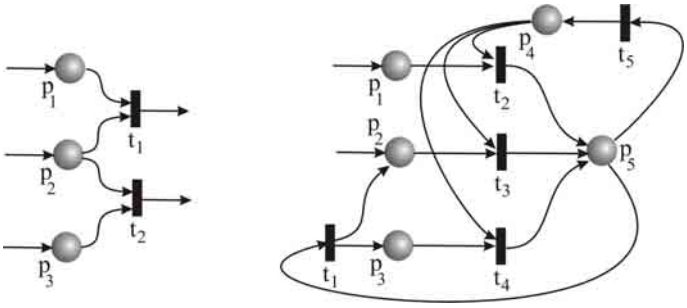
T – непустое множество элементов сети – переходов;

F – отношение инцидентности;

W – непустое множество элементов сети, определяющее кратность дуг;

M_0 – множество начальной разметки,

вводится дополнительный компонент G — множество элементов глубины конфликтов сети N, определяющих по каждому месту $p \subset P$ количество выходных по отношению к нему переходов, для которых данное место создает предпосылку конфликта. На рис.2 продемонстрирован пример задания $G(p)$ в условиях упорядочения множества мест P.



а) G = (0, 2, 0) б) G = (0, 0, 0, 3, 2)

Рис.2 – Задание множества глубины конфликтов

Максимальное значение элементов множества G определяет требуемое число уровней системы приоритетов (глубину конфликтов сети G_m): $G_m = Max(G(p))$.

При проектировании сети Петри для каждого уровня g устанавливается подмножество переходов $T'_g \subset T$, участвующих в проверке выполнения условий срабатывания, исключающее возможность возникновения конфликтов в окрестностях переходов подмножества T'_g. Естественно, процесс определения приоритетности одного конфликтного перехода по отношению к другому, а точнее говоря, приоритет одной исходящей дуги

места по отношению к другой исходящей дуге этого же места, требует внимательного изучения моделируемой системы для правильного отображения ее поведения в сети Петри.

Если исследование алгоритма функционирования моделируемой системы позволяет установить, к примеру, для переходов t_2, t_3 и t_4 сети, представленной на рис .3 (б) и имеющей глубину конфликтов сети G_m = 3, приоритеты 1, 2 и 3 соответственно, а для переходов t_5 и t_1 – соответственно приоритеты 1 и 2, то подмножества переходов $T'_g \subset T$ будут иметь следующий вид:

$T'_1 = (t_2, t_5)$; $T'_2 = (t_3, t_1)$; $T'_3 = (t_4)$.

Для сетей, использующих многоуровневую систему приоритетов, переходы, потенциально не участвующие в конфликтах, рекомендуется включать в подмножество T'_1 первого уровня приоритетов.

Второй метод предполагает введение в аппарат сетей Петри дополнительных элементов логического управления, усиливающих описательные возможности сети Петри, и позволяющих полностью исключить потенциальные конфликты сети. Использование исключительно логического семафора недостаточно для универсального решения данной задачи.

Исключение конфликтности в сетях Петри возможно в случае использования в описательных механизмах и механизмах управления сетью всех логических операций, приближая тем самым сети Петри по мощности к машинам Поста и Тьюринга. Классическая сеть оперирует непосредственно только одной логической операцией – дизъюнкцией. Конъюнкция и инверсия используются косвенно.

Например, введение в сеть Петри, моделирующей стек сетевых протоколов, только одного дополнительного элемента управления, непосредственно задающего операцию инверсии, позволило более чем на 50% сократить конфликтность сети Петри. При этом, дополнительным элементом сети Петри, введенным в сеть, являлась “дуга-инвертор”.

Указанный элемент может быть только входным по отношению к переходу и позволяет задать необходимое условие срабатывания перехода именно при отсутствии разметки на соответствующем входном месте. Этим достигается большая гибкость сети Петри, причем, с позиций булевой алгебры, без существенных изменений в математическом аппарате ординарных сетей Петри.

При этом правило срабатывания перехода трактуется следующим образом: переход может сработать при некоторой разметке M сети N, если каждое входное место p перехода t_j либо имеет разметку, не меньшую, чем кратность дуги, соединяющей p и t_j, либо не имеет разметки по дуге-инвертору, соединяющей p и t_j.

Для дуги-инвертора принято обозначение ломаной дуги. Для наглядности использования введенного элемента на рис.3 представлен вариант сети Петри и соответствующий граф разметки.

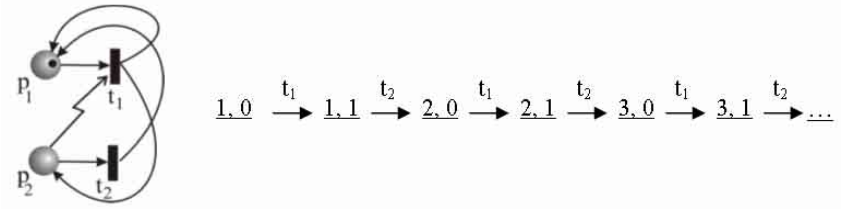


Рис. 3. Пример использования дуги-инвертора для управления сетью Петри

Приведенный пример позволяет оценить эффективность использования дуги-инвертора по ее возможности влияния на граф разметки.

Таким образом, ограничения сетей Петри, связанные с их асинхронностью, преодолимы. В связи с этим сети Петри могут представлять идеальный инструмент моделирования не только тех систем, в которых события происходят асинхронно и независимо, но и, при некотором отходе от чисто локального принципа управления функционированием сети, сложных синхронных последовательно – параллельных структур, к которым относятся СЗИ ЛВС.

Литература

1. Котов В.Е. Сети Петри – М.: Наука. Главная редакция физико-математической литературы, 1984.
2. IEEE Standard for Information technology Telecommunications and information exchange between systems: Local and metropolitan area networks: Specific requirements. Part 2: Logical Link Control– ANSI/IEEE 802.2, 1998.
3. Питерсон Дж. Теория сетей Петри и моделирование систем – М.: Мир, 1984.
4. Шеннон Р. Имитационное моделирование систем – искусство и наука– М.: Мир, 1978.

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

МЕТОДИЧЕСКИЙ ПОДХОД К ПРОВЕДЕНИЮ ОЦЕНКИ СОСТОЯНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Бурушкин А.А., Донцов Г.Ю., Жилинский С.В.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, Воронеж

Выявление существующих проблем в области обеспечения безопасности информации и определение направлений их решения основывается, в первую очередь, на решении задачи анализа и оценки безопасности информации в отдельных организациях.

Необходимая исходная информация для проведения таких оценок формируется по результатам инспекционного контроля состояния безопасности информации, а также периодического сбора исходных данных о состоянии работ в данной области.

Оценка состояния безопасности информации включает:

- оценку соответствия организации работ по обеспечению безопасности информации установленным требованиям;
- оценку соответствия количественных показателей эффективности мероприятий по обеспечению безопасности информации установленным требованиям.

Проведение мероприятий по обеспечению безопасности информации регламентируется системой документов, которые по своей сути определяют совокупность требований по организации и эффективности безопасности информации.

В связи с этим, в интересах оценки состояния безопасности информации проведен анализ системы документов, регламентирующих деятельность в данной области, по результатам которого в явном виде сформулирована такая совокупность требований, выполнение которых подлежит оценке и определена целесообразность двух шаговой процедуры оценки состояния безопасности информации.

На первом шаге рассчитываются показатели по отдельным составляющим обеспечения безопасности информации, для чего совокупность требований сгруппирована по следующим основным группам:

- наличие и содержание документов по обеспечению безопасности информации ($П_{сд}$);
- планирование и выполнение мероприятий по обеспечению безопасности информации ($П_{св}$);
- наличие и правильность применения средств обеспечения безопасности информации ($П_{ст}$);
- формирование организационной структуры системы обеспечения безопасности информации ($П_{сп}$);
- эффективность проведения работ по обеспечению безопасности информации ($П_{сэ}$).

На втором шаге, на основе расчета показателей по отдельным составляющим обеспечения безопасности информации вычисляется значение интегрального показателя ($П_{с}$), характеризующего полноту выполнения требований документов, регламентирующих деятельность в области обеспечения безопасности информации.

Для каждого из показателей определена совокупность частных оценок выполнения отдельных требований, установленных нормативными документами.

Не выполнение отдельного требования соответствует одному из следующих типов нарушений:

- нарушение первого типа - в результате невыполнения требований или норм по обеспечению безопасности информации имелась или имеется реальная возможность утечки информации с ограниченным доступом;
- нарушение второго типа - в результате невыполнения требований по обеспечению безопасности информации создаются предпосылки к утечке информации с ограниченным доступом;
- нарушение третьего типа – не выполнены другие требования по обеспечению безопасности информации;
- нарушение четвертого типа – формально требования выполнены, либо их выполнение жестко не регламентировано действующими документами, в результате чего имеются рекомендации по улучшению состояния дел.

Значение каждого из показателей определяется по совокупности выполнения отдельных требований и рассматривается как линейная функция количества нарушений различных типов [1-3]:

$$П_{cj} = П_{cj} = F(y_1, y_2, ..., y_i) = \sum_{i=1}^{I} a_i y_i \qquad (1)$$

где y_i – количество выявленных нарушений i-го типа;

j – вид оцениваемого показателя (j = {д, в, т, п, э}).

ai – весовые коэффициенты нарушений i-го типа.

Поиск весовых коэффициентов установленных типов нарушений предложено осуществлять путем формирования и решения системы нормальных уравнений Гаусса [4-8] с использованием полученных на основе экспертных методов [9] предварительных оценок состояния безопасности информации при различных ком-

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

бинациях количества нарушений различных типов [настоящий сборник]. При этом будут найдены значения, среднеквадратичные отклонения которых от действительных значений минимальны.

Для учета качественного состава выявленных нарушений введены следующие основные правила:

- значения показателей находятся в интервале от 0 до 1;
- при наличии хотя бы одного нарушения первого типа значение показателя эффективности обеспечения безопасности информации принимается равным нулю;
- нарушения второго типа оказывают более существенное влияние на состояние безопасности информации, чем нарушения третьего и четвертого типов вместе взятые, т.е. $a_1>(a_2+a_3)$;
- нарушения третьего типа оказывают большее влияние на состояние безопасности информации, чем нарушения четвертого типа, т.е. $a_2>a_3$.

Таким образом, при наличии нарушений верхняя граница возможных значений показателей определяется в соответствии со следующими правилами:

- при наличии хотя бы одного нарушения первого типа, значения оцениваемых показателей (Π_{cj}) принимаются равными нулю;
- при наличии хотя бы одного нарушения второго типа, значения оцениваемых показателей находятся в интервале $0\le \Pi_{cj}<(1-\frac{1}{\ln 10})$;
- при наличии хотя бы одного нарушения третьего типа и отсутствии нарушений второго типа, значения оцениваемых показателей находятся в интервале $0\le \Pi_{cj}<(1-\frac{1}{(\ln 10)^3})$,

а общая зависимость значений каждого из оцениваемых частных показателей от типов нарушений преобразуется в линейную функцию типа:

$$\Pi_{cj} = a_0 - \sum_{i=1}^{I} a_i y_i , \qquad (3)$$

где a_0 – верхняя граница диапазона возможных значений.

С учетом сформулированных выше правил проводится преобразование линейной функции (1) в выражение следующего вида:

$$\Pi_{cj}=\sum_{i=1}^{I} a_i y_i = \begin{cases} (1-\frac{1}{\ln 10}) - \sum_{i=1}^{I} a_i y_i , & \text{при наличии нарушений 2 типа;} \\ (1-\frac{1}{(\ln 10)^3}) - \sum_{i=1}^{I} a_i y_i , & \text{при наличии нарушений 3 типа и отсутствии нарушений 2 типа;} \\ 1-\sum_{i=1}^{I} a_i y_i , & \text{при отсутствии нарушений 2 и 3 типа} \end{cases} \qquad (4)$$

На основе приведенных выше положений для проведения работ по оценке состояния безопасности информации предложена следующая процедура.

1. Формируется совокупность оценок выполнения отдельных требований (количество выявленных нарушений различных типов по каждому из сформированных показателей).
2. Определяется значение каждого из показателей в соответствии с выражением (4).
3. По результатам полученных оценок дается общая характеристика степени выполнения установленных требований по каждому из частных показателей согласно условию:

$$\Pi_{cj} = \begin{cases} \text{Т1, если } \Pi_{cj} = 0 \\ \text{Т2, если } 0 \le \Pi_{cj} < (1-\frac{1}{\ln 10}) \\ \text{Т3, если } (1-\frac{1}{\ln 10}) \le \Pi_{cj} < (1-\frac{1}{(\ln 10)^3}) \\ \text{Т4, если } (1-\frac{1}{(\ln 10)^3}) \le \Pi_{cj} \le 1 \end{cases} , \qquad (5)$$

где Т1 – требования по безопасности информации не выполняются;

Т2 – требования по безопасности информации выполняются не в полном объеме;

Т3 - требования по безопасности информации в основном выполняются;

Т4 - требования по безопасности информации выполняются.

4. Проводится оценка состояния безопасности информации по интегральному показателю (Π_c) в соответствии с выражением:

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

$$П_c = \sum_{j=1}^{J} П_{cj} * К_{cj}, \quad (6)$$

где $К_{cj}$ – коэффициент важности показателя $П_{cj}$.

Значения коэффициентов важности частных показателей безопасности информации определяются на основе экспертных методов [10].

5. По результатам полученных оценок дается общая характеристика состояния безопасности информации по интегральному показателю согласно условию:

$$П_c = \begin{cases} С1, \text{если } 0 \le П_{cj} < (1 - \frac{1}{\ln 10}) \\ С2, \text{если } (1 - \frac{1}{\ln 10}) \le П_{cj} < (1 - \frac{1}{(\ln 10)^3}) \\ С3, \text{если } (1 - \frac{1}{(\ln 10)^3}) \le П_{cj} \le 1 \end{cases}, \quad (7)$$

где С1 – состояние безопасности информации не удовлетворяет установленным требованиям;

С2 - состояние безопасности информации удовлетворяет установленным требованиям не в полном объеме;

С3 - состояние безопасности информации удовлетворяет установленным требованиям.

Предложенный подход к оценке состояния безопасности информации в организации апробирован в ходе инспекционных проверок организаций оборонно-промышленного комплекса и субъектов Российской Федерации.

Результаты апробации подтверждают работоспособность, применимость, адекватность формируемых решений и, соответственно, целесообразность использования предложенного подхода в интересах получения оценок состояния безопасности информации в организациях.

Полученные для различных моментов времени оценки могут использоваться для построения зависимости изменения во времени показателей оценки состояния безопасности информации в организации установленным требованиям.

Такая зависимость позволяет в графическом виде представить изменение состояния безопасности информации в оцениваемой организации за определенный период времени и на этой основе выявить недостатки и проблемы в организации и осуществлении работ по обеспечению безопасности информации.

Кроме того, такая зависимость может использоваться:

- для оценки текущего уровня и перспектив развития систем обеспечения безопасности информации в отдельных организациях путем пролонгации кривой на 1 – 2 периода времени вперед от времени последней проведенной оценки (рис. 1);

- для проведения сравнительных оценок состояния безопасности информации (рис. 2) в заданной по какому-либо признаку группе организаций (по виду выполняемых работ, по принадлежности к организациям различной формы собственности и др.).

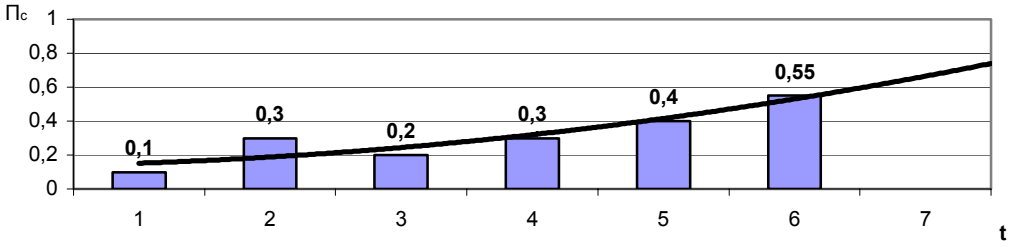


Рис. 1 - Изменение во времени показателя оценки состояния безопасности информации

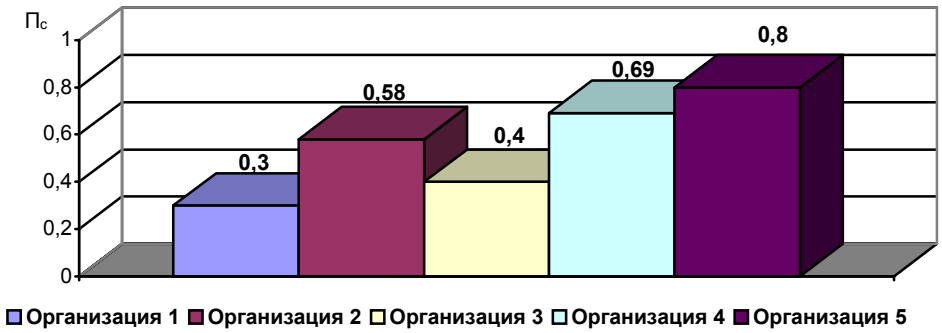


Рис. 2 – Результаты сравнительной оценки состояния безопасности информации в группе организаций

Литература

1. Дружинин В.В., Конторов Д.С. Системотехника. М.: Радио и связь, 1985. – 200 с.
2. Чумаков Н.М., Серебряный Е.И. Оценка эффективности сложных технических устройств. М.: Сов. радио, 1980. - 192 с.
3. Чинаев П.И. Основные принципы построения самонастраивающихся систем. – В кн.: Теория и применение самонастраивающихся систем. – Киев: Техника, 1968. – 328 с.
4. Ивахненко А.Г. Системы эвристической самоорганизации в технической кибернентике. Киев. "Техника", 1971, - 372 с.
5. Ивахненко А.Г. Самообучающиеся системы распознавания и автоматического управления. Киев. "Техника", 1969.
6. Введение в численные методы анализа и линейной алгебры. Учебное пособие. Горно-Алтайск, 2000, - 48 с.
7. Боглаев Ю.П. Вычислительная математика и программирование. М., Высшая школа, 1990, 544с.
8. Копченова Н.В., Марон И.А. Вычислительная математика в примерах и задачах. М., Наука, 1972, 367с.
9. Методы экспертных оценок. - М.: ВНИИПИ, 1987, - 28 с.
10. Саати Т. Принятие решений. Метод анализа иерархий. - М.: Радио и связь, 1993, - 320 с.

ВЫБОР МЕТОДИКИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Кислицын А.С., Курбатов В.А.
ЗАО «Лукойл-Информ»

Понятия “оценка рисков (Risk Assessment)” и “управление рисками (Risk Management)” появились сравнительно недавно и сегодня вызывают постоянный интерес специалистов в области обеспечения непрерывности бизнеса (Business Continuity) и сетевой безопасности (Network Security). Примерно с 1995 года в ряде высокотехнологичных стран мира, главным образом в США, Великобритании, Германии и Канаде, проводятся ежегодные слушания специально созданных комитетов и комиссий по вопросам управления информационными рисками. Подготовлено более десятка различных стандартов и спецификаций, детально регламентирующих процедуры управления информационными рисками, среди которых наибольшую известность приобрели международные спецификации и стандарты ISO 17799-2002 (BS 7799), GAO и FISCAM, SCIP, NIST, SAS 78/94 и COBIT.

В настоящее время *управление информационными рисками* представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача - объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под термином *управление информационными рисками* обычно понимается системный процесс *идентификации, контроля и уменьшения* информационных рисков компаний в соответствии с определенными ограничениями российской нормативно-правовой базы в области защиты информации и собственной корпоративной политики безопасности. Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекват-

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

ные текущим целям и задачам бизнеса компании. Далее представлены результаты анализа существующих на рынке методик управления информационными рисками, которые позволяют реализовать эффективную методику управления остаточными рисками.

Качественные методики управления рисками

Качественные методики управления рисками приняты на вооружение в технологически развитых странах многочисленной армией внутренних и внешних IT-аудиторов. Эти методики достаточно популярны и относительно просты, и разработаны, как правило, на основе требований международного стандарта ISO 17799-2002.

К качественным методикам управления рисками на основе требований ISO 17999 относятся методики COBRA и RA Software Tool.

COBRA

Во второй половине 90-х годов компания C & A Systems Security Ltd. разработала одноименные методику и соответствующий инструментарий для анализа и управления информационными рисками под названием COBRA. Эта методика позволяет выполнить в автоматизированном режиме простейший вариант оценивания информационных рисков любой компании. Для этого предлагается использовать специальные электронные базы знаний и процедуры логического вывода, ориентированные на требования ISO 17799. Существенно, что при желании перечень учитываемых требований можно дополнить различными требованиями отечественных нормативно-регулирующих органов, например, требованиями руководящих документов (РД) Гостехкомиссии при Президенте РФ.

Методика COBRA представляет требования стандарта ISO 17799 в виде тематических “вопросников” (check list’s), на которые следует ответить в ходе оценки рисков информационных активов и электронных бизнес транзакций компании. Далее введенные ответы автоматически обрабатываются и, с помощью соответствующих правил логического вывода, формируется итоговый отчет с текущими оценками информационных рисков компании и рекомендациями по их управлению.

RA Software Tool

Методика и одноименное инструментальное средство RA Software Tool основаны на требованиях международных стандартов ISO 17999 и ISO 13335, а также на требованиях некоторых руководств британского национального института стандартов (BSI), например, PD 3002 (Руководство по оценке и управлению рисками), PD 3003 (Оценка готовности компании к аудиту в соответствии с BS 7799), PD 3005 (Руководство по выбору системы защиты) и пр.

Эта методика позволяет выполнять оценку информационных рисков (модули 4 и 5) в соответствии с требованиями ISO 17799, а при желании в соответствии с более детальными спецификациями руководства PD 3002 Британского института стандартов.

Количественные методики управления рисками

Вторую группу методик управления рисками составляют количественные методики, актуальность которых обусловлена необходимостью решения различных оптимизационных задач, которые часто возникают в реальной жизни. Суть этих задач сводится к поиску единственного оптимального решения, из множества существующих. Например, необходимо ответить на следующие вопросы: “Как, оставаясь в рамках утвержденного годового (квартального) бюджета на информационную безопасность, достигнуть максимального уровня защищенности информационных активов компании?” или “Какую из альтернатив построения корпоративной защиты информации (защищенного WWW сайта или корпоративной E-mail) выбрать с учетом известных ограничений бизнес ресурсов компании?” Для решения этих задач и разрабатываются методы и методики количественной оценки и управления рисками на основе структурных и реже объектно-ориентированных методов системного анализа и проектирования (SSADM - Structured Systems Analysis and Design). На практике такие методики управления рисками позволяют:

- Создавать модели информационных активов компании с точки зрения безопасности;
- Классифицировать и оценивать ценности активов;
- Составлять списки наиболее значимых угроз и уязвимостей безопасности;
- Ранжировать угрозы и уязвимости безопасности
- Обосновывать средства и меры минимизации рисков;
- Оценивать соотношение эффективность-стоимость различных вариантов защиты;
- Формализовать и автоматизировать процедуры оценивания и управления рисками.

Одной из наиболее известных методик этого класса является методика CRAMM.

CRAMM

В 1985 году Центральное Агентство по Компьютерам и Телекоммуникациям (CCTA) Великобритании начало исследования существующих методов управления информационной безопасностью для выдачи рекомендаций по их использованию в правительственных организациях, обрабатывающих конфиденциальную информацию. Ни один из рассмотренных методов не подошел. Поэтому сначала был создан метод, а затем одноименная методика CRAMM (анализа и контроля рисков), соответствующая требованиям CCTA. Затем появилось несколько версий методики, ориентированной на требования различных государственных и коммерческих организаций и структур. Одна из версий "коммерческого профиля" широко распространилась на рынке средств защиты информации.

Основными целями методики CRAMM являются:

- Формализация и автоматизация процедур анализа и управления рисками;
- Оптимизация расходов на средства контроля и защиты;
- Комплексное планирование и управление рисками на всех стадиях жизненного цикла информационных систем;
- Сокращение времени на разработку и сопровождение корпоративной системы защиты информации;
- Обоснование эффективности предлагаемых мер защиты и средств контроля;
- Управление изменениями и инцидентами;
- Поддержка непрерывности бизнеса;
- Оперативное принятие решений по вопросам управления безопасностью.

Современные методики и технологии управления информационными рисками позволяют оценить существующий уровень остаточных информационных рисков в отечественных компаниях. Это особенно важно в тех случаях, когда к информационной системе компании предъявляются повышенные требования в области защиты информации и непрерывности бизнеса. Сегодня существует ряд методик анализа рисков, в том числе с использованием CASE-средств, адаптированных к использованию в отечественных условиях. Существенно, что качественно выполненный анализ информационных рисков позволяет провести сравнительный анализ "эффективность-стоимость" различных вариантов защиты, выбрать адекватные контрмеры и средства контроля, оценить уровень остаточных рисков. Кроме того, инструментальные средства анализа рисков, основанные на современных базах знаний и процедурах логического вывода, позволяют построить структурные и объектно-ориентированные модели информационных активов компании, модели угроз и модели рисков, связанных с отдельными информационными и бизнес транзакциями и, таким образом, выявлять такие информационные активы компании, риск нарушения защищенности, которых является критическим, то есть, неприемлемым. Такие инструментальные средства предоставляют возможность построить различные модели защиты информационных активов компании, сравнивать между собой по критерию "эффективность-стоимость" различные варианты комплексов мер защиты и контроля, а также вести мониторинг выполнения требований по организации режима информационной безопасности отечественной компании.

ПОДХОДЫ К СОЗДАНИЮ КОРПОРАТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Кислицын А.С., Курбатов В.А.

ЗАО «Лукойл-Информ»

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому решение вопроса об оценке уровня защищенности информационных активов компании обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов[1], Конституции и федеральным законам[2], руководящим документам Гостехкомиссии России и ФСБ[3], приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечест-

[1] ГОСТ 51583-00 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования.» ГОСТ Р 51624-00 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.»

[2] Федеральный закон «Об информации, информатизации и защите информации», № 24-ФЗ, 1995 г., ст. 2, Конституция Российской Федерации, ст. 23, Гражданский кодекс Российской Федерации, часть I, ст.ст. 139, 128.

[3] См. сноску 1, ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Архитектура защиты информации».

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

венным условиям и применять на практике методики международных стандартов, таких, как ISO 17799, ISO 9001, ISO 15408, BSI[4] и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации компании.

Современные методики управления рисками, проектирования и сопровождения корпоративных систем защиты информации должны позволять решить ряд задач перспективного стратегического развития компании.

Во-первых, количественно оценить текущий уровень информационной безопасности компании, что потребует выявления рисков на правовом, организационно-управленческом, технологическом, а также техническом уровнях обеспечения защиты информации.

Во-вторых, разработать и реализовать комплексный план совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании. Для этого необходимо:

- обосновать и произвести расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности компании, создать необходимый пакет организационно-распорядительной документации;
- разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;
- обеспечить поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Решение названных задач открывает новые широкие возможности перед должностными лицами разного уровня.

Руководителям верхнего звена это поможет объективно и независимо оценить текущей уровень информационной безопасности компании, обеспечить формирование единой концепции безопасности, рассчитать, согласовать и обосновать необходимые затраты на защиту компании. На основе полученной оценки начальники отделов и служб смогут выработать и обосновать необходимые организационные меры (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действия в нештатных ситуациях). Менеджеры среднего звена смогут обоснованно выбрать средства защиты информации, а также адаптировать и использовать в своей работе количественные показатели оценки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической эффективности компании.

Практические рекомендации по нейтрализации и локализации выявленных уязвимостей системы, полученные в результате аналитических исследований, помогут в работе над проблемами информационной безопасности на разных уровнях и, что особенно важно, определить основные зоны ответственности, в том числе материальной, за ненадлежащее использование информационных активов компании. При определении масштабов материальной ответственности за ущерб, причиненный работодателю, в том числе разглашением коммерческой тайны, следует руководствоваться положениями гл. 39 Трудового кодекса РФ.

При построении копоративной системы защиты информации важно помнить, что прежде чем предлагать какие-либо технические решения, предстоит разработать политику безопасности. Организационная политика безопасности описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил по-

[4] Международные стандарты безопасности ISO разработаны the International Organization for Standartization (ISO) и the International Electrotechnical Commission (IEC) и регламентируют вопросы информационной безопасности. В России стандарты ISO пока не являются общепринятыми, за исключением ISO 15408, адаптированная версия которого была принята Госстандартом и Гостехкомиссией летом 2002 года. ISO не вступают в противоречие с действующими в РФ стандартами и рекомендациями Гостехкомиссии при Президенте РФ, ФАПСИ и рекомендуются к применению ведущими специалистами в области информационной безопасности. Тексты ISO можно найти по адресу: www.iso.org

литики безопасности, и наоборот. Этапы построения организационной политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Организационная политика безопасности оформляется в виде отдельного документа, который согласовывается и утверждается Заказчиком.

Прежде всего необходимо составить детализированное описание общей цели построения системы безопасности объекта, выражаемое через совокупность факторов или критериев, уточняющих цель. Совокупность факторов служит базисом для определения требований к системе (выбор альтернатив). Факторы безопасности, в свою очередь, могут распределяться на правовые, технологические, технические и организационные.

Требования гарантии достигаемой защиты выражаются через оценки функций безопасности СИБ объекта. Оценка силы функции безопасности выполняется на уровне отдельного механизма защиты, а ее результаты позволяют определить относительную способность соответствующей функции безопасности противостоять идентифицированным угрозам. Исходя из известного потенциала нападения, сила функции защиты определяется, например, категориями «базовая», «средняя», «высокая». Потенциал нападения определяется путем экспертизы возможностей, ресурсов и мотивов побуждения нападающего.

Перечень требований к системе информационной безопасности, эскизный проект, план защиты (далее – техническая документация, ТД) содержит набор требований безопасности информационной среды объекта, которые могут ссылаться на соответствующий профиль защиты, а также содержать требования, сформулированные в явном виде.

В общем виде разработка ТД включает:

- уточнение функций защиты;
- выбор архитектурных принципов построения СИБ;
- разработку логической структуры СИБ (четкое описание интерфейсов);
- уточнение требований функций обеспечения гарантоспособности СИБ;
- разработку методики и программы испытаний на соответствие сформулированным требованиям.

На этапе оценки достигаемой защищенности производится оценка меры гарантии безопасности информационной среды. Мера гарантии основывается на оценке, с которой после выполнения рекомендованных мероприятий можно доверять информационной среде объекта. Базовые положения данной методики предполагают, что степень гарантии следует из эффективности усилий при проведении оценки безопасности. Увеличение усилий оценки предполагает:

- значительное число элементов информационной среды объекта, участвующих в процессе оценивания;
- расширение типов проектов и описаний деталей выполнения при проектировании системы обеспечения безопасности;
- строгость, заключающуюся в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

ОЦЕНКА ЗАТРАТ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Кислицын А.С., Курбатов В.А.

ЗАО «Лукойл-Информ»

Оценка эффективности организации режима ИБ в компании предполагает некоторую оценку затрат на ИБ, а также оценку достигаемого при этом эффекта. Действительно сопоставление этих оценок позволяет оценить возврат инвестиций на ИБ, а также экономически корректно планировать и управлять бюджетом компании на ИБ.

На практике многие решения в области защиты информации часто принимаются на интуитивно-понятийном уровне, без каких-либо экономических расчетов и обоснований. В результате только те начальники служб ИБ (CISO), которые за счет своей “энергетики” смогли заявить и отстоять потребность в защите информации могли как-то повлиять на планирование бюджета компании на ИБ. Однако современные требования бизнеса, предъявляемые к организации режима ИБ компании, диктуют настоятельную необходимость использовать в своей работе более обоснованные технико-экономические методы и средства, позволяющие

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

количественно измерять уровень защищенности компании, а также оценивать экономическую эффективность затрат на ИБ.

Сегодня для оценки эффективности корпоративной системы защиты информации рекомендуется использовать некоторые показатели эффективности, например показатели: *совокупной стоимости владения (TCO), экономической эффективности бизнеса и непрерывности бизнеса(BCP), коэффициенты возврата инвестиций на ИБ (ROI) и другие.*

В частности, известная методика совокупной стоимости владения (TCO) была изначально предложена аналитической компанией Gartner Group в конце 80-х годов (1986-1987) для оценки затрат на информационные технологии. Методика Gartner Group позволяет рассчитать всю расходную часть информационных активов компании, включая прямые и косвенные затраты на аппаратно-программные средства, организационные мероприятия, обучение и повышение квалификации сотрудников компании, реорганизацию, реструктуризацию бизнеса и т. д.

Существенно, что сегодня методика TCO может быть использована для доказательства экономической эффективности существующих корпоративных систем защиты информации. Она позволяет руководителям служб информационной безопасности (CISO) обосновывать бюджет на ИБ, а также доказывать эффективность работы сотрудников службы ИБ. Кроме того, поскольку оценка экономической эффективности корпоративной системы защиты информации становится "измеримой", становится возможным оперативно решать задачи контроля и коррекции показателей экономической эффективности и в частности показателя TCO. Таким образом, показатель TCO можно использовать как инструмент для оптимизации расходов на обеспечение требуемого уровня защищенности КИС и обоснование бюджета на ИБ. При этом в компании эти работы могут выполняться самостоятельно, с привлечением системных интеграторов в области защиты информации, или совместно предприятием и интегратором.

Отметим, что показатель TCO может применяться практически на всех основных этапах жизненного цикла корпоративной системы защиты информации и позволяет “навести порядок” в существующих и планируемых затратах на ИБ. С этой точки зрения показатель TCO позволяет объективно и независимо обосновать экономическую целесообразность внедрения и использования конкретных организационных и технических мер и средств защиты информации. При этом для объективности решения необходимо дополнительно учитывать и состояния внешней и внутренней среды предприятия, например показатели технологического, кадрового и финансового развития предприятия. Так как не всегда наименьший показатель TCO корпоративной системы защиты информации может быть оптимален для компании.

Понятно, что умелое управление TCO позволяет рационально и экономно реализовывать средства бюджета на ИБ, достигая при этом приемлемого уровня защищенности компании, адекватного текущим целям и задачам бизнеса. Существенно, что сравнение определенного показателя TCO с аналогичными показателями TCO по отрасли (аналогичными компаниями) и с “лучшими в группе” позволяет объективно и независимо обосновать затраты компании на ИБ. Ведь часто оказывается довольно трудно или даже практически невозможно оценить прямой экономический эффект от затрат на ИБ. Сравнение же “родственных” показателей TCO позволяет убедиться в том, что проект создания или реорганизации корпоративной системы защиты информации компании является оптимальным по сравнению с некоторым среднестатистическим проектом в области защиты информации по отрасли. Указанные сравнения можно проводить, используя усредненные показатели TCO по отрасли, рассчитанные экспертами Gartner Group или собственные экспертами компании с помощью методов математической статистики и обработки наблюдений.

Таким образом, методика TCO Gartner Group позволяет ответить на следующие актуальные вопросы:

Какие ресурсы и денежные средства тратятся на ИБ?

Оптимальны ли затраты на ИБ для бизнеса компании?

Насколько эффективна работа службы ИБ компании по сравнению с другими?

Как эффективно управлять инвестированием в защиту информации?

Какие выбрать направления развития корпоративной системы защиты информации?

Как обосновать бюджет компании на ИБ?

Как доказать эффективность существующей корпоративной системы защиты информации и службы ИБ компании в целом?

Какова оптимальная структура службы ИБ компании?

Как правильно оценить аутсортинговые услуги по сопровождению корпоративной системы защиты информации?

Как оценить эффективность нового проекта в области защиты информации?

В целом методика TCO компании Gartner Group позволяет:

получить адекватную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной системы защиты информации;

сравнить подразделения службы ИБ компании, как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли;

оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ТСО.

Здесь под показателем ТСО понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течении года. ТСО может рассматриваться как ключевой количественный показатель эффективности организации ИБ в компании, так как позволяет не только оценить совокупные затраты на ИБ, но управлять этими затратами для достижения требуемого уровня защищенности КИС.

При этом *прямые затраты* включают как капитальные компоненты затрат (ассоциируемые с фиксированными активами или «собственностью»), так и трудозатраты, которые учитываются в категориях операций и административного управления. Сюда же относят затраты на услуги удаленных пользователей, аутсорсинг и др., связанные с поддержкой деятельности организации.

В свою очередь *косвенные затраты* отражают влияние КИС и подсистемы защиты информации на сотрудников компании посредством таких измеримых показателей как простои и «зависания» корпоративной системы защиты информации и КИС в целом, затраты на операции и поддержку (не относящиеся к прямым затратам). Очень часто косвенные затраты играют значительную роль, так как они обычно изначально не отражаются в бюджете на ИБ, а выявляются явно при анализе затрат в последствии, что в конечном счете приводит к росту «скрытых» затрат компании на ИБ.

Существенно, что ТСО не только отражает «стоимость владения» отдельных элементов и связей корпоративной системы защиты информации в течение их жизненного цикла. «Овладение методикой» ТСО помогает службе ИБ лучше измерять, управлять и снижать затраты и/или улучшать уровни сервиса защиты информации с целью адекватности мер защиты бизнесу компании.

Подход к оценке ТСО базируется на результатах аудита структуры и поведения корпоративной системы защиты информации и КИС в целом, включая действия сотрудников служб автоматизации, информационной безопасности и просто пользователей КИС. Сбор и анализ статистики по структуре прямых (HW/SW, операции, административное управление) и косвенных затрат (на конечных пользователей и простои) проводится, как правило, в течение 12 месяцев. Полученные данные оцениваются по ряду критериев с учетом сравнения с аналогичными компаниями по отрасли.

Методика ТСО позволяет оценить и сравнить состояние защищенности КИС компании с типовым профилем защиты, в том числе показать узкие места в организации защиты, на которые следует обратить внимание. Иными словами, на основе полученных данных можно сформировать понятную с экономической точки зрения стратегию и тактику развития корпоративной системы защиты информации, а именно: «сейчас мы тратим на ИБ столько-то, если будем тратить столько-то по конкретным направлениям ИБ, то получим такой-то эффект».

Известно, что в методике ТСО в качестве базы для сравнения используются данные и показатели ТСО для западных компаний. Однако данная методика способна учитывать специфику российских компаний с помощью так называемых поправочных коэффициентов, например:

по стоимости основных компонентов корпоративной системы защиты информации и КИС, информационных активов компании (Cost Profiles) с учетом данных по количеству и типам серверов, персональных компьютеров, периферии и сетевого оборудования;

по заработанной плате сотрудников (Salary and Asset Scalars) с учетом дохода компании, географического положения, типа производства и размещения организации в крупном городе или нет;

по конечным пользователям ИТ (End User Scalars) с учетом типов пользователей и их размещения (для каждого типа пользователей требуется различная организация службы поддержки и вычислительной инфраструктуры);

по использованию методов так называемой лучшей практики в области управления ИБ (Best Practices) с учетом реального состояния дел по управлению изменениями, операциями, активами, сервисному обслуживанию, обучению, планированию и управлению процессами;

по уровню сложности организации (Complexity Level) с учетом состояния организации конечных пользователей (процент влияния – 40%), технологии SW (40%), технологии HW (20%).

В целом, определение затрат компании на ИБ подразумевает решение следующих трех задач:

оценку текущего уровня ТСО корпоративной системы защиты информации и КИС в целом;

аудит ИБ компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня ТСО;

формирование целевой модели ТСО.

Рассмотрим каждую из перечисленных задач.

Оценка текущего уровня ТСО. В ходе работ по оценке ТСО проводится сбор информации и расчет показателей ТСО организации по следующим направлениям:

существующие компоненты КИС (включая систему защиты информации) и информационные активы компании (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства);

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

существующие расходы на аппаратные и программные средства защиты информации (расходные материалы, амортизация);

существующие расходы на организацию ИБ в компании (обслуживание СЗИ и СКЗИ, а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, планирование и управление процессами защиты информации, разработку концепции и политики безопасности и пр.);

существующие расходы на организационные меры защиты информации;

существующие косвенные расходы на организацию ИБ в компании и в частности обеспечение непрерывности или устойчивости бизнеса компании.

Аудит ИБ компании. По результатам собеседования с TOP-менеджерами компании и проведения инструментальных проверок уровня защищенности организации проводится анализ следующих основных аспектов:

политики безопасности;
организации защиты;
классификации и управления информационными ресурсами;
управления персоналом;
физической безопасности;
администрирования компьютерных систем и сетей;
управления доступом к системам;
разработки и сопровождения систем;
планирования бесперебойной работы организации;
проверки системы на соответствие требованиям ИБ.

На основе проведенного анализа выбирается модель ТСО, сравнимая со средними и оптимальными значениями для репрезентативной группы аналогичных организаций, имеющих схожие с рассматриваемой организацией показатели по объему бизнеса. Такая группа выбирается из банка данных по эффективности затрат на ИБ и эффективности соответствующих профилей защиты аналогичных компаний.

Сравнение текущего показателя ТСО проверяемой компании с модельным значением показателя ТСО позволяет провести анализ эффективности организации ИБ компании, результатом которого является определение «узких» мест в организации, причин их появления и выработка дальнейших шагов по реорганизации корпоративной системы защиты информации и обеспечения требуемого уровня защищенности КИС.

Формирование целевой модели ТСО. По результатам проведенного аудита моделируется целевая (желаемая) модель, учитывающая перспективы развития бизнеса и корпоративной системы защиты информации (активы, сложность, методы лучшей практики, типы СЗИ и СКЗИ, квалификация сотрудников компании и т. п.).

Кроме того, рассматриваются капитальные расходы и трудозатраты, необходимые для проведения преобразований текущей среды в целевую среду. В трудозатраты на внедрение включаются затраты на планирование, развертывание, обучение и разработку. Сюда же входят возможные временные увеличения затрат на управление и поддержку.

Для обоснования эффекта от внедрения новой корпоративной системы защиты информации (ROI) могут быть использованы модельные характеристики снижения совокупных затрат (ТСО), отражающие возможные изменения в корпоративной системе защиты информации.

Вместе с методикой ТСО можно использовать разнообразные методы для расчета возврата инвестиций (ROI). Как правило, для оценки доходной части сначала анализируют те цели, задачи и направления бизнеса, которые нужно достигнуть с помощью внедрения или реорганизации существующих проектов в области системной интеграции, автоматизации и информационной безопасности. Далее используют некоторые измеримые показатели эффективности бизнеса для оценки эффекта отдельно по каждому решению. Допустим, с целью сокращения операционных расходов, обеспечения приемлемой конкурентной способности, улучшения внутреннего контроля и т. д. Указанные показатели не надо выдумывать, они существуют в избыточном виде. Далее можно использовать методики рассчета *коэффициентов возврата инвестиций в инфраструктуру предприятия (ROI)*, например, также Gartner Group. По нашему мнению, достаточно результативно использовать следующую комбинацию: ***TCO*** как расходную часть и ***ROI*** как расчетную. Кроме того, сегодня существуют и другие разнообразные методы и технологии расчета и измерения различных показателей экономической эффективности.

КОНФОРМНОЕ ГАММИРОВАНИЕ ЗВУКОВОГО СИГНАЛА ХАОТИЧЕСКИМ СИГНАЛОМ

Жарких А.А.

Мурманский государственный технический университет

Введение

Цель данного сообщения – иллюстрация метода конформного гаммирования звукового сигнала хаотическим сигналом.

Традиционно гаммирование осуществляется над дискретными последовательностями источника с элементами из некоторого конечного алфавита. Для этого специальным образом подбирается последовательность гаммы с элементами из того же самого алфавита. Эта последовательность известна как отправителю, так и получателю. Отправитель складывает поэлементно по модулю алфавита последовательности источника и гаммы и передает результирующую последовательность в канал связи. Получатель принимает результирующую последовательность из канала связи и вычитает из нее поэлементно по модулю алфавита последовательность гаммы. В результате получатель получает последовательность источника. [1].

Существующие методы стеганографии основаны на традиционных разделах алгебры и дискретной математики. В данном сообщении предлагается метод гаммирования звукового сигнала, основанный на свойствах группы конформных преобразований единичного круга в себя [2]. В данной работе используется подгруппа указанной группы – группа преобразований в себя интервала $(-1;+1)$.

Считаем далее, что значения отсчетов звукового сигнала и хаотического сигнала гаммы нормированы и лежат в интервале (-1;1).

Математическое обоснование метода конформного гаммирования

Для упрощения записи выражений введем обозначения «конформной арифметики». Сумма двух чисел из интервала (-1;1) определяется выражениями (1) и (2). Произведение вещественного числа на число из интервала (-1;1) со значениями в интервале (-1;1) определяется выражениями (3) и (4).

$$\oplus : (-1;1)^2 \Rightarrow (-1;1) \tag{1}$$

$$\forall X, Y \in (-1;1)\ \ Z = X \oplus Y = \frac{X+Y}{1+XY} \in (-1;1) \tag{2}$$

$$\otimes : (-1;1) \times (-\infty;+\infty) \Rightarrow (-1;1) \tag{3}$$

$$\forall X \in (-1;1) \,\&\, \forall r \in (-\infty;+\infty)$$

$$Z = X \otimes r = \frac{(1+X)^r - (1-X)^r}{(1+X)^r + (1-X)^r} \in (-1;1) \tag{4}$$

Обозначим через $X_G(t)$ и $X_C(t)$ сигнал гаммы и скрываемый сигнал соответственно. Здесь традиционно через t обозначается время.

Определим алгоритм гаммирования следующей формулой:

$$S(\alpha, m, t) = X_G(t) \oplus \left(X_C\left(\frac{t}{m}\right) \otimes \alpha \right) \quad , \tag{5}$$

где α - параметр преднамеренного ослабления, m - параметр преднамеренного растяжения сигнала во времени. Назовем сигнал $S(\alpha, m, t)$ закрытым сигналом.

Алгоритм выделения скрытого сигнала из закрытого можно представить следующей формулой:

$$X_C(t) = \left(S(\alpha, m, mt) \oplus \left(X_G(mt) \otimes (-1)\right)\right) \otimes \frac{1}{\alpha}. \tag{6}$$

Математическое обоснование выбора хаотического сигнала гаммы

Мы полагаем, что при выборе хаотического сигнала –гаммы, необходимо руководствоваться следующими правилами:

- Генератор сигнала гаммы должен быть достаточно прост в реализации;
- Сигнал гаммы должен быть достаточно случайным;
- Значения сигнала гаммы должны изменяться в том же диапазоне, что и значения скрываемого сигнала;
- При передаче по каналу связи, скрываемый сигнал, сигнал гаммы и скрытый сигнал должны занимать одну и ту же полосу частот.

Первым двум требованиям удовлетворяет генератор, задаваемый квадратичным отображением [3]:

$$X_{N+1} = \mu X_N (1 - X_N) \, . \tag{7}$$

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

При выборе параметра $\mu_\infty < \mu > 4, \mu_\infty = 3.5699...$ и начального значения $0 < X_0 < 1$, генератор (7) порождает хаотическую последовательность значений в интервале $(0;1)$ [3].

Третье требование удовлетворяется простым масштабированием и смещением согласно (8):

$$R_N = 2X_N - 1. \quad (8)$$

В результате получается генератор сигнала с некоторым другим квадратичным законом (12):

$$R_{N+1} = 0.5\mu\left(1 - R_N^2\right) - 1. \quad (9)$$

При том же самом выборе параметра μ, а начального значения $-1 < R_0 < 1$, генератор (9) порождает хаотическую последовательность значений в интервале $(-1;1)$.

Наконец, последнему требованию можно удовлетворить, если считать элементы последовательности (9) нормированными отсчетами некоторого аналогового сигнала, взятыми с частотой дискретизации скрываемого сигнала.

Заключение

Рассмотренные в данном сообщении математические основы частично анонсировались в докладах [4,5].

Предлагаемый метод гаммирования имеет ряд существенных достоинств. Он легко реализуем в реальном времени, свободен от эффекта переполнения в «конформной арифметике», его преобразования обратимы с высокой степенью точности. Основным его недостатком является нестойкость по отношению к атакам криптоаналитика владеющего частичной информацией о сигнале гаммы.

Литература

1. .Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах, М.: Энергоатомиздат, 1996, 304 с

2. Кириллов А. А. Элементы теории представлений/М.:Наука, 1978, 343 с.

3. Лоскутов А.Ю., Михайлов А.С. Введение в синергетику.- М.: Наука, ГРФМЛ, 1991.- 272 с.

4. Жарких А.А. Конформное преобразование формы сигнала для защиты аналоговых сообщений// Международная научно – техническая конференция Калининградского ГТУ.- Калининград: КГТУ, 1999, Сборник тезисов и докладов, ч. 4, с. 123.

5. Жарких А.А., Конформная стеганография звукового сигнала в звуковом сигнале// XI – я Всероссийская конференция «Математические методы распознавания образов» (ВЦ РАН) , 2003, Сборник докладов, с. 305-307.

CONFORMAL METHOD OF HIDING THE SOUND SIGNAL IN THE CHAOTIC SIGNAL

Murmansk State Technical University

In this paper the new analogue method of hiding the sound signal in chaotic signal without the extension of the band of signal is presented. The method is based on the group on mapping unit circle itself and on quadratic generator of chaotic signal. Method can be realized by means of analogue circuits technique or software using float-point technique.

ПЕРЕДАЧА СЕКРЕТА В ОТКРЫТЫХ КАНАЛАХ СВЯЗИ НА ОСНОВЕ ОДНОГО КРИПТОГРАФИЧЕСКОГО ПРОТОКОЛА

Александров А.В.

Владимирский государственный университет

Развитие электронных сетей связи, глобальных информационных коммуникаций, повышение быстродействия вычислительных устройств постоянно стимулирует математические разработки более стойких методов защиты конфиденциальной информации, как на стадии хранения, так и в момент передачи информации в каналах связи. Появление новых методов криптографии связано с идеями использования так называемых односторонних функций. На их основе в широком цикле работ зарубежных математиков Diffi, Hellman, Rivest, Shamir, Adleman и др. (См. обширную библиографию в [1]) созданы ассиметричные криптографические системы, криптографические протоколы идентификации, разделения секрета, протоколы доказательства с разглашением и без разглашения. Внедрение асимметричных криптографических методов в сферу секретности на уровне государственных интересов ограничено следующим соображением. Факт существования односторонних функций математически строго не доказан. На сегодняшний день доказатель-

ство существования таких функций опирается на недоказанную гипотезу о несовпадении классов алгоритмически *P*- сложных и *NP*- сложных задач: $P \neq NP$. Из недоказанности гипотезы следует, что существует постоянная возможность того, что в результате новых теоретических продвижений в проблемах алгоритмической сложности факторизации длинных целых и вычисления дискретного логарифма, асимметричные криптографические системы в одночасье перестанут быть секретными. Подобная ситуация имела место, например, с криптографической системой, в основе которой использовалась функция, основанная на решении задачи "об укладке рюкзака". После того, как был найден корректный полиномиальный алгоритм взлома шифра эта система вышла из употребления.

Математическая ненадежность односторонних функций является главной причиной, по которой государственные стандарты шифрования России, США и других стран используют идеи одноключевой криптографии. Математическая теория таких систем в исключительно завершенном виде разработана Клодом Шенноном [2].

Настоящая работа посвящена изучению вопроса передачи секрета в надежно действующих открытых каналах связи на основе протокола взаимодействия между центром C и множеством его агентов $M = \{A_1, A_2, ...\}$. Протокол обладает устойчивостью как по отношению к пассивным противникам, осуществляющих прослушивание каналов, так и по отношению к активным. Активный противник может работать в канале связи на уровне замены сообщений и ключей. Идея создания подобного разового протокола взаимодействия для передачи закрытого текста между двумя абонентами рассматривалась в [5]. В отличие от работы [5], в нашей статье раскрывается ответ на дополнительный вопрос: как передать из центра C секрет S на основе передач нейтральных сообщений или дезинформаций (обозначим эти сообщения D_j). Такой подход к постановке вопроса открывает возможности для центра C двойной игры в каналах связи как с пассивным так и с активным противником, исключая при этом аналогичную возможность по отношению к центру C со стороны противника. В основу протокола взаимодействия информационного центра C с множеством абонентов $M = \{A_1, A_2, ...\}$ положен абсолютно стойкий – по Шеннону шифр Вернама. Для разделения секрета используется система разделения секрета (СРС), введенная А.Шамиром [3], гарантирующая необходимый порядок разделения секрета.

Обозначим $A = \{a_0, ..., a_m\}$ алфавит сообщений, $|A| = m$. Пусть S открытый конфиденциальный текст, $S = s_1 ... s_l$, $\forall j = 1,...l$, $s_j \in A$. Для краткости сообщение $S = s_1 ... s_l$ называем секретом. В качестве криптографической системы выберем шифр Вернама [2] с неповторяющимся ключом $K = k_1 ... k_l$, $\forall j = 1,...l$, $k_j \in A$.Шифрование заключается в преобразовании открытого текста $S = s_1 ... s_l$ в текст $V = v_1 ... v_l$ по правилу

$$V(s_i, k_i) = (s_i + k_i) \bmod(m+1) \quad , \tag{1}$$

где k_i выбираются случайно и независимо из диапазона 0..n. Очевидно, что преобразование (1) обратимо

$$V^{-1}(v_i, k_i) = (v_i - k_i) \bmod(m+1). \tag{2}$$

Шенноном в [2] показано, что при условии однократности использования ключа $K = k_1 ... k_l$ и случайности последовательности k_i система (1) обладает свойством совершенности в том смысле, что перехват криптограммы $V = v_1 ... v_l$ не дает противнику никакой информации о передаваемом сообщении $S = s_1 ... s_l$, даже если противник обладает неограниченными вычислительными ресурсами. На практике наиболее часто используется модификация шифра Вернама для алфавита $|A| = 2^n$, где символам сообщения сопоставлен равномерный полный двоичный код длины *n*. В этом случае в (1)-(2) операции сложения и вычитания по модулю *n+1* заменяются на логическую операцию исключающего или XOR=$\oplus$. Эта операция применяется побитно к двоичным кодам символов:

$$V_{\oplus}(s_i, k_i) = s_i \oplus k_i, \quad V_{\oplus}^{-1}(v_i, k_i) = V_{\oplus}(v_i, k_i) = v_i \oplus k_i = s_i \tag{3}$$

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

Шифрование и дешифрование в (3) реализуется одним алгоритмом на одинаковом ключе. С операторной точки зрения метод шифрования $V_{\oplus}(k)$ инволютивен:

$$\forall k, \quad \forall S \quad V_{\oplus}(k) \circ V_{\oplus}(k) = E, \tag{4}$$

где *E* тождественное преобразование.

Выделим еще одно свойство шифра (3) – (4), необходимое нам для дальнейшего. В силу симметричности схемы шифрования и дешифрования, равенства длин сообщения и длин ключей, криптосистема $V_{\oplus}(k)$ обладает свойством полноты:

Лемма 1 *Для любых двух сообщений S_1 и S_2 одной и той же длины существует ключ K, такой, что* $V_{\oplus}(S_1, k) = S_2$.

Этот факт следует из равенств $S_1 \oplus S_2 = k$, $S_1 \oplus (S_1 \oplus S_2) = S_2$

В силу подобия систем Вернама (1) и метода (3), лемма 1 для криптографической системы Вернама также имеет место.

Под схемой разделения секрета понимается алгоритм распределения секрета на "проекции" между владельцами секрета таким образом, чтобы заранее разрешенные множества участников могли однозначно восстановить секрет, действуя совместно по определенному протоколу взаимодействия. Если неразрешенные участники при этом не получают никакой дополнительной к априорной информации о значении секрета, то схема называется совершенной СРС. Первые постановки задач разделения секрета восходят к работам Блейкли Г. [4], и связаны с попытками решения задач коллективного владения информацией в ситуации недоверия владельцев секрета друг к другу.

Определение 1.[1] Схема Разделения Секрета (СРС) на *n* проекций имеет порядок секретности (*n,k),* если ровно *k* любых участников разрешенного множества $\tilde{M}, \left|\tilde{M}\right| = n$ могут восстановить секрет S по имеющимся у них данным, и никакие $l < k$ участников разрешенного множества $\tilde{M}$ восстановить секрет не в состоянии.

Определение 2.[1] Абонент A_i называется несущественным, если для любого элемента неразрешенного множества $M \setminus \tilde{M}$ множество $(M \setminus \tilde{M}) \bigcup A_i$ также неразрешенное.

Несущественные абоненты настолько несущественны для разделения секрета, что им можно не посылать никакой информации.

В основе схемы разделения секрета А. Шамира [4] лежит теорема о единственности восстановлении многочлена степени *n* над полем Z_P вычетов по модулю простого числа

$$p_n(x) = a_n x^n + \ldots + a_1 x + a_0 \tag{5}$$

по его значениям $p_n(x_i)$, *i=1,2,...n+1* в *n+1* точках. Выберем поле вычетов по модулю простого числа *p, Z_p, p>*$\left|\tilde{M}\right|$. Сопоставим участникам разрешенного множества $\tilde{M}$ индексы $\{1,\ldots,n\}$, и положим $a_0 = S$. Для распределения секрета $S = a_0$, центр генерирует *n* независимых, равномерно распределенных на Z_p случайных коэффициентов многочлена a_i, *i=0,...,n-1*, и высылает абонентам A_i значения $p_n(i)$. Элементы множества $\tilde{M}$ совместно решают задачу интерполяции, восстанавливая многочлен (5), вычисляют секрет $p_n(0) = a_0 = S$.

Лемма 2 [4] Схема разделения секрета А. Шамира имеет порядок секретности (n,n) в (5).

Лемма 3 (О процедуре компрометации канала связи).

Пусть D_i и D_j исходные сообщения, и $\tilde{D}_i$ и $\tilde{D}_j$ – соответственно сообщения, полученные абонентами. Обозначим $\delta_{ij} = D_i \oplus D_j$. Тогда факт подмены пары сообщений обнаруживается соотношени-

ем $\Delta_{ij} = D_i \oplus D_j \oplus \tilde{D}_i \oplus \tilde{D}_j \neq 0$. В частности, если подменено одно из сообщений, то вычисляется его индекс i и само сообщение $\tilde{D}_i$

Доказательство. Первая часть леммы очевидна. Для доказательства второй части, для определенности положим $\tilde{D}_i = D_i$ Тогда восстановление индекса j и измененного сообщения следует из соотношений $D_i \oplus D_j \oplus D_i \oplus \tilde{D}_j = D_j \oplus \tilde{D}_j = \Delta_{ij}$ и очевидного $\Delta_{ij} \oplus D_j = \tilde{D}_j$.

Обсудим теперь сам криптографический протокол. Рассмотрим постоянно действующую сеть, состоящую из Центра C и множества абонентов M, с каждым из которых используется отдельный канал связи. Абонент A_i идентифицируется парой (i, x_i), где второй параметр x_i - пароль абонента. Обычный режим взаимодействия $C \leftrightarrow A_j$ состоит в пересылке либо открытых документов D_j. Для всех $A_i \in M$ центр высылает попарно различные открытые тексты D_i. Некоторые из них могут иметь дезинформирующий для противника характер, но абоненты об этом не должны знать. Абоненты $A_i \in M$, постоянно вычисляют $D^{ij}{}_{\oplus} = \underset{i,j \in M}{D_i \oplus D_j}$ и высылают их в центр для контроля целостности сообщений и обнаружения фактов подмены сообщений D_j в каналах связи. В силу леммы 3 индекс i скомпрометированного канала и само подмененное сообщение легко вычислить, когда имеется хотя бы одно нескомпрометированное сообщение. В случае утечки информации D_i, скомпрометированным считаем как абонента A_i, так и канал связи с таким индексом i.

На момент, когда возникает потребность передачи из центра C секрета S, создается множество $\tilde{M} \subseteq M$, из которого исключены скомпрометированные агенты и агенты со скомпрометированными каналами связи. Пусть $|\tilde{M}| = 2n+1, n \geq 1$. Абоненты множества $M \setminus \tilde{M}$ для дальнейших пунктов протокола несущественны.

Для существенных участников $\tilde{M} \subseteq M$ центр создает ключи $k_i = S \oplus D_i$. Это всегда можно сделать в силу леммы 1. Центр держит сообщение S и ключи k_i в секрете. Далее центр создает общий слепок ключей

$$K_{\oplus} = \bigoplus_{j \in \tilde{M}} k_j \tag{6}$$

Пользуясь схемой линейного разделения секрета А.Шамира [4], ключ $K_{\oplus}$ подвергается числовой декомпозиции на *n* проекций: $K_{\oplus} = \tilde{k}_1, \ldots, \tilde{k}_n$. Проекции $\tilde{k}_i = p_n(x_i)$ передаются по каналам связи абонентам $A_i \in \tilde{M}$. Абоненты $A_i \in \tilde{M}$, решая задачу интерполяции, восстанавливают слепок ключей $K_{\oplus} = \bigoplus_{j \in \tilde{M}} k_j$, и используют его для восстановления секрета S с помощью операции $D_{\oplus} \oplus K_{\oplus} = S$.

Свойства криптографического протокола сформулируем в виде теорем.

Теорема 1. Пусть $|\tilde{M}| = n,\ n \in N, n > 2$. Тогда:

$$D_{\oplus} \oplus K_{\oplus} = \begin{cases} S, \textit{если} \quad n - \textit{четно} \\ 0, \textit{если} \quad n - \textit{нечетно}, \end{cases} \tag{7}$$

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

в частности, для нечетного числа участников разрешенного множества криптографический протокол корректен.

Доказательство: В силу (6)

$$D_{\oplus} \oplus K_{\oplus} = \bigoplus_{i\in\tilde{M}} (D_i \oplus k_i) \oplus K_{\oplus}) = (\bigoplus_{i\in\tilde{M}} (S \oplus k_i)) \oplus (\bigoplus_{i\in\tilde{M}} k_i) = (\bigoplus_{i\in\tilde{M}} S) = \begin{cases} S \\ 0 \end{cases},$$

где в последнем равенстве в силу идемпотентности порядка 2 операции $\oplus$ важна нечетность или четность количества слагаемых S.

Теорема 2. *Криптографический протокол имеет порядок разделения секрета (n,n), где* $n = \left|\tilde{M}\right|$, *и n нечетно.* Доказательство: Следует из теоремы 1 и леммы 2.

Литература

1. Введение в криптографию. Новые математические дисциплины. / Под. ред. В.В.Ященко // МЦНМО Санкт-Петербург, 2001. – 288 с.

2. К. Шеннон Работы по теории информации и кибернетике. // ИИЛ, Москва 1963, 829 с.

3. Shamir A How to Share a Secret // Comm. ACM/. V. 22, №1, 1979, P612-613.

4. Blakely G.R. Safeguarding cryptographic keys//Proc. AFIPS 1979 National Computer Conference. V.48. N.Y., 1979. P.313-317.

5. Dolev D., Dwork C., Waarts O., Yung M. Perfectly secure message transmission // Proc. 31st Annu. Symp. On Found. Of Comput. Sci. 1990, P.36-45.

МЕТОДИКА ИССЛЕДОВАНИЯ СТРУКТУРЫ АКУСТИЧЕСКОГО ПОЛЯ МНОГОЭЛЕМЕНТНОГО УЛЬТРАЗВУКОВОГО ДАТЧИКА

Смагин М.А., Морозов А.В., Сапожников О.А

Московский Государственный Университет им. М.В. Ломоносова
Россия, 119992 Москва, Ленинские горы, МГУ, физический факультет
Тел.: (095) 939-2952, E-mail: asign1@yandex.ru

Для проведения качественной ультразвуковой диагностики важно точно знать свойства применяемых источников и уметь предсказывать структуру их акустического поля. В силу сложности конструкции используемых в медицине акустических датчиков, особенно многоэлементных фазированных решеток, теоретически трудно предсказать структуру механических колебаний поверхности решетки и выявить свойства и конфигурацию излучаемого ею поля. Поэтому представляет большой интерес разработка альтернативных методов исследования акустических полей. Один из них основан на методе акустической голографии, позволяющем восстановить картину колебаний поверхности акустического излучателя на основе измеренных вдоль некоторой поверхности амплитуды и фазы волны [1].

В данной работе проведено исследование поля многоэлементного медицинского датчика Medelkom 3.5 C60 абдоминального типа, с рабочей частотой 3.5 МГц и 96-элементной излучающей поверхностью. Внешний вид датчика изображен на рис. 1. При использовании в медицинской диагностике к каждому элементу подводится отдельный провод, чтобы иметь возможность проводить фокусировку и сканирование поля в плоскости *yz* (см. рис. 1) путем введения соответствующих фазовых сдвигов между подаваемыми на элементы сигналами [2]. В плоскости *xz* производится слабая фокусировка за счет цилиндрической линзы, расположенной на поверхности излучателя (на рис. 1 не показана). При проведении данной работы все элементы решетки электрически соединялись, т.е. на них подавался один и тот же сигнал. Указанный синусоидальный сигнал подавался с генератора сигналов Agilent и имел вид радиоимпульсов с прямоугольной огибающей, частотой заполнения 3.5 МГц и амплитудой 10 В. Датчик помещался в кювету с водой.

Сначала проводились измерения распределения акустического давления в поперечной плоскости. Игольчатый пьезокерамический гидрофон диаметром 0.4 мм (SEA, USA) перемещался в нужной плоскости с помощью системы позиционирования. Сигнал гидрофона считывался цифровым осциллографом Tektronix. Были исследованы распределения акустического давления по двум направлениям в поперечной плоскости на различных расстояниях от датчика. На рис. 2 представлены графики этих распределений по горизонтальной и вертикальной осям соответственно. Отчетливо видна тонкая структура акустического поля, обусловленная как дифракционными эффектами ближнего поля, так и многоэлементной структурой источника.

Как видно, поле локализовано в области размером 40x10 мм, что примерно соответствало геометрическому размеру источника. С учетом полученного поперечного размера акустического пучка, далее проводилось двумерное сканирование гидрофона в соответствующей прямоуголной области на расстоянии z=2 см перед излучающей поверхностью. Данное расстояние было выбрано, как минимальное при проведении обследований реальными медицинскими приборами и позволяло четко разделять вклад каждого элемента в общую структуру поля. Результат измерения для амплитуды сигнала гидрофона приведен на рис. 3. Наряду с амплитудой, проводилось измерение фазы волны. Указанная информация использовалась для голографи-

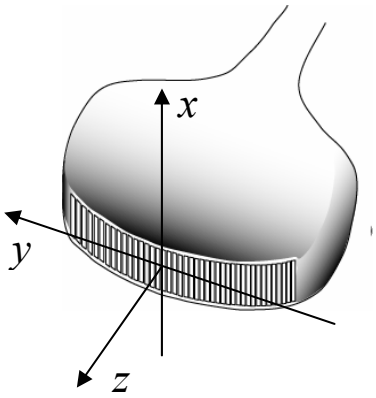


Рис.1. Расположение координатных осей при сканировании поля многоэлементного ультразвукового датчика.

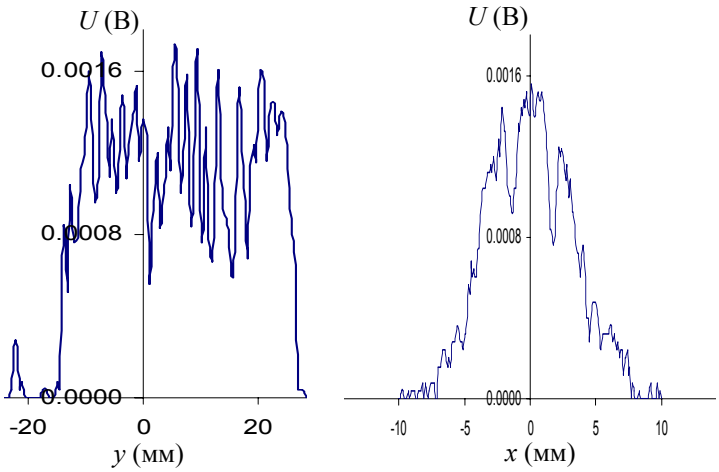


Рис. 2. Распределение амплитуды акустического давления (сигнала гидрофона U) вдоль горизонтальной (слева) и вертикальной (справа) осей на расстоянии z=20 мм.

ческого восстановления распределения колебательной скорости на поверхности источника. Результат восстановления показан на рис. 4. Видно, что распределение скорости отражает многоэлементную структуру и геометрические размеры используемого излучателя. Таким образом, проведенные исследования позволяют сделать вывод о возможности исследования структуры колебаний и точного предсказание полей многоэлементных решеток, используемых в медицине.

Литература

1. Сапожников О.А., Пищальников Ю.А., Морозов А.В. Восстановление распределения нормальной скорости на поверхности ультразвукового излучателя на основе измерения акустического давления вдоль контрольной поверхности // Акуст. ж., 2003, т.49, №3, с.416-424.

2. Осипов Л.В. Ультразвуковые диагностические приборы: Практическое руководство для пользователей // М.: Видар, 1999.

An ultrasound probe acoustic field structure investigation method was developed and tested. This method based on acoustic holography allows to reconstruct probe surface vibrations and to predict precisely acoustic field structure of multielement ultrasound probes.

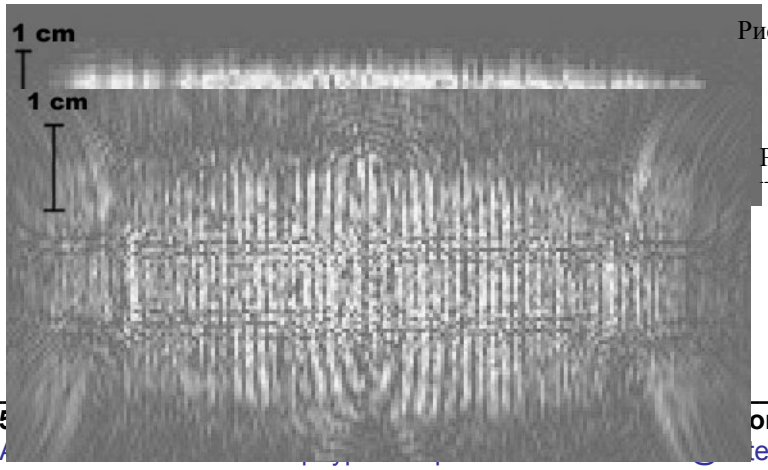


Рис. 3. Измеренное распределение

Рис. 4. Восстановленное

СИСТЕМА УПРАВЛЕНИЯ ПАРОЛЯМИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ

Воронин А.А., Илларионов Ю.А., Казарин А.Ю., Михайлов А.В.

Владимирский государственный университет

Проблема эффективного и надежного управления паролями пользователей сети Интернет стала весьма актуальной за последние 5 лет. Вместе с бурным ростом этой сети, улучшением качества услуг и увеличением количества клиентов одновременно значительно возросли убытки пользователей сети Интернет в связи с несанкционированным использованием их логина (имени и пароля для доступа в Интернет). Кража логинов с целью их перепродажи сейчас является одной из выгоднейших статей дохода начинающих, и не только, хакеров. Кража пароля может выполняться различными способами, например, с помощью вирусов - сканеров клавиатуры, а может и просто по невнимательности пользователя, потерявшего лист с паролем. Кроме того, подрастающее поколение все больше интересуется компьютерами и Интернетом, и, как следствие, участились кражи логинов друзьями детей родителей, имеющих доступ к сети.

В системе eToken Internet Logon, разработанной авторами на основе алгоритмов, предложенных в [1], вопрос хранения логина для доступа в Интернет во многом был решен. Основное преимущество данной системы заключается в том, что логин не хранится на компьютере и в отсутствие клиента никто им не воспользуется. Все данные, необходимые для доступа в Интернет, хранятся в ключе eToken (маленьком брелоке, размером с обычный ключ), который можно носить с собой. Такой ключ стыкуется с компьютером через порт USB, что позволяет без труда подключать и отключать его от компьютера по мере необходимости.

Даже в случае утери или кражи брелока доступ к его внутренним данным для посторонних лиц практически невозможен из-за необходимости ввода пароля (PIN-кода, известного только владельцу), причем данные, хранимые в брелоке, шифруются им же при помощи криптостойкого алгоритма DES-X. В случае пропажи брелока (утери по неосторожности или воровства) достаточно связаться с провайдером, предоставляющим услуги доступа в Интернет, для смены логина.

Основные принципы и цели разделения функций в системе eToken Internet Logon. Согласно методу, предложенному в [1], наибольшей эффективности при организации защиты ресурса (в данном случае защищаемым ресурсом являются реквизиты доступа клиента в сеть Internet) от несанкционированного доступа можно добиться, применяя программно-аппаратурные решения, в которых защищаемая система разделяется на стационарную и мобильную части. В системе eToken Internet Logon стационарная часть реализована программно, являясь при этом модулем операционной системы (ОС) Windows 98/2000; мобильная аппаратурная часть представлена электронным ключем (ЭК) eToken производства компании Aladdin. При этом на программную часть возлагаются основные интеллектуальные функции, обеспечивающие стыковку ЭК с ОС, организацию подключения к провайдеру Internet, идентификацию клиента и поддержку сеанса связи. ЭК используется как миниатюрное мобильное устройство памяти, хранящее в себе все реквизиты доступа клиента.

Таким образом, подобное разделение функций позволяет избавиться от необходимости ввода реквизитов с клавиатуры при проведении процедуры регистрации (это делает невозможным перехват реквизитов с помощью вирусов-троянцев), а также избавиться от необходимости хранения реквизитов в виде файлов ОС. Таким образом, из стационарной (защищаемой) части системы реквизиты изымаются и переносятся в мобильную часть. Никакими «хакерскими» методами из стационарной части (т.е. компьютера) их невозможно украсть по причине отсутствия таковых. Из мобильной части (т.е. ЭК eToken) украсть их также невозможно, поскольку во время сеанса связи доступ к ЭК контролируется не ОС Windows, а программным обеспечением системы eToken Internet Logon; по окончании сеанса ЭК изымается из компьютера и помещается в надежное место.

Рассмотрим подробнее организацию системы eToken Internet Logon. Электронный ключ-брелок eToken использует протокол APDU (Application Protocol Data Unit), являющийся последовательностью команд, которые могут посылаться приложением в eToken R2. Протокол, используемый приложением, обычно является верхним транспортным уровнем. Протокол APDU позволяет посылать в eToken R2 команды и получать от него ответ.

Стандарт ISO 7816-4 определяет функциональные аспекты APDU, важные для приложений, использующих смарт-карты. Есть две основные особенности, применимые к eToken R2:

1. Смарт-карты имеют иерархическую файловую систему. Определен набор функций, которые может использовать приложение, для получения доступа к файлам смарт-карты и содержащейся в них информации.

2. Доступ приложения к файлам смарт-карты возможен только после выполнения определенных процедур безопасности.

Структура пакета APDU, определенная в ISO 7816-4, очень похожа на структуру пакета TPDU, описанную в ISO 7816-3 для протокола T=0. Протокол APDU является независимым от реализации протокола физической связи и реализуемым на уровне приложения. Пакет (команда) APDU включает заголовок и тело, которые, в свою очередь состоят из отдельных полей. Заголовок пакета состоит из полей CLA, INS, P1 и P2. Поля CLA и INS определяют класс приложения и код инструкции, поля P1 и P2 являются командными параметрами. Тело пакета имеет переменный размер и формат. Тело служит для передачи данных, характерных для исполняемой инструкции, а так же для получения ответа после ее выполнения. Поле P3 содержит длину в байтах блока данных DATA FIELD, который будет передан в eToken R2 как часть текущей инструкции. Поле DATA FIELD содержит данные, необходимые для выполнения текущей инструкции. Поле LE содержит длину в байтах ожидаемого ответа после завершения выполнения текущей инструкции. ЭК eToken R2 имеет файловую систему, которая является подмножеством файловой системы, описанной в ISO 7816-4 и имеет следующие характеристики:

- иерархичность – поддерживаются каталоги и подкаталоги;
- короткие имена не поддерживаются;
- длина файла задается при его создании и не может быть изменена в дальнейшем;
- файловая система в любой момент времени имеет текущий каталог, текущий файл или ключ.

Файловая система eToken R2 поддерживает различные атрибуты безопасности. Атрибуты назначаются при создании файла и не могут меняться в дальнейшем.

Литература

1. Илларионов Ю.А., Монахов М.Ю. Безопасное управление ресурсами в распределенных информационных и телекоммуникационных системах: Моногр./ Владим.гос.ун-т, Владимир, 204. – 204 с.

ВИРТУАЛЬНЫЙ КЛАСТЕР И DDOS-АТАКИ

Воронин А.А., Илларионов Ю.А., Калмыков М.С., Казарин А.А., Михайлов А.В., Монахов М.Ю.

Владимирский государственный университет

Основными целями, преследуемым при организации *DDoS*-атак [1] являются либо перегрузка канала связи, либо сервера, который осуществляет обработку запросов. И то, и другое, в лучшем случае, приведут к увеличению времени обработки запросов, что может быть расценено пользователями как отказ системы.

Рассматривая классическую модель организации *DDoS*-атак применительно к кластерной структуре, можно выделить большое сходство. Используемые в качестве атакующих компьютеры–зомби могут являться серверами кластера. При организации системы на базе виртуального кластера добавляется еще одна особенность – отследить источник атаки (реально атакующую систему), не являющуюся зомби, практически невозможно. В классической кластерной структуре подобные обращения от сервера кластера вывели бы неизбежно на атакующую систему. Для виртуального кластера подобное практически невозможно (для выявления требуется серьезный анализ компьютера–зомби).

Проверка уязвимости *Web*-серверов на *DDoS*-атаки. Сложность выявления, а точнее, подтверждения участия компьютера-зомби в атаке (выявить компьютер можно обратной трассировкой) определяется тем, что при организации атаки не используется нестандартное (вирусоносное) программное обеспечение, которое может быть выявлено антивирусными программами. Использование *web*-браузера сильно ограничивает возможность обнаружения «атакующего модуля» на пользовательском компьютере. К тому же дополнительные средства управления *web*-браузерами, предоставляемые используемыми языками теговой разметки страниц (в частности, языком *HTML*), позволяют «замести» все следы своей активности на «зараженной» системе (например, запретив кэширование *web*-страниц в которые встроен атакующий код). Тогда завершив работу с *web*-браузером, пользователь уничтожит все следы.

С другой стороны, постоянное изменение состава и местоположения серверов обработки виртуального кластера не позволяет организовать достаточно приемлемый уровень защиты от подобных атак. В данном случае невозможно выделить подсеть, из которой поступают атакующие запросы. Особенно ситуация обостряется при «захвате» *web*-портала с высоким уровнем посещаемости (например, поисковых систем). В такой ситуации атака может продолжаться довольно длительное время, практически со «всех подсетей», что не дает возможности организовать защиту.

Однако в «мирных целях» подобная возможность может использоваться для проверки систем безопасности на *DDoS*-атаки, для тестирования алгоритмов обнаружения атакующих систем, для выявления потенциальных возможностей для атак. Для примера, организация может использовать локальную сеть для тести-

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

рования надежности установленного *web*-сервера, развернув в пределах локальной сети виртуальный кластер и имитировав атаку на сервер.

В данном случае можно воспользоваться как подходом на базе «черного ящика», используя стандартные (выявленные) уязвимости *http*-серверов, так и подходом на базе «белых ящиков», внедрив в атакующие системы информацию о структуре сервера. В обоих случаях проверка может быть выполнена до подключения *web*-сервера к сети *Internet*.

Другой возможностью применения является тестирование каналов передачи информации телекоммуникационной сети. В данном случае виртуальный кластер может использоваться для выявления максимальной пропускной способности канала передачи, где для организации стабильного потока запросов по выделенному каналу может также использоваться локальная сеть предприятия.

Приведем общий алгоритм организации управления виртуальным кластером для *DDoS*-атак.

Алгоритм управления виртуальным кластером при организации DDoS-атак

Шаг 1. Размещение модуля управления на атакующем компьютере (http-сервер с высокой посещаемостью). Процедура может заключаться в добавлении кода на стартовую страницу web-сайта.

Шаг 2. Ожидание сообщения контрольной программы на подключение к кластеру.

Шаг.3. Передача информации об атакуемой системе и начало атаки для сервера обработки. Для повышения скрытности атакующей системы может проводиться анализ адресов серверов обработки с целью избежания их принадлежности одной подсети.

Шаг 4. Ожидание сообщения контрольной программы о результатах атаки. Наличие этапа зависит от целей атаки. Если не предполагается получение требуемых данных от атакуемой системы, то данный этап можно исключить.

Шаг 5. Проверка достижимости цели. Если целее не достигнута, перейти к шагу 2, иначе конец алгоритма.

Повышение уровня защищенности *Web*-серверов при *DDoS*-атаках. Рассмотрим типовую *DDoS*-атаку. Атакующая система осуществляет захват компьютера-зомби, который собственно и будет производить атаку. На данной фазе повлиять на процесс захвата невозможно. Далее, когда компьютеры-зомби начинают атаку на *web*-сервер, который управляет виртуальным кластером, согласно описанному ранее принципу, происходит следующее. *Web*-сервер, при резком возрастании нагрузки, принимает решение о переключении на определенную последовательность обработки виртуального кластера. Тогда компьютеры-зомби становятся серверами обработки кластера, и на них перенаправляется часть входящих запросов. Таким образом, атакующие компьютеры, будут помогать справляться с нагрузкой, в то время как атакуемая система может осуществить запуск процедуры выявления подобных атак и поиск атакующей системы.

Конечно, подход имеет ряд недостатков, среди которых основным является дополнительное понижение пропускной способности канала связи к коммутатору кластера. Однако появляется очень интересная возможность решения проблемы. Если *web*-сервер «успел» (например, в случае подтверждения факта атаки) переместить часть своей базы данных и функциональное наполнение на серверы обработки, то после перегрузки коммутатора или канала связи с коммутатором, серверы начнут процесс выборов нового коммутатора.

После завершения выборов, получим работающий web-сервер, правда с меньшей функциональностью и меньшей базой данных (зависит от уровня разделяемой базы данных). Атакующая система, не достигнув цели, либо прекратит атаку, либо переместит ее на сервер обработки, осуществляющий в данный момент функции коммутатора кластера и *web*-сервера. В худшем случае могут потребоваться новые выборы коммутатора кластера, а в лучшем - перемещение атаки на сервер обработки обеспечит уменьшение нагрузки на исходный *web*-сервер и освобождение канала связи до него, восстановив его работоспособность в полном объеме. Таким образом, сервер обработки в данном случае выступает в качестве дублирующей и отвлекающей системы.

Литература

1. Howard F. Lipson, Ph.D. – Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, CMU/SEI-2002-SR-009, – CERT Coordination Center, – http://www.cert.org/archive/pdf/02sr009.pdf.

ПОДСИСТЕМА КОНТРОЛЯ ДОСТУПА К КОМПЬЮТЕРАМ В РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СИСТЕМЕ

Воронин А.А., Илларионов Ю.А., Казарин А.Ю., Михайлов А.В., Монахов М.Ю., Полянский Д.А.

Владимирский государственный университет

Во Владимирской распределенной информационной образовательной системе [1] (РИОС) действует комплекс стандартных средств защиты информации, созданы специальные инструкции для пользователей и администраторов. Тем не менее, каждый элемент системы может содержать как минимум одну уязвимость, позволяющую злоумышленнику проникать в РИОС с целью похищения или модификации данных и (или) программ (атака системы). При этом, в принципе, возможен последующий анализ механизма проникновения в систему, однако, в сиу ее сложности и достаточно высокой частоты атак «ручной» анализ событий становится практически невозможным. Таким образом, назрела необходимость создания автоматической службы, способной отслеживать события в РИОС, анализировать их на предмет выявления подозрительных событий и подозрительных последовательностей событий, блокировать доступ при выявлении подобных последовательностей, протоколировать их и сообщать соответствующим службам о наличии атаки. Уникальной подсистемой для систем данного класса является подсистема контроля доступа к компьютерам [2], функционирующая во Владимирской РИОС.

Предпосылкой ее появления явились факты несанкционированного доступа пользователей к специальным защищенным информационным ресурсам РИОС (чаще всего к подсистеме тестирования), число которых постоянно растет. Атакам постоянно подвергаются как центральные так и дочерние серверы. Была поставлена задача фиксации такого рода инцидентов и их анализа.

Основные задачи подсистемы контроля доступа:

- фиксирование действий пользователей за рабочими станциями;
- работа в режиме реального времени;
- быть незаметной для пользователей.

В РИОС подавляющие большинство компьютеров работают под управлением MS Windows 98, поэтому разработанная подсистема ориентированна именно на эту ОС. Применительно к ней выделены действия пользователя, подлежащие контролю: запуск процессов; нажатие клавиш; доступ к файлам; доступ к реестру.

Запуск процессов – позволяет выявить факт использования несанкционированного программного обеспечения. Нажатие клавиш – позволяет определить характер работы пользователя с приложениями. Доступ к файлам – позволяет выявить несанкционированный доступ к данным, а также случаи нецелевого использования дискового пространства. Доступ к реестру – позволяет выявить факты несанкционированного изменения конфигурации программного обеспечения.

С точки зрении организации вычислительного процесса подсистема представляет собой множество взаимодействующих процессов-агентов, запускаемых на каждой машине РИОС и скрытых от пользователя. Все агенты работают на супервизорном уровне и обладают привилегиями операционной системы. Для координации взаимодействия агенты обмениваются сообщениями в соответствии с протоколом взаимодействия агентов.

В качестве примера приведем фрагменты файлов-журналов, полученные с одной из рабочих станций расположенной в лаборатории Владимирского государственного университета.

Статистика запускаемых приложений

Дата	Время	флаг	Путь
1.06.2004	12:05	Run	c:\users\ivt198\example.exe
1.06.2004	12:10	End	e:\windows\notepad.exe
1.06.2004	12:20	Run	C:\windows\system\gpr32gh.exe

Подозрительной показалась последняя строчка таблицы. После осмотра рабочей станции, оказалось что C:\windows\system\gpr32gh.exe являлся компьютерным вирусом.

Статистика доступа к файлам

дата	время	флаг	приложение	Путь
11.06.2004	09:05	Read	c:\graph.exe	c:\user\data.dat
11.06.2004	09:06	Write	e:\lab1.exe	e:\user\ex.txt

Поле приложение показывает приложение, которое осуществило доступ к файлу. Поле путь, указывает путь где хранится файл.

Статистика доступа к реестру

дата	время	флаг	приложение	Ключ
6.06.2004	22:05	Query	c:\runer.exe	HKEY_CURRENT_USER\ Software\Microsoft\Windows\Current Version\Run\
6.06.2004	22:10	Write	c:\runer.exe	HKEY_CURRENT_USER\ Software\Microsoft\Windows\Current Version\Run\

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

На основании этих данных видно, что приложение c:\runer.exe изменило ключ реестра, отвечающий за автозапуск приложений.

Статистика нажатий клавиш

13.06.2004	14:17	Internet Explorer - test	ab z13{enter}fd
13.06.2004	14:18	The Bat!	{esc}фываord

За время работы комплекса, составляющее чуть меньше месяца, было зарегистрировано 10 попыток несанкционированного доступа к центральному серверу ИОС, а также определено среднее время нецелевого использования компьютеров локальной сети в составе РИОС, составившее примерно 1 час на 8 часов общего времени работы компьютера.

Литература

1. Монахов М.Ю. Информационная образовательная сеть: Основы теории и методика применения // Информационные технологии. №7. – 2001.

2. Монахов М.Ю., Воронин А.А. и др. Система контроля доступа к компьютерам в корпоративной сети // Проблемы обеспечения эффективности и устойчивости сложных технических систем: Сборник трудов XXII межведомственной научно-технической конференции. Серпухов. 2003.

ОСНОВНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ОТ КОЛЛЕКТИВНЫХ РАСПРЕДЕЛЕННЫХ АТАК НА ВЫЧИСЛИТЕЛЬНЫЕ РЕСУРСЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Воронин А.А., Калмыков М.С., Монахов М.Ю.

Владимирский государственный университет

Одной из наиболее опасных угроз для нормального функционирования распределенных информационных систем, функционирующих в сети Интернет, в последнее время становятся так называемые атаки типа “отказ в обслуживании” (*Denial of Service*, или сокращенно – *DoS,* и их наиболее опасная разновидность - распределённые коллективные атаки типа “отказ в обслуживании” (Distributed Denial of Service, сокращенно – DDoS). В настоящее время не существует достаточно эффективных методов защиты от коллективных распределенных атак типа «Отказ в обслуживании» (*DDoS*), позволяющих предотвратить нападение на отдельно взятую информационную систему, не меняя при этом основных алгоритмов функционирования сети Интернет. Инструменты для организации *DDoS*-атак все более усложняются, и в то же время они остаются легко доступны для загрузки из Интернет. Выделим основные проблемы защиты информационных систем, функционирующих в Интернете от *DDoS*-атак.

1. Переполнение буфера и другие логические атаки. Сложность защиты от *DoS*-атак на логическую целостность заключается в том, что все эти атаки основаны на использовании ошибок реализации алгоритма функционирования информационной системы. Поскольку эти ошибки уже присутствуют в системе, то для защиты от *DoS*-нападений необходимо либо устранить уже известные уязвимости (как правило – установить все последние «заплатки» с исправлениями от производителей операционной системы или конкретного программного продукта), либо использовать системы обнаружения вторжений (*Intrusion Detection Systems*, или сокращенно *IDS*) с постоянно обновляемой базой сигнатур атак, которые позволяют анализировать в реальном времени сетевой трафик защищаемой системы и автоматически блокировать пакеты, реализующие одну из известных атак. Оба этих способа достаточно трудоемки (нужно постоянно поддерживать в актуальном состоянии базу сигнатур *IDS* и устанавливать все последние обновления ОС и прикладного программного обеспечения). Кроме того, они не дают стопроцентной защиты от *DoS*-атаки, поскольку оба способа по сути своей реактивны, и всегда есть вероятность, что вновь обнаруженная уязвимость будет использована для масштабной атаки раньше, чем производитель системного или прикладного программного обеспечения выпустит соответствующее исправление, а *IDS* научится распознавать эту новую атаку.

Из всех перечисленных атак на логическую целостность системы, на данный момент наибольшее распространение получили *атаки переполнения буфера.* В качестве наиболее перспективного метода борьбы с данными атаками представляется использование аппаратной защиты от выполнения кода, находящегося в области памяти, предназначенной исключительно для хранения данных.

Эта технология на данный момент реализована аппаратно в 64-битных процессорах *AMD* (*Execution Protection*, или *NX-bit*) [1], а также в процессорах *Intel Itanium* (*Execute Disable Bit*), *Celeron D, Pentium* 4 и *Xeon* (ревизия *E*-0) [2].

На программном уровне технология предотвращения исполнения кода поддерживается в *Windows XP Service Pack* 2 и более поздних версиях [3], планировалась – в *Windows* 2003 *Service Pack* 1 (*Data Execution Prevention*).

2. Защита от *SYN-flood.* Одним из самых эффективных методов противодействия атаке *SYN-flood* является использование т.н. *SYN-cookies* [4]. Суть метода заключается в том, что при заполнении очереди неустановленных соединений сервер продолжает отвечать на новые запросы с помощью пакетов *SYN-ACK*. При этом сервер не заносит сведения о новом соединении в очередь, а для отслеживания соединения использует *SYN-cookie* – особым образом выбранный первоначальный номер последовательности *TCP*. Номер последовательности – стандартное поле пакета *TCP*, которое по стандарту выбирается произвольным образом при установке соединения (но при этом оно должно выбираться так, чтобы максимально затруднить злоумышленнику угадывание номера для каждого последующего соединения). При использовании *SYN-cookies*, часть номера последовательности содержит криптофункцию над *ip*-адресами клиента и сервера, номерами портов и счетчиком, увеличивающимся на 1 каждые 64 секунды. То есть сервер, отвечая на очередной *SYN*-пакет, кодирует в поле номера последовательности все необходимую информацию о соединении, и отправляет ее клиенту в пакете *SYN-ACK*. При получении от клиента третьего пакета (*ACK*) сервер проверяет номер последовательности (вновь вычисляет криптофункцию над параметрами соединения), и при совпадении заносит все данные о соединении в соответствующие структуры данных и далее обрабатывает соединение обычным образом.

Другим способом защиты от атаки *SYN-flood* является использование механизма *TCP intercept*, реализованного во многих сетевых экранах. Суть этого метода заключается в том, что сетевой экран перехватывает пакеты установки соединения (*SYN*) и сам отправляет ответ (*SYN-ACK*) от имени защищаемого сервера. И только в случае получения третьего пакета (*ACK*) от клиента (то есть после полного завершения процедуры установки соединения) сетевой экран устанавливает соединение с защищаемым сервером уже от имени клиента.

Таким образом, сетевой экран выступает посредником между клиентами и защищаемым сервером, и берет на себя проблемы, связанные с переполнением очереди полуоткрытых TCP-соединений. При таком подходе обеспечивается защита сервера от исчерпания ресурсов при атаке *SYN-flood*. Однако это не решает проблему полностью – ресурсы сетевого экрана тоже ограничены, и во время атаки он просто более агрессивно выбрасывает из своей очереди полуоткрытые соединения, а также жестко ограничивает скорость обработки новых *SYN*-пакетов. Поэтому при достаточно мощном потоке *SYN-flood* у законного клиента очень мало шансов на успешное соединение с сервером, и, таким образом, в результате атаки все-таки наступает отказ в обслуживании клиента, несмотря на то, что ресурсы сервера не исчерпаны.

3. Фильтрация пакетов с поддельными адресами. Одной из главных проблем противодействия атакам типа *DDoS* является трудоемкость обнаружения истинного источника атакующих пакетов, имеющих, как правило, поддельные адреса в поле отправителя. Эту задачу в большинстве исследований по данной тематике называют проблемой обратной трассировки (*backtrace*), поскольку большинство разрабатываемых методов основаны на постепенном построении (от точки назначения к источнику) полного маршрута, по которому проходят пакеты, участвующие в атаке. Сложность задачи определяется отсутствием универсальных методов реализации алгоритмов подобного поиска в условиях сложившейся инфраструктуры сети Интернет, ориентированной на максимально быструю коммутацию пакетов, исключающую всякую возможность анализа проходящих потоков.

Литература

1. AMD64 Execution Protection (NX-bit) (http://www.amd64.ru/index.php?link=2&addr=6&page=5)
2. Execute Disable Bit Functionality (http://www.intel.com/business/bss/infrastructure/security/xdbit.htm)
3. Changes to Functionality in Microsoft Windows XP Service Pack 2. Part 3: Memory Protection Technologies (http://www.microsoft.com/technet/prodtechnol/ winxppro/maintain/sp2mempr.mspx)
4. D.J.Bernstein – SYN Cookies (http://cr.yp.to/syncookies.html)

ОПЫТ СОСТАВЛЕНИЯ ДОКУМЕНТАЦИИ ДЛЯ ПОСТРОЕНИЯ СИСТЕМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Илларионов Ю.А., Михайлов А.В., Казарин А.Ю., Полянский Д.А.

Владимирский государственный университет

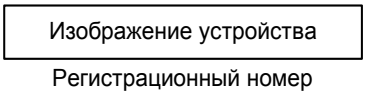
ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

Обеспечение безопасности информационно-вычислительных систем (ИВС) обычно связывают с выработкой политик (концепции) безопасности; применением комплекса специальных аппаратно-программных средств (антивирусы, брандмауэры, и т.д.) и их систематическим обновлением.

Эффективного выполнения задач защиты информации невозможно без знания структуры ИВС. Документирование ИВС является задачей нетривиальной. Для этого обычно используются системы управления сетевой инфраструктурой, которые стоят достаточно дорого. Альтернативой данному способу является применение стандартного программного обеспечения в совокупности с правилами оформления ИВС. Примером подобных правил являются «Правила построения топологических схем ИВС Владимирского государственного университета». В данных правилах рассматривается вариант документирования ИВС с использованием пакета MS Office и MS Visio. Рассмотрим данные правила оформленные в стандарте предприятия как рекомендации.

Рекомендации по созданию топологической схемы ИВС:

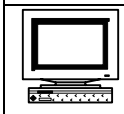
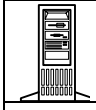
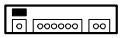
1. Разработка топологической схемы ИВС должна проводиться с использованием CASE средств Visio 2000 либо Visio 4.
2. На топологической схеме ИВС, отображаются устройства и линии связи. Под устройствами понимаются – телекоммуникационные устройства (модемы, концентраторы,…), а также вычислительные устройства (рабочие станции, серверы,…). Отображение ведется с привязкой к помещению, где расположены устройства.
3. Устройства должны отображаться следующим образом:



Изображение устройства – символическое изображение устройства, выбранное согласно таблице отображения устройств (Табл. 1). Регистрационный номер – уникальный идентификатор устройства в ИВС ВлГУ.

4. Изображения устройств и регистрационные номера должны отображаться в одном стиле, т.е. изображения должны быть одного масштаба, а текстовые надписи выполнены одним шрифтом, одинакового цвета и размера.
5. Устройства физически расположенные в одном помещении должны обрамляться прямоугольной областью, обозначающей данное помещение. При этом данная область должна быть поименована. Наименование помещения должно располагаться в правом нижнем углу прямоугольной области. Толщина линии, обозначающей помещение, должна быть в 3 раза больше толщины линий, обозначающих линии связи.
6. Для обозначения устройств должны использоваться наборы примитивов (Stencil). Для Visio200 – Basic Network Shapes (basic network shapes.vss), Basic Network Shapes 2 (basic network shapes2 .vss). Для Visio 4 –Network (network shapes.vss), Network(Additional) (network shapes 2.vss).
7. Символические изображения устройств показаны в Табл. 1.
8. Способы отображение линий связи приведены в Табл. 2. Линии связи должны быть изображены вертикальными и горизонтальными отрезками. Как и устройство, линия связи обязательно должна быть подписана регистрационным номером. Подпись линии связи должна быть выполнена таким образом, чтобы можно было однозначно идентифицировать конкретную линию связи.

Табл. 1

Код типа устройства		Наименование	Путь в наборе примитивов (Visio 2000)	Путь в наборе примитивов (Visio 4)
	WS	Рабочая станция	Basic Network Shapes-> Workstation	Network shapes.vss-> Workstation
	SRV	Сервер	Basic Network Shapes-> Tower box	Network shapes.vss-> Tower box
	H	Концентратор	Basic Network Shapes-> Hub	Network shapes.vss-> Hub
	R	Маршрутизатор	Basic Network Shapes 2 -> Router	Network shapes 2.vss-> Router

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

ОПРОСНЫЙ ЛИСТ КОМЬЮТЕРА			
Регистрационный номер			
Телекоммуникационные настройки			
Сетевой интерфейс			
РН подсоединенной ЛС			
Наименование телек-го у-ва			
MAC адрес			
IP адрес/маска подсети	Дин. ☐		
Шлюз по умолчанию			
DNS Имя			
Netbios имя (домен/имя)			
Программное обеспечение			
Тип ПО	Наименование ПО		
Системное ПО			
ОС (Service Pack)			

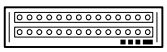
	SW	Коммута-тор	Basic Network Shapes-> MUX / DEMUX	Network shapes.vss-> MUX / DEMUX

Табл. 2

Символическое изображение	Код типа лини связи	Тип физической среды
_____	U	Неэкранированная витая пара
_____	S	Экранированная витая пара
_____	CX	Коаксиальный кабель
_ · _ · _ · _ · _ · _ · _	F	Оптоволокно

Правила именования помещений. Помещения именуются в соответствие с принятыми в ВлГУ правилами именования помещений. Если помещение не принадлежит ВлГУ, именовать его следует краткой аббревиатурой. Использованные аббревиатуры должны затем расшифровываться.

Формат регистрационного номера устройства

Формат регистрационного номера устройства =

([помещение])-[код типа устройства]-[порядковый номер]

Здесь: помещение – назначается согласно правилам именования помещений; код типа устройства – назначается в соответствии с таблицей отображения устройств; порядковый номер – число, идентифицирующие данное устройство, среди подобных устройств, эксплуатируемых в данном помещении.

Формат регистрационного номера линии связи

Формат регистрационного номера линии связи =

([помещение 1])-([помещение 2])-[код типа линии связи]-[порядковый номер]

Здесь: помещение 1 – помещение, откуда начинается линия связи. Назначается согласно правилам именования помещений; помещение 2 – помещение, где заканчивается линия связи. Назначается согласно правилам именования помещений; порядковый номер – число, идентифицирующие данную линию связи, среди подобных линий, проходящих меду помещением 1 и помещением 2**;** код типа линии связи – назначается в соответствии с таблицей отображения линий связи.

База данных устройств и линий связи составляется на базе опросных листов

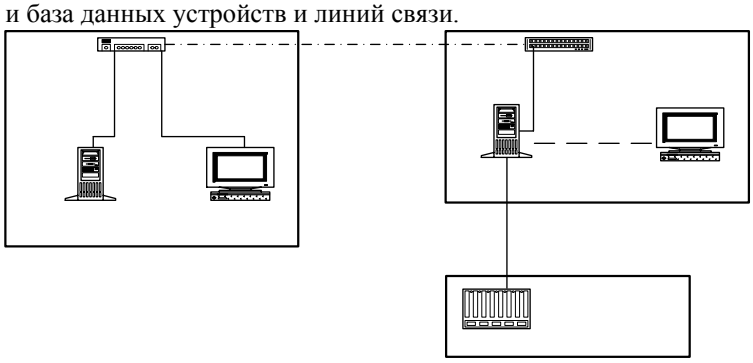
Опросный лист междуаудиторных линий связи		
Регистрационный номер ЛС	Маркировка начала ЛС	Маркировка конца ЛС

Опросный лист устройства		
РН устройства	Марка	Основные технические характеристики

На первом этапе создается модель топологической схемы информационной системы, в которой выделяются телекоммуникационные устройства, линии связи, а также помещения, в которых они находятся. Каждому устройству и линии связи присваивается уникальные регистрационные номера, содержащие информацию о типе, а также о помещении, где они расположены. Наличие уникальных идентификаторов позволяет

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

создать базу данных устройств и линий связи. В базе данных содержится расширенная информация, которая с точки зрения восприятия человеком, затрудняла бы чтение топологических схем, но в то же время является важной, чтобы ей просто пренебречь. Таким образом, в результате документирования, появляется топологическая схема ИВС и база данных устройств и линий связи.



Полученная информация, может быть использована как человеком, так как она строится с учетом удобства человеческого восприятия, так и для машинной обработки, в виду того, что форматы данных MS Visio (топологическая схема) и MS Excel (база данных устройств и линий связи) являются открытыми.

Фрагмент топологической структуры ИВС Владимирского государственного университета, насчитывающей около 1000 рабочих станций, приведен на рисунке.

РАСПРЕДЕЛЕННЫЕ КОЛЛЕКТИВНЫЕ АТАКИ НА ВЫЧИСЛИТЕЛЬНЫЕ РЕСУРСЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Калмыков М.С., Монахов М.Ю.

Владимирский государственный университет

Серьёзные опасности для вычислительных ресурсов информационных систем, функционирующих в сети Интернет, скрываются в базовых принципах работы сети – в основных сетевых протоколах, сохраняющихся практически в неизменном виде в течение более 30 лет. Именно на принципиальных недостатках спецификаций основных протоколов основаны самые опасные методы нарушения работы Интернет-систем – так называемые атаки типа “отказ в обслуживании” (Denial of Service, или сокращенно – DoS). Основным объектом настоящего рассмотрения является наиболее опасная разновидность данных атак – коллективные распределенные атаки типа “отказ в обслуживании” (Distributed DoS, или DDoS).

Главная особенность этих атак заключается в том, что их алгоритмы основаны на базовых принципах работы Интернет, что значительно усложняет разработку методов защиты.

DDoS-атаки направлены на исчерпание вычислительных ресурсов системы “жертвы”, либо (в последнее время – чаще всего) на забивание всей доступной пропускной способности подключения жертвы к Интернет, что приводит фактически к отключению системы от сети.

В ходе DDoS-атаки на жертву обрушивается мощный поток запросов от множества “зомби” – компьютеров, с установленными на них (в результате действия вируса или взлома) программами типа “троянских коней”. Как правило, это компьютеры обычных пользователей Интернет – слабо защищенные, с устаревшим антивирусным программным обеспечением (или вообще без него), однако, зачастую подключенные по широкополосным каналам доступа (например, по xDSL-линиям). Такие системы становятся легкой добычей вирусов и несложных хакерских атак, что позволяет злоумышленнику в короткие сроки собрать до нескольких тысяч современных компьютеров, и использовать их ресурсы в своих целях [1].

При заражении каждая из зомби-систем, регистрируется на одном или нескольких серверов управления. В качестве таких центров управления могут выступать, например, IRC-сервера. Обычно IRC-сервера используются для общения пользователей Интернет в реальном времени. Любой пользователь может организовать свой канал (своего рода “комнату общения”), пригласить других пользователей и обмениваться с ними сообщениями. При подготовке к DDoS-атаке в качестве “собеседников” выступают компьютеры-зомби, которые регистрируются на определенном IRC-канале и ждут команды от атакующего. Организатору атаки достаточно на минуту зарегистрироваться на этом канале, дать команду начала атаки и указать IP-адрес жертвы. После этого атакующий может покинуть IRC-канал (до тех пор пока не потребуется дать команду завершения атаки, если это вообще планируется). Кроме того, сам канал IRC может быть удален, чтобы затруднить поиск организатора атаки.

После получения сигнала начала атаки компьютеры-зомби создают непрерывный поток запросов, направленных на указанный организатором атаки IP-адрес жертвы. Как правило, внешне эти запросы выглядят как заявки на обслуживание от обычных клиентов (например запрос html-страницы), либо как управляющие сообщения протокола ICMP.

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

Согласно стандартам функционирования Интернет, система, получив запрос или управляющее сообщение, должна каким-то образом отреагировать на него. Система жертвы пытается установить соединение (при получении TCP-запроса), либо послать ответный пакет (в случае получения сообщения ICMP-эхо), или же послать сообщение о недоступности службы. В случае, если жертва попытается установить TCP-соединение, ей потребуется выделить определенную часть своих ресурсов (оперативной памяти, времени процессора) на поддержку соединения. При большом потоке запросов эти ресурсы очень быстро будут исчерпаны. Если система не принимает запрос на соединение, по стандарту она должна отправить ICMP-сообщение о недоступности службы. Это также потребует определенных затрат процессорного времени и полосы пропускания подключения к Интернет. Даже если система будет полностью игнорировать входящие сообщения, прибывающие пакеты все равно будут занимать всю доступную полосу пропускания, и система жертвы будет фактически отключена от Интернет. Это будет означать прекращение предоставления услуг обычным клиентам, то есть отказ в обслуживании. Таким образом цель атаки будет достигнута.

Выше изложен обобщенный алгоритм проведения DDoS-атаки. Конкретные реализации различаются по следующим параметрам:

1. Алгоритм управления зомби-системами. Атакующий может непосредственно давать команды каждому из компьютеров-зомби, либо использовать сервера управления. Обратная связь (регистрация зомби) может осуществляться через сервера управления, либо по электронной почте. Здесь возможно и множество других вариантов реализации.

2. Тип запросов к жертве атаки. Компьютеры-зомби могут отправлять жертве пакеты различных протоколов. Это могут быть эхо-запросы по протоколу ICMP, запросы на установление TCP-соединения (атака SYN-flood), либо UDP-пакеты (например DNS-запросы). Здесь выбор атакующего ограничен в основном теми протоколами, которые использует жертва для предоставления услуг обычным клиентам (в большинстве случаев это HTTP или SMTP). Дело в том, что пакеты от зомби внешне не должны отличаться от пакетов, которые приходят от клиентов. В противном случае их можно будет отфильтровать на маршрутизаторах вышестоящих провайдеров, предоставляющих жертве услуги доступа в Интернет. Если же атакующие пакеты неотличимы от законных запросов, фильтрация приведет к прекращению обслуживания клиентов, то есть цель атаки будет все равно достигнута.

3. Использование отражателей и усилителей. Компьютеры-зомби могут отправлять запросы не жертве атаки, а некоторым промежуточным системам, которые выступают в роли отражателей потока атакующих пакетов. Основной принцип использования отражателей заключается в том, что система-зомби отправляет запрос промежуточной системе от имени жертвы (используя поддельный адрес отправителя). Ответ на данный запрос получает уже жертва атаки. Как правило, ответный пакет по размеру в несколько раз превосходит пакет запроса, поэтому отражатели выступают одновременно и в роли усилителей потока атакующих пакетов [2]. В качестве отражателя может быть использован практически любой сервер на основе протоколов TCP или UDP (HTTP, SMTP, DNS и т.д.). К атакам подобного рода можно также отнести мало распространенную сейчас smurf-атаку, в которой в качестве усилителей использовались сети, отвечающие на широковещательные ICMP-запросы [1].

4. Алгоритм поведения зомби-систем во времени. Для усложнения процесса отслеживания атаки могут использоваться самые разные вариации поведения зомби-систем. Например, атака может носить “пульсирующий” или “мигающий” характер, когда в каждый момент времени будет активизироваться только некоторое подмножество зомби, и через определенные (либо случайные) промежутки времени будет происходить чередование атакующих машин. При использовании отражателей каждая из зомби-систем, может также варьировать со временем набор промежуточных систем, используемых для усиления атаки.

Таким образом, с появлением DDoS-атак глобальная сеть Интернет столкнулась с самой опасной угрозой за все время своего существования. Решение данной проблемы должно осуществляться как в краткосрочной (разработка методов отслеживания и подавления DDoS-атак), так и в долгосрочной перспективе (разработка новых алгоритмов функционирования сети, исключающих саму принципиальную возможность реализации DDoS-атак).

Литература

2. Howard F. Lipson, Ph.D. – Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, CMU/SEI-2002-SR-009, – CERT Coordination Center, – http://www.cert.org/archive/pdf/02sr009.pdf.

3. Steve Gibson – Distributed Reflection Denial of Service – Description and analysis of a potent, increasingly prevalent, and worrisome Internet attack, – Gibson Research Corporation – http://grc.com/dos/drdos.htm

ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

Полянский Д.А., Устинов В.Н.

Владимирский государственный университет

В настоящее время информационная безопасность предприятия является одним из ведущих факторов его эффективного развития. Информация имеет реальный стоимостный вес, который четко определяется прибылью, получаемой при ее использовании, или ущербом, который может быть нанесен предприятию в случае использования ее другими лицами.

Построение экономически эффективной системы информационной безопасности напрямую зависит от того, насколько точно проведена оценка стоимости защищаемой информации. Возможные потери от утечки информации приводят к конкретной величине экономического ущерба. Поэтому и затраты на защиту такой информации должны быть экономически ограничены суммой возможных потерь.

Точный стоимостный расчет совокупной величины всех возможных потерь достаточно сложен, а иногда и невозможен из-за отсутствия достоверных исходных данных. Поэтому в большинстве случаев достаточно укрупненной экспертной оценки потерь предприятия, обусловленных несоблюдением требований защиты информации.

Пусть защищаемая информация представлена в виде конечного множества элементов и необходимо оценить суммарную ее стоимость в денежных единицах. Она будет складываться из оценок элементов. Если денежные оценки объективны, то сумма дает искомую величину. Однако, количественная оценка элементов не всегда объективна даже при квалифицированной экспертизе. Это связано с их неоднородностью в целом.

Для оценки эффективности системы безопасности требуется построение ее формальной модели. Для формального описания можно воспользоваться моделью с полным перекрытием [1]. В ее основе лежит взаимодействие множества угроз $U = \{u_i\}$, множества ресурсов (объектов) защищаемой системы $O = \{o_j\}$ и множество механизмов безопасности $M = \{m_k\}$.

Для оценки экономической эффективности формальную модель необходимо дополнить множеством сотрудников предприятия $S = \{s_q\}$, обращающихся к объекту o_j с вероятностью t_{qj}.

$$\sum_{\forall q}\sum_{\forall j} t_{qj} = 1. \qquad (1)$$

Использование объекта o_j приносит доход предприятию w_j. Доход, получаемый от всех обращений к объекту равен:

$$W_j = w_j \sum_{\forall q} t_{qj}. \qquad (2)$$

Весь доход от использования всех объектов:

$$W = \sum_{\forall j} W_j = \sum_{\forall j} w_j \sum_{\forall q} t_{qj}. \qquad (3)$$

Пусть имеется множество злоумышленников $X = \{x_l\}$, каждый из которых может с вероятностью p_{lj} обратиться к объекту o_j. А вероятность успешного получения доступа равна τ_{xj}. Математическое ожидание потерь от одного злоумышленника в отношении объекта o_j равно:

$$Dx_{lj} = w_j\, p_{lj}\, \phi_{lj}. \qquad (4)$$

Потери от всех злоумышленников в отношении объекта o_j равны

$$Dx_j = w_j \sum_{\forall l} p_{lj}\, \phi_{lj}. \qquad (5)$$

И потери для всего предприятия:

$$D = \sum_{\forall j} w_j \sum_{\forall l} p_{lj}\, \phi_{lj}. \qquad (6)$$

Для j-го объекта стоимость его защиты определяется его характеристиками o_j и характеристиками механизма защиты m_k

$$z_j = б_k + в_k \cdot o_j. \qquad (7)$$

Для определения показателей α_k и β_k оптимальных средств защиты необходим анализ и оценка активов организации, уязвимостей, угроз информационной безопасности, возможных атак и целей безопасности.

Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, направленные на выяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых системой безопасности и условий расположения и эксплуатации объекта.

Атака действенна, если некоторая угроза u_i, используя уязвимость v_i объекта оценки, приводит к риску r_i потери активов организации. Формально описать вероятности отдельных угроз, атак, эффективности от-

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

дельных политик безопасности очень сложно. В связи с этим, для получения количественной оценки стоимости защиты объекта o_i используются методы экспертных оценок [2, 3].

Стоимость защиты всех объектов определяется из соотношения:

$$C = \sum_{\forall j} z_j . \quad (8)$$

А полные затраты равны сумме потерь от действий злоумышленника и стоимости защиты:

$C_\Sigma = D + C.$ (9)

Экономический эффект системы информационной безопасности определяется разностью доходов и затрат:

$E = W - C_\Sigma.$ (10)

А экономическая эффективность равна:

$$Ef = \frac{W - C_\Sigma}{C_\Sigma} . \quad (11)$$

Выводы

Чтобы защитить информацию, необходимо затратить ресурсы. Величина затрат предприятия складывается из издержек, связанных с применением средств защиты и потерь от действий злоумышленников. Для определения денежной стоимости достаточного уровня средств защиты требуется применение методов экспертных оценок. А количественная оценка потерь от преодоления средств защиты возможна с использованием вероятностного подхода.

Литература

1. Астахов А. Анализ защищенности корпоративных систем. - (http://www.isaca.ru/security/Pubs/Pub1_AAM_SecEval.htm).

2. Беляев А.В. Методы и средства защиты информации (http://www.sitforum.ru/internet/infsecure/index.shtml).

3. Захаров А.П. Методология оценки информационной безопасности профиля защиты. (http://beda.stup.ac.ru/rv-conf/).

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССА ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

Полянский Д.А., Устинов В.Н.

Владимирский государственный университет

Безопасность предприятия - это стабильность его существования, наличие условий, обеспечивающих эффективную защиту от всех угроз, способных нанести ущерб. Большинство угроз безопасности предприятия связано с действиями злоумышленников и в той или иной степени сводится к угрозам безопасности информационных ресурсов предприятия.

Обеспечению информационной безопасности предприятия как любой управленческой деятельности присущи функции планирования, организации, мотивации и контроля. Для выполнения всех названных функций требуется принятие решений и обмен информацией.

Целью процесса принятия управленческого решения на предприятии является определение состояния некоторой проблемы и выработка на основе этого вариантов возможных решений. Это достигается за счет решения следующих задач управления [1]:

- наблюдение за состоянием интересующих процессов и проблем;
- оценка состояния процессов и проблем, обеспечивающая выявление отклонений процессов от их нормального протекания;
- анализ причин значимых отклонений;
- выработка рекомендаций для принятия управленческих решений и прогнозирование последствий предлагаемых решений.

Уровень обеспечения информационной безопасности оказывает существенное влияние на принятие адекватного решения, от которого будет зависеть развитие предприятия.

Процесс использования информации в интересах принятия обоснованного решения включает три основных элемента:

- источник информации,
- носитель информации,
- пользователь информации.

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

Пользователь в некоторых случаях может выступать источником информации. Таким образом, имеет место некоторый круговорот информации (рис. 1).

Рис.1.

Руководитель, принимающий решение в данной схеме будет выступать потребителем информации.

Информация бывает ложной и достоверной, полезной и бесполезной, полной и частичной. Свойство достоверности информации характеризует потенциальную возможность принятия правильного решения. Свойство полезности характеризует степень соответствия информации тематике решаемых проблем. Свойство полноты характеризует степень достаточности информации для принятия правильного решения на ее основе.

В рамках процесса использования информации при принятии решения можно выделить следующие проблемы обеспечения информационной безопасности [2]:

- защита носителя от источника в процессе передачи и приема информации в части получения ложной первичной информации (информация источника носит заведомо ложный характер);
- защита носителя от источника от искажения или уничтожения полезной информации, получения бесполезной или “паразитной” информации, которая понижает в общем объеме процент полезной;
- защита пользователя от носителя в части получения частичной, ложной искаженной и ложной порожденной информации, получения бесполезной избыточной и бесполезной навязанной информации;
- защита носителя от пользователя в части уничтожения, изменения информации, порождения новой информации и выноса информации.

Говоря о защите процесса принятия решений, необходимо отметить, что часть средств должна быть направлена на обеспечение безопасности информации как таковой, а другая часть - на обеспечение информационной безопасности.

Безопасность информации как таковой предполагает защиту в процессе передачи, хранения и доступа к ней. Таким образом, средства обеспечения безопасности информации ориентированы на защиту информации от несанкционированного ее изменения.

Информационная безопасность предполагает защиту взаимодействующих объектов в процессе обработки информации и направлена на результат этой обработки. Средства обеспечения информационной безопасности процесса принятия решений должны быть ориентированы на:

- защиту от несанкционированного уровня обработки доступной объекту информации,
- защиту от получения объектом ложной, бесполезной, частичной информации.

Поэтому обеспечение безопасности информации является только необходимым, но не достаточным условием обеспечения информационной безопасности по полному циклу.

Обеспечение информационной безопасности предполагает полное использование технологий информационно-аналитической обработки данных, которые в данном случае имеют двойное применение, т.е., позволяют осуществлять требуемую обработку информации и могут использоваться для оценки возможного ущерба при их применении.

Из выше сказанного следует, что понятие информационная безопасность определяет два взаимосвязанных направления организации защиты и, вообще говоря, когда одним объектом нарушается уровень обработки информации, другой объект имеет полное право выдать ему ложную, бесполезную и неполную информацию, сообщая или не сообщая ему об этом.

Выводы

Эффективность работы предприятия напрямую зависит от информационной безопасности в процессе принятия решений руководителем предприятия. Для обеспечения информационной безопасности не достаточно безопасности информации как таковой. Комплексный подход при решении этой проблемы требует защиты всех объектов и субъектов процесса принятия решений – источника, носителя, пользователя и потребителя информации – как от внешних воздействий, так и от неправомерных действий друг друга.

Литература

1. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003.
2. Ефремов В.А. и др. Информационная безопасность при подготовке и принятии управленческих решений (http://www7.mte.ru/).

БОРЬБА СО СПАМОМ

Лаврухин А.Ю.

Московский государственный инженерно-физический институт (технический университет)

В настоящее время проблема борьбы с несанкционированными рассылками становится все более и более острой в связи с крайне высокими темпами роста процента спама в системах обмена электронными сообщениями. Еще 3 года назад его доля составляла около 40 процентов от общего числа электронных писем, сейчас же по сведениям ведущих российских поставщиков услуг электронной почты она приближается к 80% от всех входящей корреспонденции. Сообщения такого рода начинают причинять ощутимый урон всем пользователям, каким-либо образом использующим e-mail сервисы, поэтому задача создания эффективных средств противодействия несанкционированным массовым рассылкам обретает в настоящее время все большую актуальность.

На данный момент понятие спама определено как безадресная, анонимная, незапрошенная и массовая рассылка почтовых сообщений. В данном определении безадресность подразумевает отсутствие конкретного указания того, кому предназначено данное послание, анонимность означает невозможность установления каких либо данных об отправителе, массовость и незапрошенность же не позволяют пользователю в любой момент отказаться от корреспонденции, рассылаемой по десяткам, а иногда и сотням тысяч адресов.

Технологии рассылок спама совершенствовались от года к году. Первые несанкционированные рассылки не использовали сложных алгоритмов маскировки, сообщение отправлялось через несколько почтовых систем с транзитной доставкой сообщений произвольным пользователям. Для борьбы с ними ip-адреса серверов, с которых производилась отправка спама помещались в так называемые черные списки (blacklists). Однако это не остановило спаммеров, и массовые рассылки начали производиться посредством использования socks- и proxy- серверов, из-за чего установление истинного адреса отправителя стало практически невозможным.

Недавно несанкционированные рассылки начали выходить на новый уровень. Спаммеры начали использовать программы, обладающие возможностью производить рассылку из зараженных ими сетей. Наиболее совершенные из них способны не только размножаться, но и уничтожать аналогичные программы, если таковые имеются на объекте атаки, замещая их своим кодом. Также большинство из них поддерживают автообновление, например получение новых адресов, на которые производится отсылка спама. При этом возможно использование нестандартных портов, служб, протоколов, что позволяет замаскировать передачу несанкционированных данных.

В свете всего вышесказанного нетрудно предположить, что черные списки уже не могут обеспечить надлежащего уровня защиты от несанкционированных рассылок. Количество ip-адресов, с которых отправляется спам, очень быстро увеличивается, одновременно с этим возрастает вероятность потери легальной почты. Поэтому возникла необходимость разработки новых методов борьбы с этой проблемой, которые будут рассмотрены ниже.

Фильтрация спама построена на анализе и выявлении основных присущих ему признаков во входящем сообщении. Для этого используются как программные, так и программно-аппаратные средства. В каждом из них применяется определенный набор тестов, основанных на различных алгоритмах проверки письма, включая использование средств искусственного интеллекта.

До сих пор в большинстве случаев приходится прибегать к использованию черных списков. Хотя они в одиночку не способны обеспечить надлежащий уровень защиты, в совокупности с другими методами анализа их эффективность заметно повышается. Основным требованием, предъявляемым к ним, является актуальность и объем, от которых зависит обоснованность их применения для защиты определенной системы. Так, практически все крупные провайдеры услуг электронной почты имеют в своем распоряжении черные списки собственной разработки, либо используют уже созданные.

Для более тонкой проверки входящих сообщений возможно использовать контекстный анализ заголовков и тела письма. Существует несколько алгоритмов исследования текста, например в большинстве случаев в теме сообщения используются одни и те же слова, заглавные буквы. На основе имеющейся базы наиболее часто встречаемых фраз производится проверка заголовков, и если появляется совпадение, то письмо считается потенциальным спамом и подвергается более жестким тестам на последующих этапах.

Наиболее наукоемким представляется анализ тела письма. Существует несколько подходов к этой задаче, одним из них является лексический анализ текста сообщения. С его помощью проверяется, есть в ли в теле послания характерные для спама фразы (например предложение что-нибудь купить, услуги итд). Затем применяется эвристический анализ, который определяет наличие в тексте некоторых стандартных свойств, характерных для спама. Среди них сочетание различных кодировок, наличие картинок, одновременно являющихся ссылками, большое количество непечатаемых символов и.т.д. Спаммеры зачастую маскируют тело письма путем добавления в него HTML комментариев, не заметных пользователю, однако присутст-

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

вующих в исходном сообщении, вследствие чего необходимо и к нему применять вышеперечисленные методы анализа.

Другим подходом к оценке входящей почты на предмет отнесения ее к спаму является статистический подход. Он основывается на теории вероятностей и применяет для анализа тела сообщения алгоритм Байеса. Каждому слову или словосочетанию присваивается 2 значения, первое из которых характеризует вероятность его наличия в спаме, а второе – в легальных письмах. Комплексный анализ этих 2 значений и определяет, является ли входящее сообщение несанкционированным.

Для создания базы на основе которой производится анализ почты, берут два или более списка слов различных категорий писем и передают их программе для ее последующего обучения. Она в свою очередь вычисляет частоту встречаемых слов и фраз, а затем формирует частотный словарь для каждого из типов сообщений. Затем с их помощью происходит вычисление вероятности принадлежности входящего письма к одной из ранее названных категорий по формуле Байеса. Для получения общего результата для всего сообщения производится суммирование и нормализация вероятностей каждого из слов (фраз). Как правило, в результате всех вышеперечисленных действий становится возможным отнести сообщение к одной из категорий, причем вероятность правильного решения непосредственно зависит от полноты частотного словаря, а также количества исследуемых типов писем. В дальнейшем возможно улучшение полученных результатов посредством обработки писем, неправомерно причисленным к одной из категорий, причем все это осуществляется без вмешательства администратора, достаточно указать требуемый раздел для этого письма и заново осуществить процедуру обучения.

Сравнивая эти подходы, необходимо отметить существенное преимущество статистического анализа, который позволяет добиться крайне высокой эффективности фильтрации входящей корреспонденции, а также обеспечивает минимальное количество ложных срабатываний. Также он не требует трудоемких и дорогостоящих операций создания баз, применяемых при лексическом анализе, его корректировка и обновление осуществляется автоматически. Следовательно наиболее высокий результат будут показывать те средства, которые построены на основе этого алгоритма.

METHODS OF STRUGGLE WITH SPAM

The analysis of methods of spam exception is offered. Usage of black lists of ip-addresses for spam exception becomes not effective. More power method of spam exception use a context-sensitive analysis of its text. However, the best method is based on usage of the statistical approach.

ЗАЩИТА ОТ РАЗРУШАЮЩИХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ

Арабгаджиев Р.Р., Ананьев А.П., Асосков А.А., Иванов М.А.,
Косых П.А., Куликов С.С., Метлицкий Ю.В., Прилуцкий С.О.

Московский инженерно – физический институт
(технический университет)

Рассматриваются уязвимости существующих средств защиты от разрушающих программных воздействий. Отмечается перспективность стохастических методов обеспечения безопасности.

VULNERABILITY ANALYSIS OF EXISTING MALWARE SECURITY TECHNIQUES

Arabgadjiev R., Ananyev A., Asoskov A., Ivanov M.,
Kosih P., Kulikov S., Metlitsky U., Prilutsky S.

Computer-aided data processing systems are evaluated in terms of malware tolerance. Results are presents.

ФАЙЛОВАЯ СИСТЕМА СО СЛЕЖЕНИЕМ ЗА ЦЕЛОСТНОСТЬЮ SIGNFS

Косых П.А.,

Московский инженерно – физический институт
(технический университет)

Рассматривается файловая система, использующая криптографические алгоритмы, основанные на свойствах эллиптических кривых, для слежения за целостностью. Вводится понятие контейнера. Контейнер обеспечивает интеграцию электронной подписи и содержимое файла без потери функциональности ПО.

INTEGRITY CHECKING FILE SYSTEM

Kosih P.

This work deals with on the fly integrity checking file system using elliptic curves cryptography. The main feature of the file system is container concept. Container provides signature integration with file content without breaking functionality of the common software.

ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru