Федеральное агентство по образованию
Сибирский государственный аэрокосмический университет
имени академика М. Ф. Решетнева

АКТУАЛЬНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Сборник материалов III Международной научно-практической конференции

Красноярск 2009

Федеральное агентство по образованию
Сибирский государственный аэрокосмический университет
имени академика М. Ф. Решетнева

АКТУАЛЬНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Материалы III Международной научно-практической конференции

Красноярск 2009

УДК 004.056
ББК 32.973.26-018.2
А43

А43 **Актуальные проблемы безопасности информационных технологий:** материалы III Международной научно-практической конференции / под общей ред. О.Н. Жданова, В. В. Золотарева; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2009. – 144 с.

В представленных материалах отражены достижения как студенческой научной деятельности в различных вузах России, так и результаты исследований отечественных и зарубежных ученых и специалистов.

Сборник предназначен для научных работников, аспирантов, студентов.

УДК 004.056
ББК 32.973.26-018.2

ОГЛАВЛЕНИЕ

ОТ ОРГКОМИТЕТА

Хорошо известно, что в настоящее время возрастает значение методов и средств защиты информации. При жизни одного поколения произошло качественное изменение ситуации в этой области. Совсем недавно вопросами защиты информации занимались лишь спецслужбы, а сегодня круг лиц, так или иначе связанных с обеспечением информационной безопасности, весьма широк и процесс дальнейшего его расширения продолжается. Более того, сейчас уже является актуальной задача проведения всеобуча по информационной безопасности.

Одной из важнейших составляющих системы защиты информации является криптография. В частности, широкое распространение электронного документооборота требует от многих (даже рядовых) сотрудников овладения знаниями и навыками, связанными с формированием электронной цифровой подписи. В начале 21 века криптографические методы все активнее входят в быт. Так, например, отправляя Email, мы в некоторых случаях отвечаем на вопрос меню: «Нужен ли режим зашифрования?» Владелец интеллектуальной банковской карточки, обращаясь через терминал к банку, вначале выполняет криптографический протокол аутентификации карточки. Пользователи сети Интернет наверняка знакомы с дискуссиями вокруг возможного принятия стандарта цифровой подписи для тех страниц, которые содержат «критическую» информацию (юридическую, прайс-листы и др.). С недавних пор пользователи сетей стали указывать после своей фамилии наряду с уже привычным «Email ...» и менее привычное — «Отпечаток открытого ключа ...».С каждым днем таких примеров становится все больше. И новые практические приложения криптографии и являются одним из источников ее развития. Современная криптография использует тонкие методы абстрактной алгебры, теории чисел, теории вероятностей.

Следует заметить, что защита информации – комплексная задача, для ее решения необходимо применение не только криптографических методов. Современный этап развития науки и общества характеризуется все увеличивающимся разнообразием задач, возникающих при работе с информацией. Правильный выбор методов и средств, оценка их эффективности и стоимости возможны лишь при сотрудничестве специалистов в разных областях знания. Обеспечение информационной безопасности автоматизированных систем представляет собой непрерывный процесс анализа, проектирования, эксплуатации и оценки систем защиты информации

В настоящее время формируется сообщество специалистов по защите информации. Кроме того, многие аспекты информационной безопасности интересны профессионалам смежных областей. Поэтому особое значение приобретают обмен результатами, обобщение и внедрение опыта. Определенные шаги в этом предпринимаются сотрудниками (и что очень важно, и студентами!) Сибирского Государственного Аэрокосмического Университета. Так, с 2006 года работает научный семинар кафедры Безопасности Информационных Технологий по защите информации, а с 2007 года и городской научный семинар по криптографии. Можно утверждать, что всеми заинтересованными специалистами и руководителями осознается необходимость проведения специализированных научных и научно-практических конференций и семинаров, доступных широкому кругу участников.

Цель проведения конференции – в развитии и укреплении научного сотрудничества между различными вузами, научными и образовательными структурами России и ближнего зарубежья, развитие комплексной всероссийской системы обмена опытом через проведение специализированных научных конференций.

По инициативе ряда преподавателей СибГАУ в 2007 году была проведена первая конференция АПроБИТ. Одобрение и заинтересованность коллег убедили организаторов в полезности и необходимости проведения таких конференций в будущем. Так конференция АПроБИТ стала традиционной. Постепенно расширялась география участников. И в

настоящем сборнике представлены работы коллег не только из Сибири, но и из других регионов России и из зарубежных стран.

Результаты научных исследований, представленные в сборнике, отражают развитие технологий в области защиты информации. На конференции были представлены работы по следующим направлениям исследований:

Криптографические методы и средства защиты информации.

Оптимизация, моделирование и разработка систем защиты информации.

Защита персональных данных в информационных системах.

Организаторы и участники конференции надеются на дальнейшее сотрудничество и расширение представительства.

Секция 1. «Криптографические методы и средства защиты информации»

УДК 003.26

А.Т. Алиев, А. Н. Щербакова

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД СИНОНИМИЧНЫХ ПРЕОБРАЗОВАНИЙ ОТКРЫТОГО ТЕКСТА С УЧЕТОМ КОНТЕКСТА

В данной работе нами рассмотрен метод лингвистической стеганографии основанный на синонимичной замене с учетом контекста. В методе используется ограниченный словарь синонимов и специальная база контекстозависимого употребления слов, использование которой позволяет значительно снизить вероятность серьезного искажения структуры и смысла исходного текста.

Существующее на сегодняшний день большое разнообразие различных форматов хранения и представления электронных документов предоставляет широкие возможности для построения на их основе систем скрытой передачи информации. Вместе с тем большинство стеганографических методов оказываются нестойкими в случае сохранения электронного документа-контейнера в другом формате. В [1, 2, 3] описаны методы лингвистической стеганографии, основанные на синонимическом перефразировании. Применение методов синонимичной замены позволяет значительно повысить стойкость скрытой информации к непреднамеренному разрушению в указанных случаях. Однако разработка программных реализаций данных методов для русского языка вызывает ряд затруднений, так как должна сохраняться осмысленность и однозначность текста документа-контейнера.

Нами предлагается решение, основанное на методе синонимических замен, позволяющее сохранить синтаксическую структуру предложения и его смысловую нагрузку. Известно, что в русском языке существует достаточно большое количество пар {слово; синоним}. Использование всех таких пар для целей стеганографического сокрытия информации, когда слову ставиться в соответствие двоичный «0», его синониму «1» очередного бита скрываемого сообщения, часто приводит к значительным искажениям смысловой нагрузки скрывающего текста. Как следствие из-за неправильного употребления синонимов текст, содержащий скрытую информацию, становиться легко идентифицируемым. В результате противник может установить наличие скрытого сообщения.

Построение словаря синонимов и базы контекстозависимого употребления слов

В целях сведения к минимуму неконтролируемых замен синонимов вместо полных словарей синонимов для русского языка [4] предлагается использовать ограниченный набор пар {слово; синоним}, состоящий только из наиболее часто употребляемых слов. С этой целью был проведен анализ текстовой базы состоящей более чем из 20000 произведений различных жанров. В результате нами были получены достаточно точные данные по частотам употребляемости слов русского языка. Анализ полученных результатов показал, что уже 650 наиболее часто встречающихся слов в среднем обеспечивают покрытие более 50% любого осмысленного текста. Соответствующий график представлен на рисунке 1.

Полученные результаты говорят о том, что словарь синонимов можно ограничить лишь наиболее часто встречающимися в тексте словами без угрозы серьезного снижения информационной емкости. В тоже время, такое ограничение позволит более точно контролировать использование отобранных синонимов и исключить неконтролируемые замены редко употребляемых слов.

Так как у одного слова может быть множество синонимов, то словарь синонимов строится по уже отобранным наиболее часто встречающимся словам, в виде списка

содержащего векторы вида: {слово, синоним 1, синоним 2, …}. В отличие от известных стеганографических методов длина вектора не обязательно должна быть кратной двойке. Допускается включение в вектор не только однозначных синонимов, но и редко используемых синонимов, употребление которых возможно только в определенном контексте. Такой подход позволяет максимально расширить набор синонимов для каждого из отобранных слов, что в свою очередь повышает общую информационную емкость метода. Далее мы будем рассматривать векторы, в которых первое слово, рассматривается так же как одни из эквивалентных синонимов. Таким образом, итоговый словарь синонимов содержит векторы вида: {синоним 0, синоним 1, синоним 2, …}.

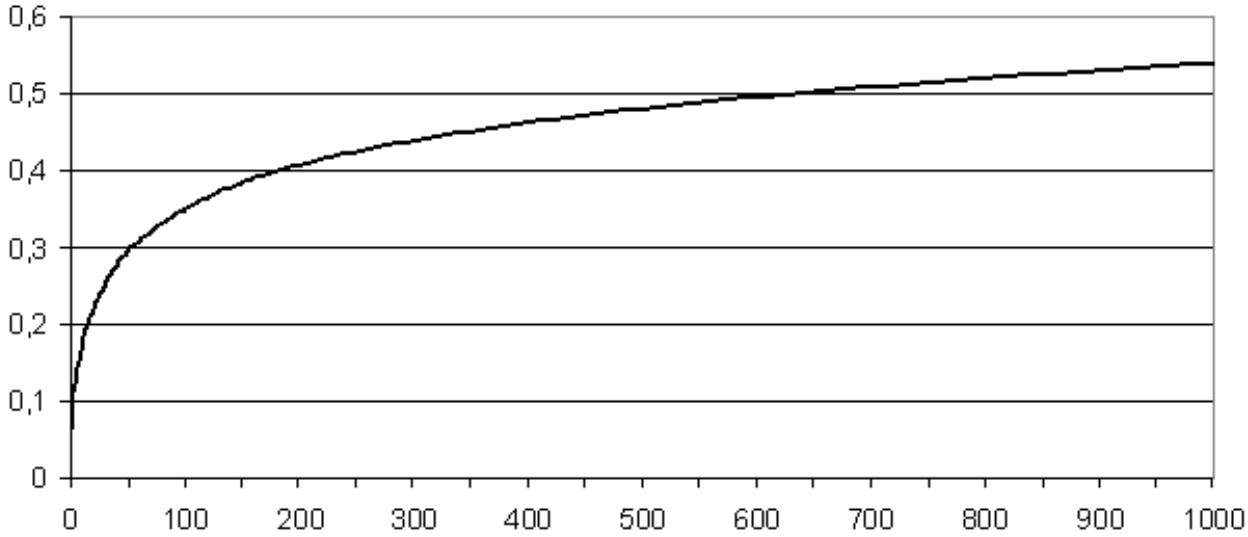

Рис. 1. Покрытие текстов первой тысячей наиболее часто употребляемых слов

Очевидно, что даже в условиях ограниченного набора слов прямая замена одного синонима другим только в зависимости от очередного бита скрываемого сообщения может привести к непредсказуемым результатам, и вполне вероятно разрушению структуры и смысла исходного скрывающего текста. Использование тех или иных синонимов возможно в условиях различного контекста (окружения слов). В целях обеспечения учета контекста при выборе возможных синонимичных замен нами предлагается использование дополнительной базы контекстозависимого употребления слов. Данная база, с целью ограничения количества записей строится исключительно по уже сформированному словарю синонимов. Используемая нами база контекстозависимого употребления слов состоит из двух таблиц содержащих записи вида: {слово из словаря синонимов, слово справа, частота встречаемости пары} и {слово из словаря синонимов, слово слева, частота встречаемости пары}. При формировании базы нами была использована та же база текстов, которая использовалась ранее при построении словаря синонимов. Так как одно и то же слово в зависимости от части речи может употребляться в тексте с различным склонением, спряжением и окончанием. Учитывая это, при проверке наличия и помещении очередной записи в базу контекстозависимого употребления производится отбрасывание окончаний слов с учетом правил аффиксации для русского языка. Если очередная рассматриваемая пара слов из анализируемого текста уже присутствует в базе контекстозависимого употребления, то добавление рассматриваемой пары в базу не производится, а увеличивается счетчик частоты встречаемости соответствующей ей пары в базе контекстозависимого употребления.

Процедура сокрытия информации

Для сокрытия информации методом синонимичных замен необходим документ-контейнер, содержащий открытый безобидный текст. В процессе сокрытия информации

текст документа-контейнера просматривается последовательно по словам, при этом каждое очередное слово с учетом окончания, проверяется на присутствие в словаре синонимов. Если слово содержится в словаре синонимов, то производится анализ его окружения. Далее на соответствие данному окружению по базе контекстозависимого употребления проверяются все синонимы данного слова, содержащиеся в словаре синонимов. Результатом проверки должен стать временный вектор синонимов, содержащий только слова, употребление которых является допустимым в рамках данного контекста. Для этого вначале, в вектор синонимов заносятся все синонимы данного найденного слова из словаря синонимов. Затем для каждого слова из временного списка синонимов проверяется возможность его использования в окружении исходного слова. Данная проверка осуществляется путем поиска соответствующей записи в базе контекстозависимого употребления. Если такая запись отсутствует, то слово исключается из временного вектора синонимов. В целях построения упорядоченного по частоте использования в условиях данного контекста вектора синонимов, к каждому синониму в качестве его веса дописывается частота встречаемости соответствующей пары из базы контекстозависимого употребления. Итоговый вектор синонимов выглядит следующим образом: {синоним 1, вес; синоним 2, вес; …}.

Так как изначально предполагается сокрытие двоичной информации, то полученный временный вектор синонимов необходимо нормировать по длине, которая должна быть кратной степени двойки. В случае если длина полученного вектора синонимов оказывается больше необходимой, то из временного вектора синонимов удаляются синонимы с наименьшим весом. Если длина полученного в результате вектора больше нуля, то осуществляем сокрытие очередных бит скрываемой информации. При этом количество битов скрываемой информации t определяется исходя из длины вектора l как $t = \log_2 l$. Синонимы, входящие во временный вектор упорядочиваются в соответствии с весом. Далее каждому из синонимов последовательно ставится в соответствие номер – двоичное представление числа из диапазона 0, …, $2^t - 1$. Затем из временного вектора синонимов выбирается слово, двоичное представление номера которого соответствует текущему двоичному вектору скрываемой информации длины t. Выбранное слово является синонимичной заменой текущего слова в тексте документа. Замена исходного слова в документе осуществляется с учетом окончания данного слова и слов, составляющих его ближайшее окружение.

После замены очередного слова осуществляется смещение указателя в документе на два слова вправо, если текущее рассматриваемое слово не имеет синонимов (согласно словарю синонимов), смещение осуществляется вправо на одну позицию. Следует отметить, что предложенная схема позволяет обеспечить возможность предварительного анализа объема контейнера без учета скрываемой информации. Данная особенность позволяет подобрать скрывающий текст из множества предварительно подготовленных документов, под данное скрываемое сообщение без непосредственного встраивания данных сообщения. Это позволяет избежать использования контейнеров большой емкости для передачи коротких сообщений и гарантировать возможность записи в контейнер заранее определенного объема скрываемой информации. В результате метод позволяет рационально использовать заранее подготовленный набор текстовых документов в автоматическом режиме.

Выводы

В работе предложен новый стеганографический метод осуществляющий сокрытие дополнительной информации в текстовых электронных документах. Метод непосредственно ориентирован на работу с русскоязычными текстами. Особенностью предложенного метода является сокрытие информации методом синонимичных замен с учетом контекста. Полученные результаты могут быть использованы для целей скрытой передачи информации и защиты авторского права на электронные произведения. Кроме

того, в процессе исследования по большой выборке текстов произведений различных жанров построены частотный словарь русского языка, словарь синонимов наиболее часто употребляемых слов и база контекстозависимого употребления слов. Данные результаты могут быть использованы в системах автоматического поиска и классификации электронных документов.

Библиографический список

1. Bennett K., Linguistic Steganography: survey, analysis, and robustness concerns for hiding information in text, Center for Education and Research in Information Assurance and Security, CERIAS Tech Report 2004-13, 30 p.

2. Calvo H., Bolshakov I. A., Using selectional preferences for extending a synonymous paraphrasing method in steganography, Advances en Ciencias de la Computacion e Ingenieria de Computo - CIC'2004: XIII Congreso Internacional de Computacion, October 2004, pp. 231–242.

3. Wayner P., Disappearing Cryptography – Information Hiding: Steganography & Watermarking, Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 2002, 413 p.

4. Абрамов Н., Словарь русских синонимов и сходных по смыслу выражений, М.: Русские словари, 1999.

A.T. Aliev, A.N. Scherbakova

A CONTEXT SENSITIVE STEGANOGRAPHY METHOD FOR OPEN TEXT SYNONYMOUS SUBSTITUTION

In this article, we considered the method of linguistic steganography based on context sensitive synonymous substitution. The method uses a limited vocabulary of synonyms and a special database of context sensitive use of words. It allows substantially reduce the probability of a serious distortion of the structure and meaning of the original text.

УДК 004.056:003.26

С.С. Барильник, И.В. Минин, О.В. Минин

ПРИМЕНЕНИЕ АЛГОРИТМОВ СТЕГАНОГРАФИИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Рассматриваются способы применения алгоритмов стеганографии в современных распределенных информационных системах и Web-ориентированных приложениях, виды возможных фишинг-атак, существующие методы борьбы с такими видами атак, а также система защиты от фишинга, разработанная авторами на основе алгоритмов текстовой стеганографии в Web-приложениях.

Человек на пути своего существования всегда стремился к облегчению своей работы. Сначала появились орудия труда, позволяющие быстрее, легче и качественней обрабатывать землю и добывать провиант, много веков спустя промышленная революция и появление мануфактур. Двадцатый век подарил человеку вычислительную технику и как следствие, появление различных информационных технологий, без которых сегодня уже немыслима промышленность. Информационные технологии сегодня – это орудие труда, проникшее во все области жизнедеятельности человека.

Информационные технологии не стоят на месте, они довольно бурно и быстро развиваются с момента их возникновения. Развивается вычислительная техника, увеличиваются скорости передачи данных, расширяется всемирная сеть интернет.

Интернет дал огромный толчок к развитию Web-ориентированных приложений. Каждый день появляются новые сайты и сервисы, также увеличивается число их пользователей. В настоящее время Web-приложения вытесняют прикладные программы, к которым мы уже успели привыкнуть. Пользователю Web-приложения не нужны вычислительные мощи, память, платные операционные системы, настройка персонального компьютера под определенные задачи и т.д. Ему достаточно запустить браузер и набрать нужный адрес, после чего он уже внутри рабочего пространства. Ярким примером может послужить продукт компании Google – Gmail. Gmail является полноценным почтовым клиентом, который делает все, что делает любой другой почтовый клиент, запускаемый на вашем компьютере, и даже немного больше. Подобные Web-приложения работают на сервере, а пользовательский интерфейс отображается в виде Web-страниц. Структура Web-приложения такова, что вся программная логика сконцентрирована в одном месте (на сервере), а пользовательский интерфейс доступен любому человеку в виде небольшой программы (Web-страницы).

При более глубоком рассмотрении архитектуры Web-приложения, можно увидеть, что вся программная логика Web-приложения находится на сервере, в отличие от обычных прикладных программ, где логика приложения располагается на компьютере каждого пользователя. Такая архитектура позволяет упростить решения большого ряда проблем как технических, так и не технических. Так как имеется только одна рабочая копия Web-приложения (на сервере), его намного проще распространять среди пользователей. По сути о распространении приложения вообще можно забыть, так как пользователь в реальности не получает копии приложения, как это происходит в обычных прикладных программах. Все, что получает пользователь, это интерфейс программы, т.е. только то, что ему необходимо для работы. Получается, что проблемы распространения Web-приложения не существует в том смысле, что вы можете работать с Web-приложением, не имея такового, в любой момент в любом месте через Web-интерфейс предоставляемый сервером Web-приложения.

Говорить о достоинствах Web-приложений можно бесконечно, а рассмотреть тонкости технологических решений применяемых в Web-приложениях и их проблемах – полезно.

Внутри любого Web-приложения так или иначе передается вся обрабатываемая информация, а суть Web-приложения в том, что оно работает через сеть. Таким образом, все данные, обрабатываемые пользователем и приложением, оказываются в сети. Поэтому встают вопросы об информационной безопасности использования Web-приложений.

Информационная безопасность Web-приложений сегодня актуальна как никогда. Появляются различные технологии, обеспечивающие безопасность передачи данных через сеть. Одним из самых распространенных средств является протокол SSL. Суть протокола SSL заключается в шифровании передаваемой информации, используя специальные цифровые сертификаты, выдаваемые разработчиком Web-приложения. К сожалению, применение такого подхода требует мощные и соответственно дорогостоящие вычислительные машины на стороне сервера для шифрования и дешифрования информации от многочисленных клиентов. Иначе Web-приложение начинает работать очень медленно, а в промышленности и бизнесе, как известно, время – деньги. Также при применении данного подхода у разработчиков встают проблемы верификации цифровых сертификатов: все цифровые сертификаты должны быть внесены в глобальную базу цифровых сертификатов, с которой соединяется браузер клиента при получении сертификата.

Существуют и другие подходы к решению проблемы несанкционированного доступа к информации. Например, распространенные в интернет методы идентификации и аутентификации пользователя по логину и паролю. Данный подход не требует шифрования передаваемых данных и в некотором роде гарантирует безопасность обрабатываемой информации. Но стоит злоумышленнику узнать ваш пароль, он получает всю необходимую для него информацию.

Современный «хакер» обладает знаниями, как совершить несанкционированный доступ к данным, защищаемым по любому из представленных методов. Если данные шифруются, то их расшифровка – это лишь вопрос времени. А взлому Web-приложений, работающих через логин и пароль, посвящены целые Web-сайты в интернет.

Выходом из сложившейся ситуации могут быть подходы, концептуально отличающиеся от применяемых методов. Таким подходом может стать концепция Web-приложения, использующего стего-каналы для передачи некоторой информации.

Развитие Web-технологий принесло большое количество решений задачи передачи информации между клиентом и сервером. Сейчас, при создании распределенных приложений используют модели, в которых сервер не зависит от реализации клиента, сервер передает информацию в строгом структурированном виде, не зависящем от того как она будет представлена клиентом. Таким примером служит передача информации в формате XML. Клиент принимает данные и отображает их так, как ему удобно. Таким образом, разработчику при написание серверной части приложения нет необходимости заботиться о том, как реализована клиентская часть, будь то прикладное ПО или Web-страница. Примером такого подхода служат различные Web-сервисы, а также распространенная сегодня технология AJAX.

Xml, являясь текстовым форматом, очень хорошо подходит на роль стего-контейнера. Можно разработать большое количество алгоритмов стеговставок в xml. Стеганографии в текстовых форматах данных посвящено большое количество научных статей и публикаций, но не так много информации о том, как зачем и где применять подобные стегоканалы.

Рассмотрим несколько алгоритмов стеганографии в текстовых форматах хранения и передачи информации.

HTML – Hyper Text Meta Language – язык разметки гипер-текста, появился достаточно давно, используется для отображения Web-страниц. Приведем несколько примеров алгоритмов стеганографии адаптированных для HTML:

1. Метод невидимых знаков в конце тэгов[1]: различные комбинации пробелов и знаков горизонтальной табуляции в конце строки, заканчивающейся на тэг.
2. Метод чередования символов конца строки после определенных тэгов[1].
3. Использование невидимых знаков пробелов и горизонтальной табуляции внутри тэга, перед символом, закрывающим тэг[2].

XML - Extensible Markup Language – расширяемый язык разметки, представляющий собой свод общих синтаксических правил. HTML и XML имеют очень схожие синтаксические правила, что позволяет использовать алгоритмы стеганографии адаптированные для HTML и в XML. Рассмотрим несколько примеров алгоритмов стеганографии для XML:

1. Любые алгоритмы стеганографии, применяемые в HTML
2. Алгоритм чередования закрывающего тэга[3].

JSON – JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript и обычно используемый именно с этим языком. JSON получил большое распространение после выхода в свет технологии AJAX. Технология JSON такова, что есть возможность разрабатывать большое количество алгоритмов стеганографии основанных на чередовании символов перевода строки, вставку невидимых символов в конец строки, а также вставку пробелов и горизонтальных табуляторов внутри JSON текста. В силу того что синтаксис JSON является разновидностью синтаксиса JavaScript, можно «прятать» биты информации используя особенности синтаксиса JavaScript, например строку текста в JavaScript можно заключить в двойные или в одинарные кавычки, разницы для интерпретатора JavaScript никакой не будет. Более подробное изучение особенностей синтаксиса JavaScript и JSON обязательно приведет большому числу алгоритмов стеганографии.

К сожалению, у большинства алгоритмов текстовой стеганографии есть один серьезный недостаток, ограничивающий их широкое применение. В отличие от криптографии, где знание алгоритма шифрования не дает возможности расшифровать сообщение, в стеганографии, если известен алгоритм, то сообщение «раскрыто». По этой же причине не рекомендуется использовать один тот же алгоритм стеганографии несколько раз. Поэтому помимо самого алгоритма стеганографии для качественного скрытия информации, необходимо понятие ключа. Ключом может служить маска, по которой в дальнейшем определять скрытые биты полезной информации. А остальные биты, считать мусором, что приводит к большим трудностям или вовсе невозможности восстановления скрытой информации не зная ключа.

Рассмотрим, как можно сделать алгоритм стеганографии с ключом из алгоритма стеганографии для XML с чередованием закрывающего тэга. Пусть мы имеем xml файл, в котором 20 полей. Каждое поле открывается и закрывается тэгом. Мы скрываем биты информации методом чередования закрывающего тэга[3]. Но из 20 полей для скрытия информации мы используем только 5 выбранных случайным образом полей, а в остальные поля прячем случайные биты. Таким образом, ключом будет являться данные о том, в каких полях передается полезная информация. Получается закономерность, чем больше полей в xml файле и меньше размер передаваемой скрытой информации, тем сложнее подобрать ключ. Сегодня размеры передаваемых xml данных составляет несколько сотен полей для небольших Web-приложений и несколько тысяч полей для крупных Web-сервисов. Таким образом, XML является довольно надежным стегоконтейнером, при использовании алгоритмов стеганографии с ключом.

В теории все выглядит не сложно, рассмотрим, как можно осуществить рассмотренный механизм на практике.

В любой современной распределенной информационной системе присутствуют два основных действующих лица – это клиент и сервер. Для реализации стегоканала необходимо разработать модули для работы, как на стороне клиента, так и на стороне сервера. При разработке серверного модуля стегоканала нет особых трудностей. Программист имеет прямой доступ к отправляемым и передаваемым данным. Поэтому, его программа без особого труда может обрабатывать информацию, скрытую по определенному алгоритму с использованием ключа. Клиентская часть приложения может быть реализована по одному из двух принципов: это может быть обычное прикладное приложение, написанное на том же языке и теми же программистами что и серверная часть, или это может быть приложение, работающее через Web-интерфейс. В первом случае, программист добавляет к клиентской части программы такой же модуль обработки скрытой информации, как и на сервере. Во втором случае есть некоторые технологические тонкости, которые необходимо учитывать. О преимуществах приложений работающих через Web-интерфейс говорилось выше, но есть один недостаток: программист, разрабатывающий Web-интерфейс (Web-страницу) не имеет прямого доступа к передаваемым данным. Функцию низкоуровневой обработки информации выполняет браузер, а разработчик видит информацию, которая уже прошла обработку в браузере. Браузер не предоставляет возможности побайтового анализа пришедших данных. Так же браузер не предоставляет возможности добавление байтов в отправляемую информацию. В таких условиях, для осуществления стегоканала, программисту придется писать низкоуровневое программное обеспечение, которое перехватывает пришедший и ушедший трафик средствами, предоставляемыми операционной системой. Таким образом, осуществление стегоканала в Web-приложении более трудоемко, чем в обычных приложениях, но осуществимо.

Мы рассмотрели, как возможно осуществить скрытую передачу информацию с применением секретных ключей в различных приложениях. При передаче информации по стегоканалу необходимо понимать, что чем больше стегоконтейнер и чем меньше размер передаваемой информацией, тем надежнее скрыта передаваемая информация. Поэтому

целесообразно использование стеганографии для передачи не больше чем нескольких десятков байтов. При помощи стеганографии можно решать задачи, в которых размер информации – это не главное, главное – это её наличие. Например, нанесение водяных знаков на различные цифровые документы для подтверждения авторства[1], скрытие электронно-цифровой подписи внутри документа, сохранение контрольной суммы для поддержания целостности передаваемых данных и т.д. Как видно из примеров, при помощи стеганографии можно решать целый ряд прикладных задач.

Рассмотрим, как текстовая стеганография позволяет защититься от одной из современных атак – Фишинг-атаки.

Фишинг (Phishing) - процесс обмана или социальная разработка клиентов организаций для последующего воровства их идентификационных данных и передачи их конфиденциальной информации для преступного использования. Преступники для своего нападения используют spam или компьютеры-боты. При этом размер компании-жертвы не имеет значения; качество личной информации полученной преступниками в результате нападения, имеет значение само по себе[4].

Фишинг-мошенничества продолжают расти не только количественно, но и качественно. Phishing-атакам сегодня подвергается все большее число клиентов, массовая рассылка подобных писем идет на миллионы адресов электронной почты во всем мире. Более того, осуществляются целенаправленные атаки на определенные группы клиентов. Используя множество разновидностей атак, фишеры могут легко ввести в заблуждение клиентов для передачи их финансовых данных (например, номера платежной карты и пароля). В то время как спам был (и продолжает быть) раздражающим, отвлекая и обременяя его получателей, Phishing уже показал свой потенциал, причиняя серьезный ущерб данным и прямые потери из-за мошеннического перемещения валюты[4].

Обладая высоким уровнем защиты от фишинговых атак, организации получат немалую выгоду от сохранения лояльности своих клиентов.

Рассмотрим один из примеров фишинг атаки. Не о чем не подозревающий пользователь получает письмо от привычного для него отправителя, например почтовой службы. Письмо оформлено в таком же строгом стиле. В письме вас просят зайти на сайт почтовой службы и идентифицироваться для якобы правильной работы сервера после сбоя. Внизу указывается ссылка почтового сервера, которая выглядит также или очень похоже на настоящий адрес почтовой службы. После входа перед пользователем тот же привычный сайт, где просят ввести имя пользователя и пароль. Человек, не о чем не подозревающий, вводит свои данные и отправляет на сервер, вот только сервер не почтовой службы, а поддельный.

От такого случая никто не застрахован. Но можно защититься. Существуют различные фишинг-фильтры, где браузер сверяет адреса серверов, но базы адресов необходимо постоянно обновлять, адреса в свою очередь могут меняться, а если злоумышленнику удастся подделать адрес, тогда фильтр не сработает. В таком случае защиты браузера недостаточно. Но такую ситуацию можно заранее предупредить и защититься. Ниже предлагается алгоритм защиты от подобных атак с применением текстовой стеганографии (рис.1).

В предлагаемом решении присутствуют три главных действующих лица: Пользователь, Сервер (который могут подменить) и Сервер генерации ключей.

Любая передаваемая информация, будь то Web-страница или один из форматов текстовой передачи информации (XML, JSON и т.д.) является стегоконтейнером. В стегоконтейнер помещается информация, позволяющая идентифицировать страницу и сказать, кем и когда эта страница была создана, а также цифровая подпись, говорящая о том, что эта страница не была изменена.

Всю скрытую информацию считывает и проверяет специальное программное обеспечение (ПО), которое предоставляется разработчиками приложения и работает не

зависимо от браузера, как фильтр для приходящей и уходящей информации, что делает его прозрачным для пользователя.

Если информация в стегоконтейнере не соответствует ожидаемой (не соответствует контрольная сумма или ЭЦП, не актуальное время создания страницы), значит страница – подделка. Так, можно защититься фишинг-хакеров, которые «не точно» подделывают Вэб-страницы.

Если же подделка качественная, или же это вовсе оригинал, то в таком случае включается второй уровень защиты. Пользователя просят ввести свой Логин для входа в систему. Пользователь отправляет свой логин, сервер проверяет, есть ли такой пользователь в базе данных, если есть, то просит пользователя ввести специальный номер (SN). Специальный номер – это особое число, своего рода ключ, который присваивается каждому пользователю, хранится в базе данных и меняется после каждого использования. Похожая система используется в проходном контроле в крупных организациях, например в банках. Пользователю нет необходимости запоминать специальный номер, более того, пользователь может даже не догадываться о его существовании, за него все сделает загруженное ранее с сервера приложение. Специальный номер генерируется третьей стороной – Сервером генерации ключей.

В стегоконтейнере пришедшей странице для ввода специального номера, кроме всей прочей информации спрятан тот самый специальный номер, который сверяется при помощи программного обеспечения со специальным номером, который сгенерировал Сервер генерации ключей. Связь с Сервером генерации ключей происходит по другому каналу, нежели связь с Вэб-сервером. Этот канал зашифрован и скрыт, при помощи стеганографии[5], например, под видом рекламы. Затем проверенный номер отсылается Вэб-серверу, где снова проверяется и затем меняется до следующего сеанса. Далее сервер посылает страницу для ввода пароля. Таким образом, пользователь может быть уверен, что пароль уйдет на настоящий сервер, а не на поддельный.

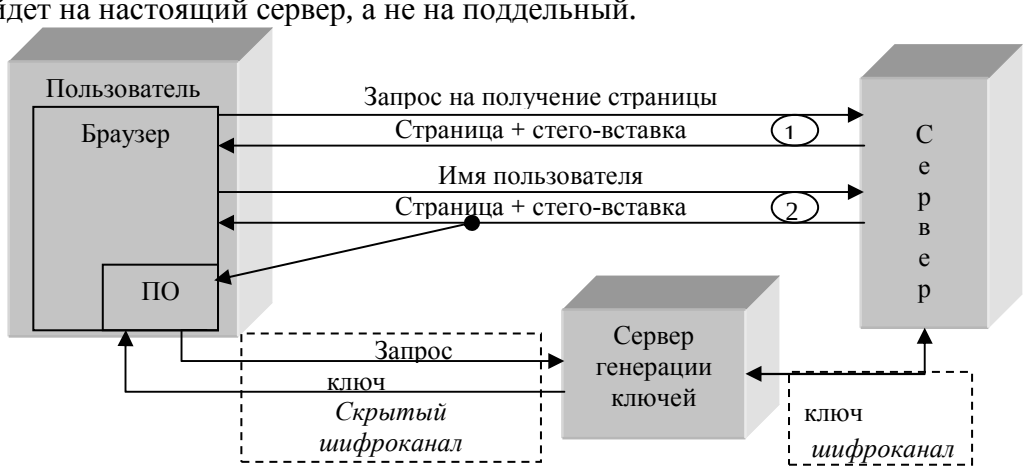

Рис. 1 Схема системы защиты от Фишинг-атаки

В данной схеме можно подделать Сервер, но подделать Сервер генерации ключей, в силу применяемых крипто-алгоритмов, а также стего-алгоритмов очень сложно. До тех пор, пока оба Специальных номера, полученных по разным каналам не будут совпадать или отвечать определенным условиям на стороне клиента, Сервер не выдаст запрос на ввод пароля, а специальное ранее загруженное приложение не даст пользователю ввести и отправить свой пароль.

Таким образом, в статье были рассмотрены и предложены алгоритмы стеганографии в наиболее распространенных современных форматах передачи информации внутри распределенных информационных систем и приложений, предложен принцип стеганографии с использованием ключа, предложены способы реализации стегоканалов с ключом, а также предложен механизм защиты распределенных приложений от фишинг-атак.

Библиографический список:

1. Stanislav S. Barilnik, Igor V. Minin, Oleg V. Minin, «Adaptation of Text Steganographic Algorithms for HTML», 8th International Siberian Workshop and Tutorials EDM'2007, Session IV, JULY 1-5, ERLAGOL

2. Jonathan Cummins, Patrick Diskin, Samuel. Lau and Robert Parlett, «Steganography and Digital Watermarking 2004», School of Computer Science, The University of Birmingham.

3. Aasma Ghani Memon, Sumbul Khawaja, Asadullah Shah, «Steganography: A New Horizon for Safe Communication through XML». Isra UniversityHyderabad, Pakistan.Journal of heoretical and Applied Information Technology ©2005 – 2008

4. Безмалый Владимир Федорович «Фишинг-атаки», режим доступа: http://www.oszone.net/5009/, свободно.

5. Барильник С.С., Минин И.В., Минин О.В., Щетинин Ю.В. «Текстовая стеганография в HTML: реализация скрытых каналов передачи данных» // Вторая международная научно-практическая конференция Виртуальные и интеллектуальные системы 2007 «Ползуновский Альманах», 2007, Барнаул, АГТУ, стр. 28-29.

S.S. Barilnik, I.V. Minin, O.V. Minin
Novosibirsk State Technical University, Russia, Novosibirsk

APPLICATION OF STEGANOGRAPHICS ALGORITHMS FOR THE PRESENT INFORMATION SYSTEMS

It is covered a ways of application of steganographics algorithms for the present information systems and the Web-oriented applications, the types of the possible phishing-attacks, existing methods of the fight with such types of the attacks, as well as system of protection from phishing designed authors on base algorithms of text steganographics in Web-applications.

УДК 004.056.55

Р.Г. Бияшев, Н.А. Капалова, С.Е. Нысанбаева

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДИФИЦИРОВАННОГО АЛГОРИТМА ДИФФИ–ХЕЛЛМАНА НА БАЗЕ МОДУЛЯРНОЙ АРИФМЕТИКИ

Предложена процедура открытого распределения криптографических ключей с использованием непозиционной полиномиальной системы счисления и исследована его криптостойкость.

Обеспечение доставки криптографических ключей отправителям и получателям шифрованных сообщений является одной из основных задач построения криптографической системы. При этом должны выполняться условия по оперативности и точности распределения ключей и скрытности распределяемых ключей.

Применение систем открытого распространения ключей позволяет пользователям обмениваться ключами по незащищенным каналам передачи информации и основана на тех же принципах, что и система шифрования с открытыми ключами. У. Диффи и М. Хеллман предложили в 1976 г. алгоритм для открытого распространения ключей, используемых в симметричных криптографических системах [1]. Идея организации двухстороннего взаимодействия абонентов A и C по открытым каналам связи состоит в следующем. Сначала у A и C отсутствует общая секретная информация, но в конце сеанса связи такая секретная информация (секретный ключ) у A и C вырабатывается. В этом случае при пассивном перехвате информации противник знает, что должно быть получено, но определить выработанный абонентами A и C общий секретный ключ он не может.

Реализовали эту идею У. Диффи и М. Хеллман с помощью функции $y(x) = \theta^x \bmod p$, где p – большое простое число, x – произвольное натуральное число, θ – некоторый примитивный элемент поля $GF(p)$, т.е. $1 \le \theta \le p-1$, а его степени $\theta, \theta^2, \theta^3, ..., \theta^{p-1}$ являются всеми ненулевыми вычетами по модулю p. Числа p и θ считаются общедоступными для всех пользователей системы.

Надежность алгоритма Диффи–Хеллмана обусловлена трудностью вычисления дискретных логарифмов в конечном поле – инвертирование функции $\theta^x \bmod p$ или дискретное логарифмирование является трудной математической задачей. Практическое применение алгоритма Диффи-Хеллмана открытого распространения секретных ключей связано с проблемой выбора такого большого числа p, чтобы задача дискретного логарифмирования была трудной. Основное требование – оно должно быть строго простым.

В докладе представлены результаты по построению и анализу криптостойкости модифицированного (нетрадиционного) алгоритма Диффи-Хеллмана с использованием непозиционных полиномиальных систем счисления (НПСС) [2,3]. Основанием для этого послужили работы, проведенные по разработке и исследованию алгоритмов кодирования, шифрования и формирования электронной цифровой подписи на базе этого нетрадиционного подхода [3,4].

Построение НПСС начинается с выбора системы рабочих полиномиальных оснований $p_1(x), p_1(x), \ldots, p_S(x)$, являющихся неприводимыми многочленами над полем $GF(2)$ степени $m_1, m_2, \ldots, m_S$ соответственно. Рабочий диапазон НПСС определяется многочленом $P_S(x) = p_1(x) p_1(x) \cdot \cdot p_S(x)$ степени $m = \sum_{i=1}^{S} m_i$. Тогда единственное непозиционное представление любого многочлена $F(x)$, степени меньше m, записывается в виде его вычетов (остатков) по модулям рабочих оснований $p_1(x), p_1(x), \ldots, p_S(x)$ соответственно:

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x));$$

(1)

где $F(x) \equiv \alpha_i(x) (\bmod p_i(x))$. По непозиционному виду (1) восстанавливается позиционное представление многочлена $F(x)$ в соответствии с формулой:

$$F(x) = \sum_{i=1}^{S} \alpha_i \{x\} B_i(x), \quad B_i(x) = \frac{P_S(x)}{p_i(x)} M_i(x) \equiv 1 (\bmod p_i(x)),$$

(2)

где $i = 1,2,\ldots,S$, а значения многочленов $M_i(x)$ выбираются из условия выполнения сравнения. При разработке предлагаемого нетрадиционного алгоритма для каждого основания $p_i(x)$ выбирается примитивный элемент (многочлен) $\theta_i(x)$ из полной системы вычетов по модулю $p_i(x)$, т. е. степени $\theta_i(x)$ меньше m_i, $i = 1,2,\ldots,S$. По аналогии с представлением (1) примитивные многочлены $\theta_i(x)$ интерпретируются как остатки от деления некоторого многочлена $PR(x)$ на рабочие основания соответственно:

$$PR(x) = (\theta_1(x), \theta_2(x), ..., \theta_S(x)).$$

Рабочие основания НПСС $p_1(x), p_1(x), \ldots, p_S(x)$ и примитивные элементы $\theta_1(x), \theta_2(x), ..., \theta_S(x)$ являются секретной информацией.

Для восстановления позиционного вида многочленов находятся базисы НПСС по выражению (2). Для этого определяются полиномы $\delta_i(x) \equiv \frac{P_S(x)}{p_i(x)} (\bmod p_i(x))$, $i = 1,2,\ldots,S$. Находятся также и инверсные к ним многочлены $\delta_i^{-1}(x)$: $\delta_i^{-1}(x) \delta_i(x) \equiv 1 (\bmod p_i(x))$, $i = 1,2,\ldots,S$. В соответствии с формулой (2) вычисляются базисы по следующим выражениям:

$$B_i(x) = \delta_i^{-1}(x) \cdot \frac{P_S(x)}{p_i(x)}.$$

Многочлены $B_i(x)$ также держатся в секрете. Затем абоненты A и C, как и классическом алгоритме Диффи–Хеллмана, выбирают случайно и независимо друг от друга по одному секретному ключу β_A и β_C соответственно: $1<\beta_A, \beta_C < 2^m$. Далее каждый из участников обмена вычисляет новый элемент – открытый ключ. Абонент A определяет:

$$G_A(x) = (G_{A_1}(x), G_{A_2}(x), ..., G_{A_S}(x)), \text{ где } G_{A_i}(x) \equiv \theta_i^{\beta_A}(x) (\text{mod } p_i(x)).$$

где i =1,2,…,S. Абонент C находит:

$$G_C(x) = (G_{C_1}(x), G_{C_2}(x), ..., G_{C_S}(x)), \text{ где } G_{C_i}(x) \equiv \theta_i^{\beta_C}(x) (\text{mod } p_i(x));$$

где i =1,2,…,S. Операции возведения в степень могут выполняться параллельно по модулям полиномов, выбранных в качестве рабочих оснований НПСС. Затем A и C обмениваются элементами $G_A(x)$ и $G_C(x)$ по открытому каналу связи. После получения $G_C(x)$ абонент A по своему секретному ключу β_A вычисляет новый элемент – общий секретный ключ:

$$G_{cg}(x) = (G_C(x))^{\beta_A} = (G_{cg1}(x), G_{cg2}(x), ..., G_{cgS}(x)), \; G_{cgi}(x) \equiv (G_{C_i}(x))^{\beta_A} (\text{mod } p_i(x));$$

где i=1,2,…,S. Абонент C по полученному $G_A(x)$ и по своему секретному ключу β_C вычисляет

$$G'_{cg}(x) = (G_A(x))^{\beta_C} = (G'_{cg1}(x), G'_{cg2}(x), ..., G'_{cgS}(x)), \; G'_{cgi}(x) \equiv (G_{A_i}(x))^{\beta_C} (\text{mod } p_i(x));.$$

где i=1,2,…,S. Поскольку $(PR(x)^{\beta_C})^{\beta_A} (\text{mod} P_S(x) \equiv (PR(x)^{\beta_A})^{\beta_C} (\text{mod} P_S(x))$, то и $G_{cg}(x) = G'_{cg}(x)$. В результате указанных действий абоненты A и C стали обладателями общего элемента $G_{cg}(x)$, который и объявляется общим ключом абонентов A и C.

Утверждение. Криптостойкость нетрадиционного алгоритма открытого распределения ключей определяется всеми возможными способами выбора систем рабочих оснований и соответствующих им примитивных элементов, а также нахождением секретного ключа одного из участников открытого обмена.

Пусть криптоаналитик знает степень рабочего диапазона алгоритма и длины открытых ключей. Чтобы найти секретный ключ, он также должен знать один из ключей β_A или β_C.

Выбор рабочих оснований производится с условием выполнения равенства:

$$k_1 m_1 + k_2 m_2 + ... + k_S m_S = m;$$

(3)

где $0 \le k_i \le n_i$ - число выбранных неприводимых многочленов степени m_i, n_i - количество всех неприводимых многочленов степени m_i, $1 \le m_i \le N$, i=1,2,...,S, $S = k_1 + k_2 + ... + k_S$ - количество выбранных рабочих оснований. Уравнение (3) определяют количество S неприводимых многочленов различных степеней, которые можно выбрать в качестве оснований системы, запись вычетов по которым покрывает длину $G_A(x)$ и $G_C(x)$.

Возможное количество способов выбора одной системы из S оснований определяется также всеми возможными в ней перестановками оснований $p_1(x), p_1(x), \ldots, p_S(x)$, т. е. конкретными значениями коэффициентов $k_1, k_2, ..., k_S$, удовлетворяющих уравнению (3).

На следующем этапе противник находит выражение для определения числа способов выбора примитивных элементов для одной сформированной системы рабочих оснований. Выбор примитивного многочлена $\theta_i(x)$ осуществляется с проверкой на примитивность, а степень его должна быть не выше степени m_i основания $p_i(x)$, i=1,2,...,S. Общее число всех возможных вариантов выбора примитивных многочленов по всем рабочим основаниям тогда будет равно:

$$f = \prod_{i=1}^{S}(2^{m_i} - 2).$$

(4)

Завершающий шаг криптоаналитика после положительных итогов на двух предыдущих этапах – нахождение одного из секретных ключей абонентов *A* и *C*. Он возводит примитивные элементы $\theta_i(x)$ в степень *r*, *i*=1,2,...,*S*, до совпадения результата возведения в степень с $G_A(x)$ или $G_C(x)$, тогда $r = \beta_A$ или $r = \beta_C$. Поскольку секретный ключ для системы оснований один, то по одному найденному $\theta_i(x)$ автоматически определяются и другие примитивные элементы. На этом этапе число всех возможных проверок описывается выражением, которое совпадает с (4). Тогда, с учетом (3) и (4), криптостойкость нетрадиционного алгоритма Диффи-Хеллмана определяется выражением:

$$p_{cg} = \frac{1}{\sum\limits_{k_1 k_2 \ldots k_S} \left[(k_1 + k_2 + \ldots + k_S)! C_{n_1}^{k_1} C_{n_2}^{k_2} \ldots C_{n_S}^{k_S} \cdot \left(\prod_{i=1}^{S}(2^{m_i} - 2) \right)^2 \right]}. \qquad (5)$$

Из выражения (5) следует, что криптоаналитику для поиска одного из секретных ключей открытого их распространения необходимо решить весьма непростую задачу. В таблице приведены полученные значения p_{cg} для длины секретного ключа от 2 до 16 бит. Увеличение длины ключа $G_{cg}(x)$ от 2 до 16 бит приводит к росту криптостойкости на 14 порядков, а на 1 бит – примерно на 1 порядок.

Для сравнения вычислим значения криптостойкости разработанного на базе модулярной арифметики алгоритма открытого распространения ключей p_{cg} для длин ключей 128, 192 и 256 бит стандарта шифрования AES .

Для длины секретного ключа $G_{cg}(x)$ =128 бит сформируем систему рабочих оснований из 8 неприводимых многочленов 16-й степени, тогда $p_{cg} = \frac{1}{8! C_{7749}^{8} \{(2^{16} - 2)^8\}^2} \approx \frac{1}{10^{109}}$, где число 7749 – количество неприводимых многочленов 16 степени над полем *GF*(2).

Для секретного ключа из 192 бит при выборе системы рабочих оснований из 12 неприводимых многочленов 16-й степени имеем: $p_{cg} = \frac{1}{12! C_{7749}^{12} \{(2^{16} - 2)^{128}\}^2} \approx \frac{1}{10^{163}}$.

При длине ключа 256 бит для выбранной системы оснований из 16 неприводимых полиномов 16-й степени получим: $p_{cg} = \frac{1}{16! C_{7749}^{16} \{(2^{16} - 2)^{16}\}^2} \approx \frac{1}{10^{217}}$.

Таблица 1

Криптостойкость нетрадиционного алгоритма открытого распространения ключей

Длина секретного ключа, бит	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Крипто-стойкость открытого обмена, p_{cg}	–	$2{,}1 \cdot 10^{-1}$	$1{,}4 \cdot 10^{-2}$	$1{,}0 \cdot 10^{-3}$	$1{,}7 \cdot 10^{-4}$	$2{,}4 \cdot 10^{-5}$	$2{,}4 \cdot 10^{-6}$	$3{,}2 \cdot 10^{-7}$	$3{,}4 \cdot 10^{-8}$	$3{,}9 \cdot 10^{-9}$	$3{,}4 \cdot 10^{-10}$	$4{,}8 \cdot 10^{-11}$	$4{,}7 \cdot 10^{-12}$	$6{,}5 \cdot 10^{-13}$	$6{,}7 \cdot 10^{-14}$	$7{,}1 \cdot 10^{-15}$

Таким образом, использование НПСС (нетрадиционного подхода) при построении алгоритма открытого обмена секретными ключами позволяет существенно повысить его криптостойкость. Эффективность этого алгоритма обусловлена тем, что, в соответствии с операциями непозиционной системы счисления, вычисления в нем выполняются параллельно по модулям оснований НПСС.

Работа выполнена в рамках программы фундаментальных исследований, финансируемой Министерством образования и науки Республики Казахстан.

Библиографический список

1. Диффи, У. Защищенность и имитостойкость: Введение в криптографию / У. Диффи, М. Э. Хеллман // ТИИЭР – Труды института инженеров по электротехнике и радиоэлектронике / Том 67, № 3. 1979. с. 71–109.

2. Акушский, И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д. И. Юдицкий. М.: Советское радио, 1968. - 439 с.

3. Бияшев, Р. Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: Дис. на соискание уч. степ. докт. тех. наук / Р. Г. Бияшев. М., 1985. - 328 с.

4. Бияшев, Р. Г. Исследование надежности корректирующей электронной цифровой подписи / Р. Г. Бияшев, С. Е. Нысанбаева // Управление защитой информации / Минск-Москва, 2007. Том 11, № 4. с. 447-453.

R.G. Biyashev, N.A. Kapalova, S.E. Nyssanbayeva

DEVELOPMENT AND RESEARCH OF MODIFIED DIFFIE-HELLMAN ALGORITHM ON BASIS MODULAR ARITHMETIC

The open distribution algorithm of secret keys with use non-positional polynomial notations is constructed and it cryptostability is investigated.

УДК 621.391.1.004

Д. В. Малухин

ПРОТОКОЛ СМЕНЫ КЛЮЧЕВОЙ ИНФОРМАЦИИ ДЛЯ ПРОЗРАЧНОГО ШИФРОВАНИЯ СИГНАЛА УПРАВЛЕНИЯ КОСМИЧЕСКИМ АППАРАТОМ

В работе описано дополнение протокола прозрачного шифрования, разработанного для организации сеансов передачи данных по защищенному каналу связи «земля-борт» протоколом смены ключевой информации. Протокол определяет порядок смены ключевой информации в каналах «земля-борт» и «борт-земля».

Задача рассматриваемой работы – разработка протокола смены ключевой информации для программно-аппаратного комплекса фазовой модуляции команд управления космическим аппаратом.

Актуальность работы. Для обеспечения должного уровня конфиденциальности информации, поступающей на борт космического аппарата (КА) и приходящей с борта КА необходима поддержка защиты ключевой информации от её компрометации. Одним из способов обеспечения данной защиты является своевременная смена ключевой информации в канале связи.

Для организации защищенного канала передачи данных в систему космической связи устанавливаются аппаратные модули обработки информации (МОИ), выполняющие шифрование данных по заданному алгоритму шифрования в режиме, определенном для обработки логической единицы передаваемых данных (кадра). В качестве используемого

в системе алгоритма используется ГОСТ 28147-89 [2]. Функционирование алгоритма осуществляется в режиме гаммирования с обратной связью с дополнительной выработкой имитовставки для каждого кадра передаваемых данных [3]. Данные с выхода соответствующей КС ЦУП поступают на вход МОИ, где происходит их зашифрование. Зашифрованные данные поступают на вход наземной КИС, выполняется формирование кадра, модулированный по соответствующему стандарту сигнал конвертируется и передается на наземную приемно-передающую систему (ППС). С ППС ЦУП сигнал транслируется и принимается ППС КА. Затем сигнал поступает в КИС КА, с выхода которой полученные зашифрованные данные передаются в МОИ, расшифровываются и поступают в бортовой компьютер (БК) КА. Передача данных с КА в ЦУП осуществляется аналогичным образом (рис. 1). Особенности функционирования данной системы и обоснование выбора режима работы алгоритма шифрования данных приведены в [1].

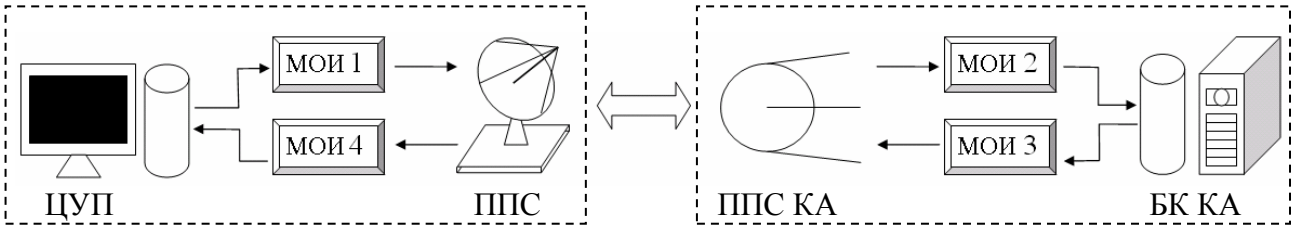

Рис. 1. Место МОИ в канале передачи данных «земля-борт»

Также каждый МОИ имеет двунаправленную связь со смежным МОИ (МОИ 1 с МОИ 4, МОИ 2 с МОИ 3) по дополнительному проводному интерфейсу связи.

Структура кадра, формируемого в МОИ представлена на рис. 2:

Синхропосылка	Служебные данные	Вектор 1	Вектор 2	Шифруемые данные	Имитовставка
		64 бита	64 бита	128...1024 бит	32 бита

Рис. 2. Структура кадра, формируемого в МОИ

Здесь «Вектор 1» – инициализирующий вектор (синхропосылка) для выработки сеансового ключа. «Вектор 2» – инициализирующий вектор (синхропосылка) для расшифрования данных. К сформированному кадру добавляется синхропосылка, служебные данные, и кадр передаётся далее на ППС.

В служебных данных указывается тип кадра: служебный либо кадр с данными. Кадры с данными подвергаются распаковке и расшифровке в МОИ-приёмнике, и передаются далее на БК КА, либо в ЦУП. Информационная часть служебных кадров не передаётся МОИ далее по цепи, а анализируется им же.

Ключевая информация в системе представлена в виде долговременной ключевой информации (долговременные ключи и таблицы замен) и сеансовых ключей. Долговременная ключевая информация (ДКИ) прописывается в каждый МОИ на этапе его создания, и дальнейшая её смена осуществляется путём задания адреса ключа или таблицы, а не их передачи. ДКИ, прописанная для пары МОИ «земля – борт» должна быть идентичной. Сеансовые ключи используются для шифрования только текущего кадра.

Предусмотрено два режима управления заменой используемой ДКИ:

1. Посредством директивы ЦУП.
   a. директива на смену ДКИ в канале «МОИ 1 – МОИ 2»
   b. директива на смену ДКИ в канале «МОИ 3 – МОИ 4»
2. В автоматическом режиме по превышению счётчиком объёма зашифрованных данных с использованием текущей ДКИ определённого лимита.

МОИ 1 и МОИ 3 настроены на автоматическую смену ДКИ по счётчику объёма зашифрованных данных. При этом пороговые уровни смены долговременных ключей и таблиц замен различны. Посредством директивы ЦУП возможна смена ДКИ в любом из

двух каналов до превышения счётчиком лимита. Это необходимо, к примеру, при обнаружении факта компрометации ДКИ. Значение счётчика при этом обнуляется.

Далее представлены алгоритмы работы системы для различных ситуаций.

I. Смена ДКИ в канале МОИ 1 – МОИ 2 (по директиве из ЦУП, либо в автоматическом режиме).
   1. В МОИ 1 формируется служебный кадр (рис. 2) с информационной частью, включающей в себя следующие данные:
      a) Временная метка создания кадра;
      b) Адресат данного кадра (МОИ 2);
      c) Тип служебного кадра (управляющий);
      d) Тип сменяемой ДКИ (долговременный ключ или таблица замен);
      e) Указатель на адрес новой ДКИ.

      После передачи служебного кадра МОИ 1 переходит в состояние ожидания подтверждения об успешной смене на МОИ 2 ДКИ. Передача информационных кадров в этот период прекращается.
   2. Приняв кадр, МОИ 2 убеждается, что он служебный и подвергает его распаковке, расшифровке и проверки целостности. Далее МОИ 2 сравнивает временную метку кадра с бортовым временем, и если разница времени превышает определённый интервал – кадр отбрасывается. В противном случае МОИ 2 проверяет, адресован ли кадр ему, является ли кадр управляющим и при положительном результате производит смену ДКИ.
   3. МОИ 2 передаёт по дополнительному интерфейсу связи в МОИ 3 команду об отправке подтверждения о смене ДКИ на землю.
   4. МОИ 3 формирует служебный кадр (рис. 2) с информационной частью, включающей в себя следующие данные:
      a) временная метка создания кадра;
      b) адресат данного кадра (МОИ 1);
      c) тип служебного кадра (подтверждающий).

      Данный кадр вставляется в поток кадров, проходящий из МОИ 3 в МОИ 4.
   5. МОИ 4 принимает служебный кадр, распаковывает и расшифровывает его, проверяет временную метку и отправляет адресату кадра (МОИ 1) по дополнительному интерфейсу связи подтверждение о корректной смене ДКИ на МОИ 2.
   6. МОИ 1 получает от МОИ 4 подтверждение, и работа алгоритма I завершается. После получения подтверждения передача информационных кадров возобновляется. Следующий кадр МОИ 1 формирует уже с использованием новой ДКИ.
   7. Если подтверждение от МОИ 2 не приходит на МОИ 1 за определённый промежуток времени T (этот промежуток должен быть на порядок ниже промежутка для оценки временной метки), переходим на п. I.1. При этом кадр в п. I.1 формируется на старой ДКИ. При второй неудачной попытке кадр в п. I.1 формируется на новой ДКИ. Данное чередование продолжается до тех пор, пока не будет получено подтверждение об успешной смене ДКИ.

II. Передача директивы из ЦУП на смену ДКИ в канале МОИ 3 – МОИ 4 через канал МОИ 1 – МОИ 2.
   1. В МОИ 1 формируется служебный кадр (рис. 2) с информационной частью, включающей в себя следующие данные:
      a) Временная метка создания кадра;
      b) Адресат данного кадра (МОИ 3);
      c) Тип служебного кадра (управляющий);
      d) Тип сменяемой ДКИ;

e) Указатель на адрес новой ДКИ.

После передачи служебного кадра МОИ 1 переходит в состояние ожидания команды от МОИ 4 на передачу подтверждения для МОИ 3 об успешной смене на МОИ 4 ДКИ. Передача информационных кадров в этот период в канале МОИ 1 – МОИ 2 не прекращается.

2. Приняв служебный кадр МОИ 2 распаковывает и расшифровывает его, проверяет временную метку и отправляет адресату кадра (МОИ 3) по дополнительному интерфейсу связи команду на смену ДКИ в канале и информацию о новой ДКИ. Далее переходим к алгоритму III.
3. Если команда на передачу подтверждения от МОИ 4 не приходит на МОИ 1 за промежуток времени T, переходим на п. II.1.

III. Смена ДКИ в канале МОИ 3 – МОИ 4 (по директиве из ЦУП, переданной посредством МОИ 2, либо в автоматическом режиме).

1. В МОИ 3 формируется служебный кадр (рис. 2) с информационной частью, включающей в себя следующие данные:
   a) Временная метка создания кадра;
   b) Адресат данного кадра (МОИ 4);
   c) Тип служебного кадра (управляющий);
   d) Тип сменяемой ДКИ;
   e) Указатель на адрес новой ДКИ.

   После передачи служебного кадра МОИ 3 переходит в состояние ожидания подтверждения об успешной смене на МОИ 4 ДКИ. Передача информационных кадров в этот период прекращается.
2. Приняв служебный кадр МОИ 4 распаковывает и расшифровывает его, проверяет временную метку. В случае успеха МОИ 4 проверяет, адресован ли кадр ему, является ли кадр управляющим и при положительном результате производит смену ДКИ.
3. МОИ 4 передаёт по дополнительному интерфейсу связи в МОИ 1 команду об отправке подтверждения о смене ДКИ на борт КА.
4. МОИ 1 формирует служебный кадр (рис. 2) с информационной частью, включающей в себя следующие данные:
   a) Временная метка создания кадра;
   b) Адресат данного кадра (МОИ 3);
   c) Тип служебного кадра (подтверждающий);

   Данный кадр вставляется в поток кадров, проходящий из МОИ 1 в МОИ 2.
5. МОИ 2 принимает служебный кадр, распаковывает и расшифровывает его, проверяет временную метку и отправляет адресату кадра (МОИ 3) по дополнительному интерфейсу связи подтверждение о корректной смене ДКИ на МОИ 4.
6. МОИ 3 получает от МОИ 2 подтверждение, и работа алгоритма III завершается. После получения подтверждения передача информационных кадров возобновляется. Следующий кадр МОИ 3 формирует уже с использованием новой ДКИ.
7. Если подтверждение от МОИ 4 не приходит на МОИ 3 за определённый промежуток времени, переходим на п. III.1. При этом кадр в п. III.1 формируется на старой ДКИ. При второй неудачной попытке кадр в п. III.1 формируется на новой ДКИ. Данное чередование продолжается до тех пор, пока не будет получено подтверждение об успешной смене ДКИ.

В результате был разработан протокол смены ДКИ. Алгоритмы, входящие в состав протокола активизируются как автоматически, так и по директиве из ЦУП.

Положительными моментами данных алгоритмов является наличие обратной связи для подтверждения безошибочного приёма служебной команды, прозрачность работы комплекса МОИ (остальные элементы системы не участвуют в смене ДКИ) и обеспечение защиты от разрушающих действий злоумышленника (защита от повторной отправки служебных кадров, криптографическое скрытие адреса новой ДКИ).

Библиографический список

1. Чалкин, Т. А. Разработка алгоритма построения узлов замен алгоритма шифрования ГОСТ 28147-89 / Т. А. Чалкин, К. М. Волощук // Вестник СибГАУ : сб. науч. тр., в 2 ч. Вып. 1. Красноярск, 2009. Ч. 2. С. 46-50.

2. Государственный комитет СССР по стандартам. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147-89. – М.: ИПК Издательство стандартов, 1996. – 28 с.

3. Винокуров, А. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы x86 [Электронный ресурс] / А. Винокуров. - Режим доступа: http://re-tech.narod.ru/inf/crypto/gost.htm.

УДК 004.056

К.В. Мушовец

МОДИФИКАЦИЯ ПРОТОКОЛА АУТЕНТИФИКАЦИИ CHAP ДЛЯ ПРОТИВОДЕЙСТВИЯ НЕКОТОРЫМ ТИПОВЫМ АТАКАМ

В статье приведен обзор методов защиты программ от несанкционированного использования и модификации. Приведены методы атак на технологии защиты.

В настоящее время телекоммуникационные технологии стремительно развиваются. Для передачи информации в них используются разные механизмы, обеспечивающие различные функции. Будь то устранение шумов в канале передачи информации, поддержание высокой скорости передачи, обеспечение конфиденциальности передаваемых данных, осуществление удобного для пользователя интерфейса. В данной статье рассматривается основной элемент сетевой системы аутентификации - протокол аутентификации. В процессе обмена данными аутентификация имеет очень большое значение. Ведь для того чтобы начать процесс передачи важных сведений их владелец, должен быть уверен в подлинности получателя. В настоящее время существует много различных протоколов аутентификации. Изучение этого вопроса приобретает все большее значение на рынке телекоммуникационных услуг.

Автором ранее был проведен анализ протоколов аутентификации, по результатам которого выяснилось, что протокол CHAP обладает рядом преимуществ перед другими рассмотренными протоколами, главным из которых является достаточно простой метод аутентификации пользователя. Также к преимуществам CHAP относится отсутствие избыточности служебной информации в пакетах, небольшое количество сообщений передаваемых между пользователями, что положительным образом отражается на быстродействии протокола. Но у CHAP есть свои недостатки. Основным из них является низкий уровень защищенности протокола. Используемый в протоколе механизм “оклик\отзыв”, позволяет исключить некоторые виды атак. Но по-прежнему остаются уязвимые места, которыми может воспользоваться злоумышленник. Для их устранения предлагается провести ряд модификаций протокола.

Для упрощения описания порцедуры аутентификации протокола CHAP введем обозначения: П2 - пользователь запрашивающий аутентификацию, П1 – аутентифицирующий пользователь.

В ходе протокола между его участниками пересылаются три пакета: Challenge, Response и Success или Failure. Предложенная модификация вносит изменения только в формат пакета Challenge.

В общем виде формат пакета Challenge выглядит следующим образом:

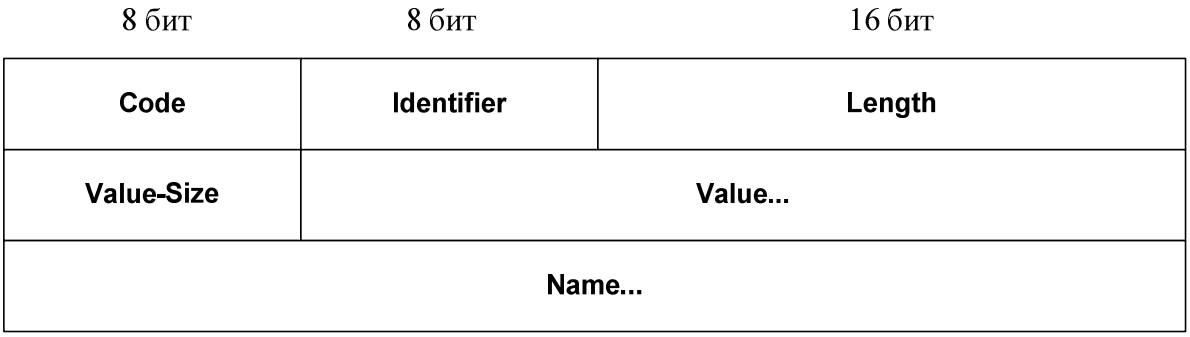

Рисунок 1 – Формат пакета Challenge протокола CHAP

Поле Identifier предсталяет собой идентификатор, который позволяет устанавливатиь соответствие посланных запросов и полученных на эти запросы ответов. Оно также необходимо для формирования пакета Response. Это поле содержит уникальную последовательность из 8 бит. В качестве модификации протокола CHAP предлагается в поле Identifier помещать не просто уникальную последовательность битов, а метку времени. Но возникает проблема. Для того чтобы метка времени была уникальной она должна содержать данные в следующем формате год:месяц:число:час:минута:секунда. Поле Identifier состоит из восьми бит и может принимать 2^8=256 различных значений. Этого не достаточно для описания метки в требуемом формате. Необходимо 24 бита. Для уменьшения объема метки предлагатся использовать результат функции $f(x) = x \bmod 2^8$ (где x – значение метки), что позволит поместить ее в поле Identifier.

Таким образом, после получения пакета Challenge, пользователь П2, вычисляет функцию f(x) от текушего значения времени и вычисляет разницу со значением поля Identifier. Если разница превышает допустимое значение, пользователь П2 посылает пакет Failure пользователю П1.

Также предлогается в пакет Challenge добавить дополнительный блок данных зашифрованный общим ключом. Этот блок должен содержать следующие данные: Имя получателя || Identifier || Имя отправителя сообщения Challenge. Знак “||” обозначает операцию конкатенации.

Таким образом, работу модифицированного протокола CHAP можно описать так:

Пользователь П1 формирует пакет Challenge. Для этого он вычисляет метку времени, генерирует случайное значение поля Value.

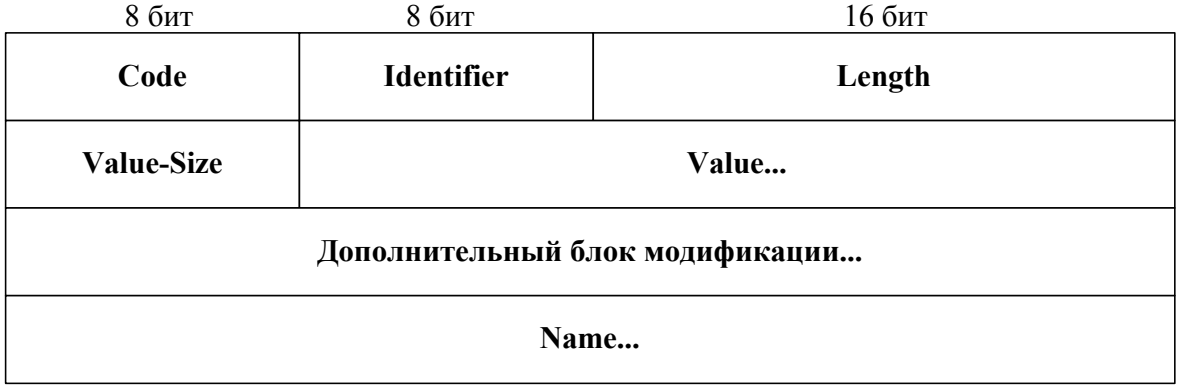

Рисунок 2 – Формат пакета Challenge модифицированного протокола CHAP

Code – однооктетное поле, испльзуемое для указания типа пакета. Поле Code может принимать следующие значения:

1 Challenge
2 Response
3 Success
4 Failure

Identifier – однооктетное поле. Представляет собой метку указывающую на момент создания сообщения. Поле Identifier необходимо для сопоставления пакетов, относящихся к одному сеансу работы протокола, а также для контроля значения задержки пакета при передаче.

Length – двухоктетное поле, указывающее размер пакета.

Value-Size – однооктетное поле, указывающее размер поля Value.

Value – поле переменного размера, содержащее сгенерированное пользователем значение challenge.

Дополнительный блок модификации – поле переменного размера, содержит данные: имя получателя, соответствующее данным об адресате указанным в заголовке пакета PPP || Identifier || Имя отправителя сообщения Challenge. Данное поле зашифрованно однонаправленно хэш-функцией.

Name – поле переменного размера, позволяющего идентифицировать систему передачи пакета.

После того как П2 получил пакет Challenge, он должен применить одностороннюю хэш-функцию на строку состоящую из значений своего имени, поля Identifier и имени пользователя отправившего сообщение. Затем он должен сравнить получившееся значение со значением поля Дополнительный блок модификации пакета Challenge. В случае совпадения значений он должен продолжить процесс аутентификации. В случае несовпадения отправить сообщение Failure пользователю П1. Также пользователь П2 должен сравнить момент времени, указанный в поле Identifier с его текущим временем и в случае превышения допустимой задержки также послать сообщение Failure пользователю П1.

Если обе проверки прошли успешно то пользоветель П2 формирует сообщение Response путем применения хэш-фукнции на строку, состоящую из значений идентификатора, “секрета” и значения поля Value из пакета Challenge.

После того как пльзователь П1 получит пакет Response, он должен проделать процедуру аналогичную той, которую делал пользователь П2 при формировании поля Value для пакета Response и сравнить полученное значение со значением поля Value пакета Response. В случае совпадения пользователь П2 формирует пакет Success и отправляет его пользователю П1. Аутентификация считается пройденной. Если значения не совпадают, то П2 формирует пакет Failure и отправляет его П1. В этом случае аутентификация считается не пройденной.

Протокол аутентификации CHAP предусматривает одностороннюю аутентификацию. Применяемые в нем механизмы позволяют предотвращать следующие виды атак:

1. Пересылка зашифрованных значений Identifier и challenge в сообщении Response препятствует злоумышленнику осуществить атаку с повторной передачей сообщения. Так как эти значения уникальны и вероятность их повторения ничтожно мала;

2. Секрет, присутствующий в поле Value пакета Response, указывает на принадлежность пакета пользователю, что предотвращает возможность атак с помощью отражения сообщений.

3. Также секрет препятствует осуществлению злоумышленником атаки с помощью чередования сообщений, так как явно указывает на принадлежность пакета отправителю.

Предложенная же модификация позволяет исключить еще некоторые варианты атак на протокол аутентификации CHAP.

1. Так как поле Identifier содержит не просто уникальную последовательность битов, а указывает на время создания сообщения, можно избежать атаки с помощью повторения сообщения, реализованной злоумышленником выдающим себя за пользователя П1.

2. Имя отправителя, указанное в поле Дополнительный блок модификации, позволяет предотвратить атаку “человек посередине”. Так как результат применения хэш-функции на строку, состоящую из имени получателя, Identifier и имени злоумышленника не совпадет со значением поля Дополнительный блок модификации.

3. Указание имени отправителя в поле Дополнительный блок модификации пакета Challenge, указывает на принадлежность пакета пользователю П1, что предотвращает возможность атак возможность атак с помощью отражения сообщений.

После проведения модификации протокола CHAP, вырос уровень его защищенности, за счет сокращения количества уязвимостей. Дальнейшие модификации протокола могут привести к нежелательному снижению его быстродействия.

K.V. Mushovets

MODIFICATION OF MS CHAP FOR SOME TYPICAL ATTACKS PREVENTION

Here is considered some modifications of MS CHAP. Also in paper illustrates typical attack methods and their preventions with use of new modifications.

УДК 519.72 (075.8)

Подколзин В.В., Осипян В.О.

ВЕРХНЯЯ ГРАНИЦА ЧИСЛА РЕШЕНИЙ ОБОБЩЕННОЙ ЗАДАЧИ О РЮКЗАКЕ НА ЗАДАННОМ ВХОДЕ

В настоящей статье рассматриваются вопросы определения верхней границы числа решений входов рюкзачных систем защиты информации. В ней определены критерии инъективности рюкзачных систем, а также метод вычисления максимального количества решений для заданного входа для неинъективных рюкзачных систем

При моделировании систем защиты информации с открытым ключом и с рюкзаком, обладающим заранее заданными свойствами, особое место занимает задача определения верхней границы числа входов для РСЗИ.

Пусть $A=(a_1,a_2, \ldots, a_n)$ – рюкзачный вектор размерности n ($n\geq 3$) из n различных натуральных компонентов a_i, i=1..n (здесь 1..n - отрезок натуральных чисел от 1 до n); (A, v) – вход задачи о рюкзаке, где v – также некоторое натуральное число; $Z_p=\{0, 1, 2 ,\ldots, p-1\}$ – множество коэффициентов повторений компонент входа. Рюкзачный вектор $A=(a_1,a_2, \ldots, a_n)$ назовём с повторениями или без повторений, если его элементы повторяются или нет – соответственно. Для простоты изложения будем считать, что значения компонент рюкзачного вектора расположены в неубывающем порядке своих значений.

Рассмотрим рюкзачные вектора без повторений. В дальнейшем рюкзачный вектор A будем называть рюкзаком A.

Определение 1. Два рюкзака $A=(a_1,a_2, \ldots, a_n)$ и $B=(b_1,b_2,\ldots,b_m)$ размерностей n и m соответственно назовем несовпадающими, если в одном из них существует компонент, не содержащийся в другом.

Определение 2. Два рюкзака $A=(a_1,a_2, \ldots, a_n)$ и $B=(b_1,b_2,\ldots,b_m)$ размерностей n и m соответственно назовем различными если всякий компонент A не содержится в B.

Определение 3. Два несовпадающих рюкзака $A=(a_1,a_2, \ldots, a_n)$ и $B=(b_1,b_2,\ldots,b_m)$ размерностей n и m соответственно назовем совместимыми в Z_p, если существует ненулевое значение v, которое может быть выражено в обоих рюкзаках с коэффициентами компонентов из Z_p, т.е. допустимы входы (A,v) и (B,v). В противном случае – несовместимыми.

Другими словами уравнения

$$\sum_{i=1}^{n} \alpha_i a_i = v, \ (\alpha_i \in Z_p, \ i = 1..n) \quad (1)$$

$$\sum_{j=1}^{m} \beta_j b_j = v \ , \ (\beta_j \in Z_p, \ j = 1..m) \quad (2)$$

относительно переменных (α_1, α_2, …, α_n) и (β_1, β_2, …, β_m) соответственно, имеют ненулевые решения.

Таким образом, для двух несовпадающих совместимых в Z_p рюкзаков A=(a_1,a_2, …, a_n) и B=(b_1,b_2,…,b_m) существуют два вектора (δ_1, δ_2,…, δ_n) размерности n и (σ_1, σ_2,…, σ_m) размерности m таких, что выполняется равенства

$$\sum_{i=1}^{n} \delta_i a_i = \sum_{j=1}^{m} \sigma_j b_j = v, \quad (3)$$

при условии:

$\delta_i \in Z_p, \ i = 1..n$ и $\sigma_j \in Z_p, \ j = 1..m$. (4)

Определение 4. Рюкзак A=(a_1,a_2, …, a_n) размерности n является подрюкзаком B=(b_1,b_2,…,b_m) размерности m (n≤m) тогда и только тогда, когда всякий компонент A является компонентом B. Если A – подрюкзак B, то будем обозначать $A \prec B$

Утверждение 1. Для рюкзака A=(a_1,a_2, …, a_n) размерности n, все компоненты которого различны ($\forall i,j \ a_i \neq a_j, \ i \neq j$), уравнение (1) может иметь более одного решения тогда, и только тогда, когда существуют два различных совместимых в Z_p рюкзака B и C таких, что $B \prec A$ и $C \prec A$.

Следствие: Обобщенно сверхрастущий рюкзак является инъективным.

Рассмотрим два различных совместимых в Z_p рюкзака A=(a_1,a_2, …, a_n) и B=(b_1,b_2,…,b_m). Для каждой пары (δ_1, δ_2,…, δ_n) и (σ_1, σ_2,…, σ_m) значений наборов коэффициентов переменных (α_1, α_2, …, α_n) и (β_1, β_2, …, β_m), удовлетворяющих (3) при условии (4) найдем максимум $\mu = \max\{\delta_1, \delta_2,\ldots, \delta_n, \sigma_1, \sigma_2,\ldots, \sigma_m\}$. Среди полученных значений μ выберем наименьшее, которое обозначим $\mu(A, B)$.

Назовем значение

$$\left\| (A,B) \right\| = [P/\mu(A, B)]+1. \quad (6)$$

коэффициентом подмены для двух различных совместимых в Z_p рюкзаков A и B.

Определение 5. Пара рюкзаков (A, B), A=(a_1, a_2, …, a_n) и B=(b_1, b_2, …, b_m), упорядочена по возрастанию, если $\begin{cases} a_1 < b_1 \\ a_i < b_i \ \& \ a_j = b_j, \ j = 1..i-1 \\ a_i = b_i, i = 1..n, n \le m \end{cases}$

Если пара рюкзаков (A, B) упорядочена, то этот факт будем обозначать как A≤B.

Утверждение 2. Пусть для рюкзака A=(a_1,a_2, …, a_n) размерности n, все компоненты которого различны ($\forall i,j \ a_i \neq a_j, \ i \neq j$), множество $\Lambda = \{(B_k, C_k)\}$ образует множество пар различных совместимых в Z_p рюкзаков B_k и C_k таких, что $B_k \prec A$, $C_k \prec A$ и $B_k \le C_k$. Тогда

1) Рюкзак A инъективен $\Leftrightarrow \Lambda = \varnothing$;
2) Для рюкзака A уравнение (1) имеет решений не более чем $\prod_{i=1}^{|\Lambda|} \left\| (B_i, C_i) \right\|$.

Доказательство:

1) Следует непосредственно из Утверждения 1.
2) Пусть B=($\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}$) и C=($\overline{\overline{a_1}}, \overline{\overline{a_2}}, \ldots, \overline{\overline{a_n}}$) — два различных совместимых рюкзака, т.ч. $B \prec A$, $C \prec A$ и $B_k \le C_k$. Тогда существуют два различных ненулевых набора ($\overline{\delta_1}, \overline{\delta_2}, \ldots, \overline{\delta_n}$) и ($\overline{\sigma_1}, \overline{\sigma_2}, \ldots, \overline{\sigma_n}$) таких, что $\sum_{i=1}^{\bar{n}} \overline{\delta_i} \overline{a_i} = \sum_{j=1}^{\bar{\bar{n}}} \overline{\sigma_j} \overline{\overline{a_j}}$.

Найдется число *v*, т.ч. $\sum_{l=1}^{n}\sigma_l a_l = \sum_{i=1}^{n}\delta_i a_i + \gamma\sum_{j=1}^{\bar{n}}\overline{\delta}_j \overline{a}_j = v$.

И следовательно

$$\sum_{l=1}^{n}\sigma_l a_l = \sum_{i=1}^{n}\delta_i a_i + \alpha\sum_{j=1}^{\bar{n}}\overline{\delta}_j \overline{a}_j + \beta \sum_{k=1}^{\bar{\bar{n}}}\overline{\overline{\sigma}}_k \overline{\overline{a}}_k = v, \qquad \alpha+\beta=\gamma \qquad (7)$$

Из (7) следует, что количество различных решений уравнения (1) зависит от количества различных пар значений (α, β), удовлетворяющих (7). Количество вышеуказанных пар не превышает $\|(B, C)\|$.

Аналогичными рассуждениями можно показать, что для каждого элемента (B_k, C_k) множества Λ, количество различных решений не превышает $\|(B_k, C_k)\|$, а следовательно если все элементы множества Λ входят в (7), то общее количество решений не превышает

$$\prod_{i=1}^{|\Lambda|}\|(B_i, C_i)\| \ .$$

Перейдем к рассмотрению рюкзаков, в которых имеются повторяющиеся элементы. Очевидно, что в этом случае количество решений увеличится за счет взаимных перестановок коэффициентов повторяющихся элементов. Пусть рюкзак A имеет m повторяющихся компонентов a_{i1}, a_{i2}, …, a_{im}, тогда перестановка значений коэффициентов α_{i1}, α_{i2}, …, α_{im} уравнения (1) при данных компонентах определяет другое решение уравнения.

Определим верхнюю границу количества различных решений для уравнения (1) при условии, что все компоненты рюкзака A=(a_1,a_2, …, a_m) равны между собой. Количество значений целочисленной функции $f(\alpha_1,\alpha_2,...,\alpha_m) = \sum_{i=1}^{m}\alpha_i a = a\sum_{i=1}^{m}\alpha_i$,

($\alpha_i \in Z_p$, i=1..m) определяется только $\sum_{i=1}^{m}\alpha_i$, поэтому далее будем рассматривать

$$F(\alpha_1,\alpha_2,...,\alpha_m) = \sum_{i=1}^{m}\alpha_i \text{, } (\alpha_i \in Z_p, \text{ i=1..m}).$$

$F(\alpha_1, \alpha_2, …, \alpha_n)$ отображает все элементы множества n-ичных наборов P_p^m в значения из отрезка [0, m*(p-1)], причем данное отображение является сюръективным. Количество решений уравнения

$F(\alpha_1, \alpha_2, …, \alpha_n)$=S (8)

определяется разложением числа S на не более чем m сомножителей меньших p и их распределением по α_i.

Определим значение $C_p(m, S)$, которое равно количеству различных решений уравнения (8) от m переменных (α_1, α_2, …, α_m). Значение $C_p(m, S)$ определяется рекуррентным соотношением [5]:

$C_p(m, S)= C_p(m-1, S)+ C_p(m-1, S-1)+ C_p(m-1,S-2)+…+ C_p(m-1,S-(p-1))$ (9)

Из (9) следует, что $C_p(m, S_1) \le C_p(m, S_2)$ если $0 \le S_1 \le S_2 \le \left\lceil \frac{m*(p-1)}{2} \right\rceil$ или $\left\lceil \frac{m*(p-1)}{2} \right\rceil \le S_1 \le S_2 \le m*(p-1)$. Таким образом, $C_p(m, S)$ достигает своего максимума при $S=\left\lceil \frac{m*(p-1)}{2} \right\rceil$.

Обозначим через t_k количество слагаемых в разложении $\left\lceil \frac{m*(p-1)}{2} \right\rceil$ равных k. Тогда для каждого разложения количество различных вариантов определить значения

переменных (α_1, α_2, …, α_m) равно $\frac{m!}{t_0!t_1!t_2!\cdots t_{p-1}!}$. А общее количество решений уравнения (8) при $S=\left\lceil \frac{m*(p-1)}{2} \right\rceil$ задается формулой:

$$C_p(m,\left\lceil \frac{m*(p-1)}{2} \right\rceil) = \sum_{\substack{t_0+t_1+..+t_{p-1}=m \\ t_1+2t_2+..+(p-1)t_{p-1}=\left\lceil \frac{m(p-1)}{2} \right\rceil}} \frac{m!}{t_0!t_1!\cdots t_{p-1}!}. \quad (10)$$

Воспользовавшись формулой бинома Ньютона [5] можно получить другое представление $C_p(m,S)$:

$$C_p(m,S) = \sum_{k=0}^{[S/p]} (-1)^k C_m^k C_{m-1+S-kp}^{m-1} \quad (11)$$

Следовательно:

$$C_p(m,\left\lceil \frac{m*(p-1)}{2} \right\rceil) = \sum_{k=0}^{\left\lceil \frac{m*(p-1)}{2*p} \right\rceil} (-1)^k C_m^k C_{m-1+\left\lceil \frac{m*(p-1)}{2} \right\rceil -kp}^{m-1} \quad (12)$$

На основе вышесказанного определим

Утверждение 3. Пусть для рюкзака $A=(a_1,a_2, \ldots, a_n)$ размерности n, все компоненты которого различны, множество $\Lambda=\{(B_k,C_k)\}$ образует множество пар различных совместимых в Z_p рюкзаков B_k и C_k таких, что $B_k \prec A$, $C_k \prec A$ и $B_k \le C_k$. Кроме того, рюкзак A имеет r различных повторяющихся компонентов причем первый из них повторяется m_1 раз, второй — m_2, r-ый — m_r. Тогда

1) Рюкзак A инъективен $\Leftrightarrow \Lambda=\varnothing$ & r=0;
2) Для рюкзака A уравнение (1) имеет решений не более чем:

$$\prod_{i=1}^{|\Lambda|} \| (B_i,C_i) \| \prod_{j=1}^{r} \left(\sum_{k=0}^{\left\lceil \frac{m_j^*(p-1)}{2*p} \right\rceil} (-1)^k C_{m_j}^k C_{m_j-1+\left\lceil \frac{m_j^*(p-1)}{2} \right\rceil -kp}^{m_j-1} \right) \quad (13).$$

Причем верхняя граница достижима только в случае когда элементы Λ не пересекаются, а повторяющиеся компоненты A не входят ни в один из с подрюкзаков составляющих пары Λ.

В частности, если $\Lambda=\varnothing$, r=1, m_1=n и воспользоваться формулой (10), то (13) примет вид, описанный в [4].

Таким образом, в рамках работы определены критерий инъективности рюкзачных систем и верхняя граница количества решений обобщенной задачи о рюкзаке на заданном входе.

Библиографический список

1. Саломаа А, Криптография с открытым ключом, – М,: Мир, 1995. – 320с.
2. Осипян В.О. Разработка методов построения систем передачи и защиты информации. – Краснодар, 2003. – 180с.
3. Коблиц Н. Курс теории чисел и криптографии М: ТВП, 2001. – 260 с.
4. Ролдугин П.В. Верхняя оценка числа решений обобщенной задачи о рюкзаке. Тезисы VII Всероссийского симпозиума по прикладной и промышленной математике и XIII Всероссийской школы-коллоквиума по стохастическим методам.
5. Виленкин Н.Я. Популярная комбинаторика. – М,: Наука, 1975. – 208с.

Podkolzin V.V., Osipyan V.O.
THE UPPER LIMIT OF NUMBER OF SOLUTIONS OF GENERALIZATION KNAPSACK PROBLEM FOR KNOWN INPUTS

In present article questions of definition of the upper limit of number of decisions of inputs of knapsack systems of protection of the information are considered. In it criteria of injective knapsack systems, and also a method of calculation of a maximum quantity of decisions for the given input for not injective knapsack systems are determined

УДК 004.056.55

Т. А. Чалкин, К. М. Волощук
АЛГОРИТМ ПОСТРОЕНИЯ УЗЛОВ ЗАМЕН АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147-89

Рассматриваются основные требования к проектированию узлов замен (S-блоков) блочных шифров и разработанный авторами на их основе алгоритм построения узлов замен алгоритма шифрования ГОСТ 28147-89, обеспечивающий заданный уровень устойчивости шифра к линейному и дифференциальному криптоанализу.

Отечественный стандарт алгоритма блочного симметричного шифрования ГОСТ 28147-89 [1] согласно действующему в РФ законодательству является обязательным к применению при криптографической защите секретных сведений любой степени секретности и рекомендуемым к применению при защите конфиденциальных сведений, не составляющих государственную тайну (в частности, коммерческой тайны). При этом помимо стандартной для всех симметричных шифров ключевой информации – последовательности бит фиксированной длины, называемой ключом шифрования (для ГОСТ 28147-89 длина ключа составляет 256 бит), стандарт ГОСТ 28147-89 предусматривает использование в качестве элемента ключевой информации так называемой таблицы замен, представляющей собой матрицу чисел размерности 8×16, содержащей в своих ячейках числа от 0 до 15. Строки таблицы замен называются узлами замен. Назначение этой таблицы в целом аналогично назначению S-блоков алгоритма DES и подобных ему шифров, основанных на сети Фейстеля – перемешивание битов данных в ходе раунда шифрования путем замены отрезков блока данных по таблице, определяющей соответствие выходного значения входному.

Таблица замен является долговременным ключевым элементом, то есть действует в течение гораздо более длительного срока, чем ключ шифрования. Предполагается, что она является общей для всех узлов шифрования в рамках одной криптосистемы. Известно, что даже при нарушении секретности таблицы замен (если она становится известной криптоаналитику) стойкость шифра остается достаточно высокой и не снижается ниже определенного предела [2].

Согласно действующему законодательству, при шифровании секретных сведений используемые таблицы замен предоставляются субъекту, осуществляющему криптографическую защиту информации, уполномоченной организацией. При шифровании сведений, не составляющих государственную тайну, встает задача выбора ключевой информации, обеспечивающей криптографическую стойкость зашифрованных данных. Стандарт ГОСТ 28147-89 не определяет требований к выбору значений ключей и таблиц замен. И если для ключа шифрования существует ряд общепринятых критериев качества, общих для всех блочных симметричных шифров (равная вероятность появления 0 и 1 в последовательности бит и отсутствие статистических закономерностей в ней), то для таблиц замен эти критерии требуют адаптации для применения к построению таблиц

замен шифра ГОСТ 28147-89 в силу его определенных особенностей, о которых будет сказано ниже.

На сегодняшний день существует два основных, наиболее распространенных и хорошо разработанных метода криптоанализа – это линейный и дифференциальный криптоанализ [3]:

1) Линейный криптоанализ состоит в нахождении линейной функции зависимости выходных данных от входных, близкой по своим выходным значениям к нелинейной функции шифрования (эффективного статистического линейного аналога), и определении битов ключа с использованием этой функции.

2) Дифференциальный криптоанализ состоит в изучении процесса изменения различий для пары открытых текстов, имеющих определенные исходные различия в нескольких битах, в процессе прохождения через циклы шифрования с одним и тем же ключом.

Целью настоящей работы является разработка алгоритма выбора таблиц замен для блочного шифра ГОСТ 28147-89, обеспечивающего устойчивость шифрования к линейному и дифференциальному методам криптоанализа. На текущем этапе предполагается независимый выбор по определенным правилам восьми узлов замен, из которых строится таблица замен.

Рассмотрим подробнее отдельный раунд шифрования по ГОСТ 28147-89 (см. рис. 1).

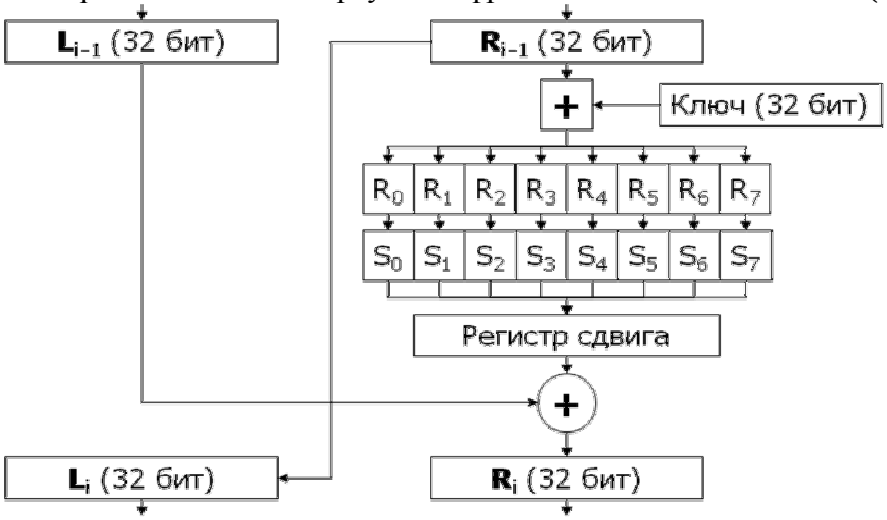

Рис. 1. Схема одного раунда блочного шифра ГОСТ 28147-89

Как и во всех шифрах, построенных на основе сети Фейстеля, на вход *i*-го раунда шифрования поступают два блока данных длиной 32 бит – левая и правая половины 64-битного блока L_{i-1} и R_{i-1} соответственно, получившиеся в результате выполнения предыдущего раунда. В ходе выполнения раунда сначала блок R_{i-1} суммируется по модулю 2^{32} с подключом раунда (отрезком ключа длиной 32 бит). Затем результат операции суммирования разбивается на 8 отрезков длиной 4 бит R_0, R_1, …, R_7, которые поступают на вход узлов замен S_0, S_1, …, S_7 используемой таблицы замен (напомним, что узлами замен мы называем строки таблицы замен). Каждый узел замен определяет правило, по которому входному 4-битовому вектору сопоставляется выходной 4-битовый вектор. Результаты замен всех восьми узлов объединяются в 32-битный блок, являющийся выходным значением таблицы замен. Этот блок затем подвергается операции побитового циклического сдвига влево (в сторону старших бит) на 11 бит. Наконец, результат сдвига побитово суммируется по модулю 2 с блоком L_{i-1} и передается на выход раунда шифрования в качестве правой половины выходного блока R_i. В качестве левой половины выходного блока L_i на выход подается значение R_{i-1}.

Рассмотрим теперь процесс замены бит при помощи таблицы замен. Каждый узел замен содержит 16 различных чисел от 0 до 15 в произвольном порядке. Выходное значение для каждого узла замен определяется следующим образом: входной 4-битный

вектор представляется в виде числа от 0 до 15, и из строки узла замен выбирается значение с порядковым номером, равным этому числу (нумерация ведется с нуля). Так как элементами узла замен являются числа от 0 до 15, то выход узла в двоичном виде также будет иметь длину 4 бита.

С точки зрения криптостойкости ключевыми требованиями к операциям преобразования бит в раунде шифрования являются нелинейность (невозможность подобрать линейную функцию, хорошо аппроксимирующую данное преобразование) и лавинный эффект (изменения в одном бите входных данных должны распространяться по всем битам выходных данных) – выполнение этих требований затрудняет проведение линейного и дифференциального криптоанализа шифра соответственно [4].

Если рассмотреть с этих позиций операции преобразования в раунде шифрования по ГОСТ 28147-89, то легко убедиться в том, что криптостойкость обеспечивают лишь операции сложения с ключом и выполнения замены бит по таблице, так как операции побитового сдвига и суммирования по модулю 2 являются линейными и не обладают лавинным эффектом. Из этого можно сделать вывод, что определяющим фактором надежности шифрования по ГОСТ 28147-89 является надлежащим образом выбранная ключевая информация (ключ и таблица замен). Очевидно, что в случае зашифрования данных с нулевым ключом и тривиальной таблицей замен, все узлы которой содержат числа от 0 до 15 в порядке возрастания, найти по известному шифртексту открытый текст достаточно просто при помощи как линейного, так и дифференциального криптоанализа.

Более того, как показано в [5], операция сложения данных с подключом не может обеспечить достаточного лавинного эффекта, поскольку при изменении одного бита на входе этой процедуры лишь один бит на выходе меняется с вероятностью 0,5, остальные биты меняются с вероятностью существенно меньшей. Это говорит о том, что для обеспечения криптостойкости шифрования недостаточно только обеспечения достаточного качества ключа – необходимо также использовать сильные таблицы замен с высокими показателями нелинейности и лавинного эффекта. Это показано в работе [6], где предлагается метод криптоанализа ГОСТ 28147-89, позволяющий с низкой вычислительной сложностью вскрыть шифр в случае использования слабых ключей и таблиц замен. Таким образом, задача выбора таблиц замен, устойчивых к линейному и дифференциальному криптоанализу, является одной из основных при реализации криптосистем на основе ГОСТ 28147-89.

Как было сказано выше, в настоящей работе предполагается формировать узлы замен независимо с их последующим объединением в таблицу замен. Поэтому в дальнейшем изложении будем рассматривать с точки зрения устойчивости к методам криптоанализа отдельные узлы замен.

Общие требования к узлам замен (S-блокам) блочных шифров повторяют требования к функции шифрования в целом – это нелинейность и лавинный эффект. В идеале любые изменения входных данных узла должны приводить к «случайным» изменениям выходных данных (если рассматривать узел замен как «черный ящик»).

Существует ряд общеизвестных критериев для проектирования устойчивых к дифференциальному криптоанализу узлов замен для любых блочных шифров [7]:

1) Строгий критерий лавинного эффекта (SAC – Strict Avalanche Criterion) – требует, чтобы для любых i и j при инвертировании входного бита i на входе узла замен выходной бит j изменялся с вероятностью 0,5.

2) Критерий независимости битов (BIC – Bit Independence Criterion) – требует, чтобы для любых значений i, j и k при инвертировании входного бита i на входе узла замен выходные биты j и k изменялись независимо (то есть вероятность одновременного изменения битов должна быть равна произведению вероятностей изменения отдельных бит). Считается, что одновременное выполнение SAC и BIC для всех узлов замен обеспечивает шифру достаточный уровень лавинного эффекта.

3) Критерий гарантированного лавинного эффекта (GAC – guaranteed avalanche criterion) порядка γ – выполняется, если при изменении одного бита на входе узла замен на выходе меняются как минимум γ выходных битов. Выполнение GAC порядка γ в диапазоне от 2 до 5 для узлов замен обеспечивает любому шифру очень высокий лавинный эффект вследствие распространения изменений в битах при прохождении данных по раундам шифрования в схеме Фейстеля.

Существуют следующие наиболее распространенные подходы к выбору узлов замен:

1) Случайный выбор. Элементы узлов замен выбираются с помощью генератора псевдослучайных чисел. Это наиболее простой способ, однако в случае небольшого размера узлов, как в алгоритме ГОСТ 28147-89 (4×4 бит), такой способ может привести к генерации таблицы замен с нежелательными с точки зрения стойкости шифрования характеристиками нелинейности и лавинного эффекта.

2) Случайный выбор с последующей проверкой. Элементы узлов замен выбираются случайным образом, но после этого полученные результаты проверяются на соответствие различным критериям с отсеиванием тех узлов, которые не выдержали такой проверки. Этот способ также прост и в то же время он устраняет указанный недостаток первого способа, однако в таком случае встает вопрос о том, по каким критериям проверять выбранные случайным образом узлы, так как не существует узлов замен, удовлетворяющих всем предъявляемым к ним критериям одновременно.

3) Выбор вручную. Элементы узлов замен выбираются вручную с использованием математических преобразований. Именно эта методика легла в основу разработки DES с его фиксированными S-блоками. Такой подход является наиболее сложным, так как требует разработки и теоретического обоснования методики выбора замен, что не всегда представляется возможным.

4) Математический подход. Элементы узлов замен генерируются при помощи определенного алгоритма, основанного на тех или иных математических принципах. Такой подход обеспечивает выбор узлов замен, гарантирующих заданный уровень надежности по отношению к методам линейного и дифференциального криптоанализа.

Мы предлагаем использовать для генерации узлов замен шифра ГОСТ 28147-89 аппарат булевых функций. В данном случае один узел замен представляется в виде набора из 16 различных 4-битовых строк как показано на рис. 2.

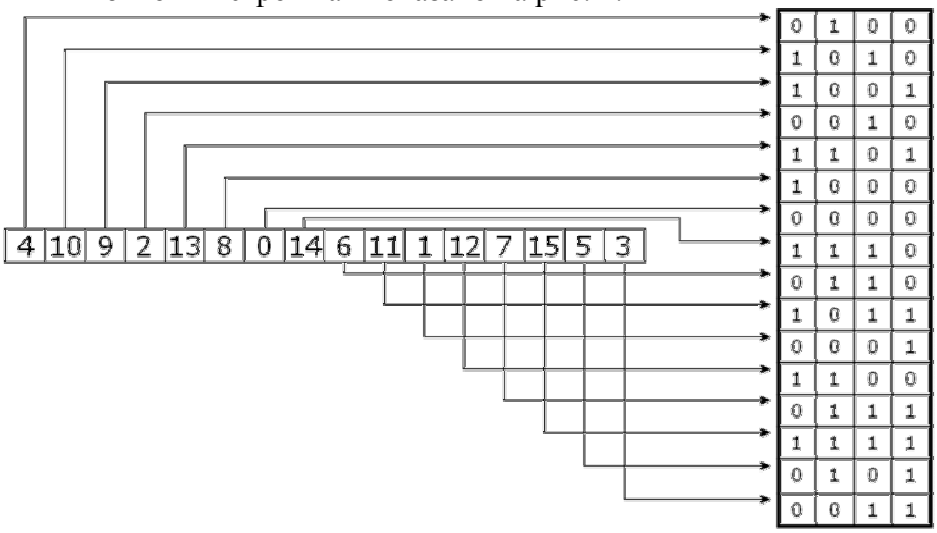

Рис. 2. Схема представления узла замен в виде битовой матрицы

В силу требования стандарта ГОСТ 28147-89 об отсутствии повторяющихся элементов в узле замен, битовая матрица узла не должна содержать повторяющихся строк. Столбцы такой битовой матрицы можно рассматривать как булевы функции от четырех переменных $f_i : \{0,1\}^4 \to \{0,1\}, i = 1,2,3,4$. Для них можно вычислить числовые

характеристики нелинейности и лавинного эффекта [4]. Так, нелинейность функции f определяется формулой

$$\mathrm{nl}(f) = \min_{l \in A_4} \mathrm{wt}(f \oplus l), \quad (1)$$

где wt – функция веса Хэмминга (число различных входных комбинаций бит, для которых функция дает на выходе 1), $\oplus$ – операция побитового сложения по модулю 2, A_4 – множество аффинных булевых функций от четырех переменных (линейных функций и их побитовых инверсий).

Нелинейность всего узла замен S тогда определяется формулой

$$\mathrm{nl}(S) = \min_{f \in C} \mathrm{nl}(f), \quad (2)$$

где C – множество всех линейных комбинаций столбцов битовой матрицы M (размерностью 16×4) узла замен S: $C = \left\{ Mc, c \in \{0,1\}^4 \right\}$ (вычисление произведения матрицы M на вектор c производится с использованием суммирования по модулю 2).

Таким образом, требование нелинейности узла замен можно сформулировать следующим образом: необходимо, чтобы все линейные комбинации столбцов битовой матрицы узла имели как можно большую нелинейность, определяемую формулой (1). Путем полного перебора всех булевых функций от четырех переменных было установлено, что нелинейность столбца может принимать только значения 0, 2 и 4.

Степень лавинного эффекта, обеспечиваемого узлом замен, характеризуется показателем динамического расстояния столбцов его битовой матрицы порядка j [4]:

$$\mathrm{DD}_j(f) = \max_{\substack{d \in \{0,1\}^4 \\ 1 \le \mathrm{wt}(d) \le j}} \frac{1}{2} \left| 2^{n-1} - \sum_{x=0}^{2^n-1} f(x) \oplus f(x \oplus d) \right|. \quad (3)$$

Динамическое расстояние всего узла замен S порядка (i, j) тогда определяется формулой

$$\mathrm{DD}_{i,j}(S) = \max_{\substack{c \in \{0,1\}^4 \\ 1 \le \mathrm{wt}(c) \le i}} \mathrm{DD}_j(Mc), \quad (4)$$

где M – битовая матрица узла замен S.

Так, критерий SAC для узла замен S выполняется тогда и только тогда, когда $\mathrm{DD}_{1,1}(S) = 0$, или, что то же самое, все столбцы битовой матрицы узла замен S имеют динамическое расстояние порядка 1, равное 0, а критерий BIC выполняется, когда $\mathrm{DD}_{2,1}(S) = 0$ – все линейные комбинации пар столбцов битовой матрицы узла замен S имеют динамическое расстояние порядка 1, равное 0.

Таким образом, требование обеспечения лавинного эффекта для узла замен можно сформулировать следующим образом: необходимо, чтобы все линейные комбинации столбцов битовой матрицы узла имели как можно меньшее динамическое расстояние как можно более высокого порядка, определяемое формулой (3).

Дополнительной характеристикой устойчивости узла замен к дифференциальному криптоанализу, определенной в [4], является так называемая XOR-таблица размерностью 15×16, элементы которой вычисляются по формуле

$$\mathrm{XOR}(S, \alpha, \beta) = \#\left\{ x \in \{0,1\}^4 : S(x) \oplus S(x \oplus \alpha) = \beta \right\}, \quad (5)$$

где $\alpha \in \{0,1\}^4 \setminus \{0\}$ (может быть представлено в виде числа от 1 до 15), $\beta \in \{0,1\}^4$ (может быть представлено в виде числа от 0 до 15), $S(x)$ – x-я строка битовой матрицы узла замен S, $\#X$ - мощность множества X.

XOR-значение узла замен S определяется по следующей формуле:

$$\mathrm{XOR}(S) = \max_{\alpha,\beta} \mathrm{XOR}(S, \alpha, \beta). \quad (6)$$

Таким образом, можно сформулировать свойства идеального узла замен ГОСТ 28147-89:

1) Все линейные комбинации столбцов битовой матрицы узла имеют нелинейность 4 (или, что то же самое, узел замен имеет нелинейность 4).

2) Все линейные комбинации столбцов битовой матрицы узла имеют динамическое расстояние порядка 4, равное 0 (или, что то же самое, узел замен имеет динамическое расстояние порядка (4, 4), равное 0).

3) Все элементы XOR-таблицы узла замен равны 0 или 2 (или, что то же самое, узел замен имеет XOR-значение 2).

Свойство 1 обеспечивает устойчивость шифрования к линейному криптоанализу, а свойства 2 и 3 – к дифференциальному криптоанализу. В ходе исследований выяснилось, что при построении узлов замен шифра ГОСТ 28147-89 невозможно добиться одновременно максимальных показателей нелинейности и динамического расстояния даже порядка 1. Это, в частности, является следствием того, что узел замен должен быть перестановкой чисел от 0 до 15, то есть в битовой матрице узла замен не должно быть одинаковых строк.

Нами предложен следующий алгоритм построения узлов замен, предполагающий формирование узла замен поэтапно – по столбцам:

Шаг 1. Выбирается минимально допустимый уровень нелинейности nl_{min} и максимальное допустимое динамическое расстояние порядка 1 DD_{max} линейных комбинаций столбцов битовой матрицы узла замен.

Шаг 2. Из всех возможных 2^{16} = 65536 булевых функций от четырех переменных выбирается подмножество, удовлетворяющее выбранным на шаге 1 критериям (методом полного перебора).

Шаг 3. Из построенного на шаге 2 подмножества выбирается функция-«кандидат» и помещается в первый столбец битовой матрицы узла замен.

Шаг 4. Из построенного на шаге 2 подмножества выбирается функция-«кандидат» и помещается во второй столбец битовой матрицы, после чего на соответствие критериям, выбранным на шаге 1, проверяется сумма по модулю 2 первого и второго столбцов. Если она им не удовлетворяет, то функция, помещенная во второй столбец, отбрасывается и выполняется возврат к шагу 3.

Шаг 5. Функции-«кандидаты» выбираются из построенного на шаге 2 подмножества, помещаются в столбцы битовой матрицы, следующие за последним заполненным столбцом, и выполняются проверки всех линейных комбинаций заполненных столбцов с участием столбца-«кандидата», до тех пор, пока заполненными не окажутся все 4 столбца матрицы

Шаг 6. Полученная в итоге битовая матрица узла замен дополнительно проверяется на соответствие GAC, а также дополнительно проверяется на устойчивость к дифференциальному криптоанализу путем построения XOR-таблицы узла замен. Если эти критерии выполняются – узел замен становится выходом алгоритма, если нет – последний столбец битовой матрицы отбрасывается и выполняется возврат к шагу 5 (продолжается процесс тестирования функций-«кандидатов»).

Данный алгоритм был программно реализован, протестирован и успешно использован для выбора подмножества таблиц замен при выбранных на шаге 1 параметрах nl_{min} = 4 и DD_{max} = 0. В результате работы алгоритма было получено множество из порядка 1032192 всех возможных узлов замен ГОСТ 28147-89, имеющих нелинейность 4 и удовлетворяющих SAC, BIC и более сильному аналогу BIC для всех выходных бит (при изменении любого входного бита все выходные биты узла меняются независимо). В то же время для всех узлов из этого множества XOR-значение равно 8, что является нежелательным показателем с точки зрения устойчивости к дифференциальному криптоанализу.

Также по всем приведенным выше критериям был проведен анализ тестовой таблицы замен из стандарта функции хеширования ГОСТ Р 34.10-94, который показал, что в них достигается баланс между степенью удовлетворения всем трем вышеприведенным критериям идеального узла замен.

Таким образом, следующей важнейшей задачей настоящей работы является разработка методики выбора оптимальных значений nl_{min} и DD_{max}, выбираемых на шаге 1, а также минимально допустимого порядка GAC и максимально допустимого XOR-значения узла замен при проверке готового узла замен на шаге 6 разработанного алгоритма.

Другим вариантом продолжения работы является построение интегральной оценки качества узла замен с точки зрения криптостойкости исходя из показателей нелинейности, динамического расстояния определенного порядка, элементов XOR-таблицы узла замен и минимального порядка γ, при котором узел замен удовлетворяет GAC. Тогда задача выбора узла замен сведется к задаче однокритериальной оптимизации на множестве всех возможных узлов, которая может быть решена как классическими методами, так и, например, с использованием генетических алгоритмов.

Также важными с нашей точки зрения вопросами для будущих исследований являются:

1) Разработка методики формирования таблицы замен из отдельных узлов, позволяющая оценить влияние отдельного узла замен таблицы на стойкость шифрования в целом, а также описать правила, по которым из узлов с различными характеристиками нелинейности и лавинного эффекта можно сформировать таблицу замен, оптимальную с точки зрения устойчивости к линейному и дифференциальному методам криптоанализа.

2) Исследование взаимного влияния качества ключа и таблицы замен на криптостойкость. В настоящее время практикуется независимый выбор ключа и таблицы замен. Однако, возможно, выбор ключа влияет на силу таблицы замен с точки зрения криптостойкости и наоборот, в частности, вполне возможно, что существуют ключи, сильные при одних выбранных узлах замен и слабые – при других. Открытые материалы исследований этого вопроса авторам неизвестны.

3) Практическое исследование криптостойкости алгоритма ГОСТ 28147-89 путем реализации атак методом линейного и дифференциального криптоанализа на упрощенную версию шифра, например, с меньшим числом раундов или меньшей длиной блока и/или ключа. В таком случае, возможно, удастся получить оценки вычислительной сложности вскрытия упрощенного шифра обоими методами криптоанализа, а затем экстраполировать их на полноценный ГОСТ 28147-89, исходя из предположения, что более высокая вычислительная сложность вскрытия упрощенного шифра влечет за собой пропорциональное увеличение сложности вскрытия полного алгоритма.

Таким образом, текущим результатом работы является разработанный и программно реализованный авторами алгоритм построения узлов замен блочного шифра ГОСТ 28147-89, который может применяться для выработки таблиц замен при шифровании несекретной информации ограниченного доступа. Результаты данной работы могут быть применены при проектировании и реализации криптографических систем защиты несекретной информации ограниченного доступа, передаваемой по открытым каналам.

Библиографический список

1. Государственный комитет СССР по стандартам. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147-89. М. : ИПК Издательство стандартов, 1996. – 29 с.

2. Винокуров, А. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы x86 [Электронный ресурс] / А. Винокуров. – Режим доступа: http://re-tech.narod.ru/inf/crypto/gost.htm.

3. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности / Л. К. Бабенко, Е. А. Ищукова. М. : Гелиос АРВ, 2006. – 376 с.

4. Mister S. Practical S-box design / S. Mister, C. Adams // Proceedings, Workshop in selected areas of cryptography / SAC'96, 1996. – 17 с.

5. Charnes C. Further comments on the soviet encryption algorithm / C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naini, Y. Zheng // University of Wollongong, NSW, Australia, 1994. – 10 с.

6. Ростовцев, А.Г. О стойкости ГОСТ 28147-89 / А.Г.Ростовцев, Е.Б. Маховенко, А.С. Филиппов, А.А. Чечулин // СПбГПУ, 2001. – 8 с.

7. Столлингс, В. Криптография и защита сетей: принципы и практика / В. Столлингс. М. : Издательский дом «Вильямс», 2001. – 672 с.

T. A. Chalkin, K. M. Voloshchuk

THE ALGORITHM OF CHANGE NODES CONSTRUCTION FOR GOST 28147-89 ENCRYPTION ALGORITHM

It is considered basic requirements for block ciphers change nodes (S-boxes) design and the algorithm of change nodes construction for GOST 28147-89 encryption algorithm developed by authors on basis of these requirements providing preselected level of cipher resistance to linear and differential cryptanalysis.

УДК 004.49.056.57

А. Н. Шниперов

СИНТЕЗ ХЭШ-ФУНКЦИЙ НА ОСНОВЕ БЛОЧНЫХ ПРЕОБРАЗОВАНИЙ С ИСПОЛЬЗОВАНИЕМ УПРАВЛЯЕМЫХ ОПЕРАЦИЙ[1]

В работе рассматриваются вопросы, связанные с проблематикой построения стойких хэш-функций на основе блочных криптографических преобразований. Управляемые операции представляют собой удобный примитив для конструирования, как блочных шифров, так и односторонних преобразований. Использование управляемых операций при построении основных криптографических процедур преобразования данных позволяет получить высокие показатели перемешивания и рассеивания, с сохранением высокой скорости преобразований.

Управляемые операции представляют собой удобный и перспективный примитив для конструирования блочных шифров [1, 2] и односторонних преобразований. Поскольку, как правило, блочные алгоритмы на базе управляемых операций используют простое расписание ключа, они могу быть использованы в качестве базового блочного преобразования при построении хэш-функций в соответствии с известными конструктивными схемами. В силу того, что простое расписание ключей предполагает использование частей ключа (в качестве подключей) как непосредственных операндов выполняемых при шифровании операций, то следует принять во внимание возможность существования слабых ключей. Наличие последних в криптосистемах не является критическим, если их доля в общем множестве возможных ключей мала, однако при построении хэш-функций на основе таких шифров могут появиться серьёзные уязвимости. Некоторые схемы, обеспечивающие построение стойких хэш-функций при использовании шифров, свободных от слабых ключей, могут оказаться нестойкими при

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 09 - 07 – 00108 - а).

использовании шифров, имеющих даже крайне малую долю слабых ключей. Наглядным примером может служить схема Рабина [3]. Этот пример демонстрирует, что наличие слабых ключей вносит определённые ограничения на используемые конструктивные схемы. Применение управляемых переключаемых операций при проектировании шифров обеспечивает устранение слабых ключей при использовании простого расписания ключа. Следует отметить, что использование простого расписания ключа позволяет получить высокие скорости вычисления хэш-функций и упрощение программной и аппаратной реализации, что представляет существенный практический интерес.

Более детально управляемые операции, как криптографический примитив, рассмотрены в [3, 4]. Управляемые операции, построенные на основе управляемых подстановочно-перестановочных сетей (УППС), вносят незначительное время задержки, поэтому они могут быть применены вместо операции поразрядного суммирования по модулю два в общих схемах построения хэш-функций. В этом случае комбинирование входных и выходных параметров блочного преобразования выполняемого на текущем раунде шифрования, осуществляется с одновременным внесением дополнительного вклада в лавинный эффект и нелинейность преобразования.

Таким образом, можно получить три механизма, приведённые на рис. 1, на базе которых могут быть построены различные варианты раундовых хэш-функций, включая и комбинированные.

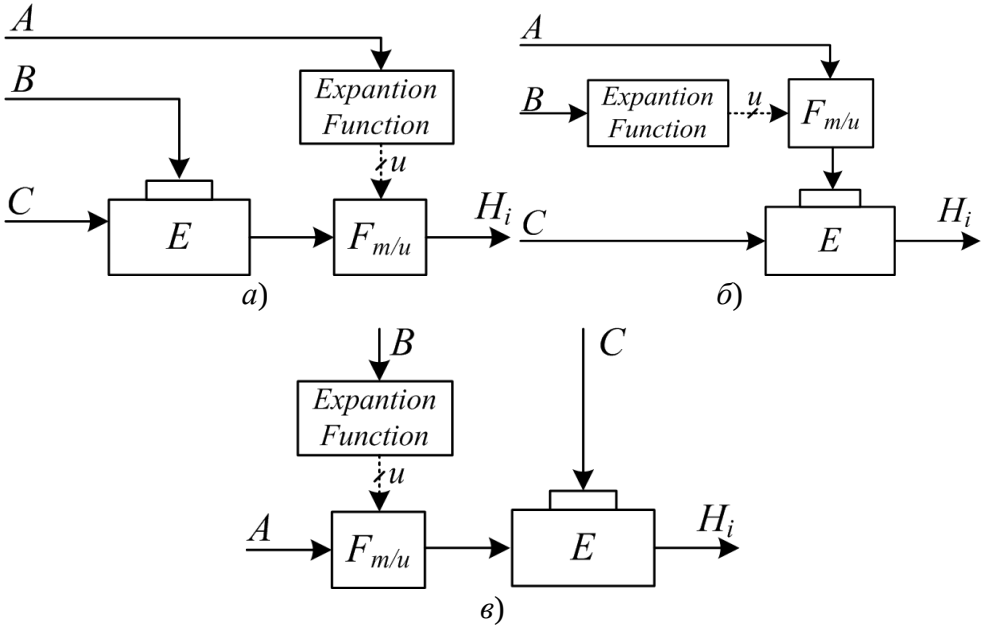

Рис. 1. Некоторые варианты обобщённой схемы построения раундовой хэш-функции с использованием управляемых операций: *а* – на выходе, *б* – на входе ключевого канала, *в* – входе функции шифрования (*E*).

Следует отметить, что вместо формальных A, B и C, указанных на рисунке, предполагается использование значений H_{i-1}, M_{i-1} или M_i. При использовании нескольких управляемых операций, обрамляющих блочное преобразование E, они могут относиться к различному типу. В общем случае использование управляемых операций позволяет существенно расширить множество вариантов построения хэш-функций для некоторого фиксированного блочного преобразования.

Таким образом, управляемые операции могут быть применены

- для синтеза базового (обратимого или одностороннего) блочного преобразования;
- в качестве вспомогательных обрамляющих операций, формирующих различные механизмы сцепления промежуточных значений раундовой хэш-функции.

Следует отметить, поскольку криптографические преобразования на основе управляемых обладают высокими показателями быстродействия [5], то при построении базового блочного преобразования может быть применимо одновременное преобразование значений M_i и H_{i-1} с помощью шифрующего преобразования, управляемого ключом K, в качестве которого используется одна из величин H_{i-1}, M_{i-1}, M_i или их комбинация. В таком случае блочное преобразование E имеет удвоенную разрядность входа ($2m$ бит). После его выполнения выходной блок делится на два равных по размеру подблока и они складываются, давая в результате текущее m-битовое значение раундовой хэш-функции (рис. 2) [6].

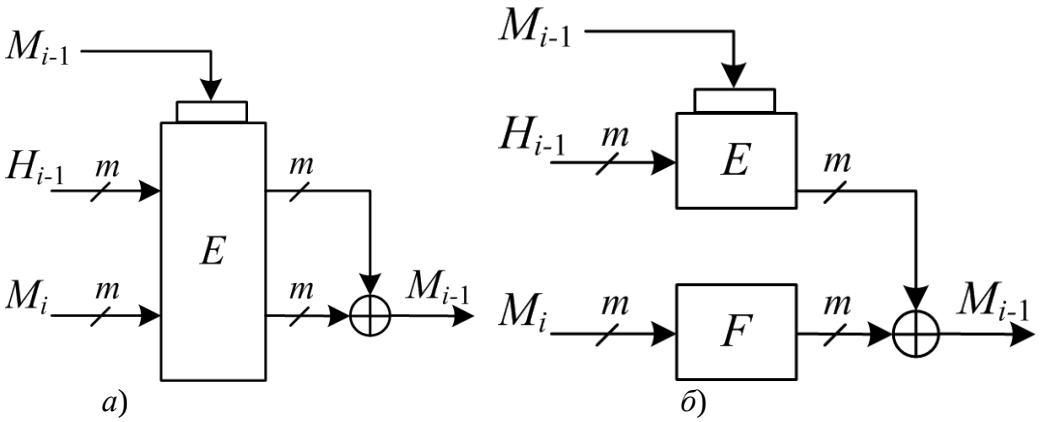

Рис. 2. Варианты схем с одновременным преобразованием значений M_i и H_{i-1}:
а – использование единого блочного преобразования удвоенной размерности,
б – использование двух различных блочных преобразований с
m-битовым входом

Для одновременного преобразования значений M_i и H_i можно применить два независимых преобразования, например, одно шифрующее, а другое – одностороннее, как например, показано на рис. 2,б. При выполнении большого числа параллельных операций лавинный эффект развивается в каждом из них, поэтому необходимых свойств преобразования можно достичь за меньшее время, что ведёт к повышению скорости вычисления хэш-функции. Это приводит к идее построения раундовой хэш-функции с предварительным расширением векторов M_i и H_i, за которым следует блочное преобразование с расширенным входом или несколько одновременно выполняемых блочных преобразований (в общем случае различного типа). Преобразованное расширенное значение суммируется таким образом, что получается m-битовое значение раундовой хэш-функции, в котором аккумулируются накопленные изменения [5].

Особенностью схем параллельного построения вычислений является использование двух значений раундовой функции H_i и J_i. Это даёт возможность задать хэш-функцию с разрядность $2m$ при использовании разбиения сообщения на m-битовые блоки данных. При этом стойкость к атакам на основе парадокса дней рождения будет определятся расширенным размером хэш-функции $H(M) = (H_n, J_n)$. Более того, хэш-функции с расширенным входом позволяют получить более высокую производительность при использовании многоядерных процессоров или аналогичным схемотехническом решении (в случае аппаратной реализации).

Выводы

Использование управляемых операций, зависящих от преобразуемых данных, в качестве криптографического примитива для создания однонаправленных хэш-функций, имеет большое теоретическое и практическое значение. Теоретическое значение состоит в возможности совершенствования известных труднообратимых преобразований с позиции повышения скорости вычисления хэш-функции, а также их криптографической стойкости, в том числе и коллизионной. Теоретически важным является то обстоятельство, что все

битовые манипуляции, осуществляемые блоками управляемых операций, а также схемы хэш-преобразований на их основе достаточно просто описываются аналитически. Таким образом, можно сравнительно несложно аналитически проследить влияние управляемых операционных блоков на коллизионную стойкость всей хэш-функции.

Практическое значение использованию управляемых преобразований состоит в возможности создания на её основе программного обеспечения, реализующего скоростные труднообратимые преобразования и хэш-функции, адаптированного к многоядерным и многопроцессорным вычислительным системам, которые обеспечивают (в современных условиях) вычислительную и коллизионную стойкость.

Библиографический список

1. Шниперов, А. Н. Симметричная криптосистема на основе управляемых и фиксированных операций / А. Н. Шниперов // Информационная безопасность: тезисы докладов Международной научно-практической конференции. – Таганрог, 2008. – С. 140–143.

2. Шниперов, А. Н. Проектирование программно-ориентированных симметричных криптосистем на основе управляемых операций / А. Н. Шниперов // Вестник Ассоциации выпускников КГТУ. Вып. – 16. – Красноярск: ИПК СФУ, 2008 – С. 106–125.

3. Молдовян, А. А. Криптография: скоростные шифры / А. А. Молдовян, Н. А. Молдовян, Н. Д. Гуц, Б. В. Изотов. – СПб.: БХВ-Петербург, 2002. – 496 с.

4. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов – М.: Кудиц-Образ, 2001. – 368 с.

5. Молдовян, Н. А. Криптография: от примитивов к синтезу алгоритмов / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев. – СПб.: БХВ-Петербург, 2004. – 448 с.

Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code (Second Edition) – New York.: John Wiley & Sons. 1996. – 758 p.

A. N. Shniperov

SYNTHESIS OF HASH FUNCTIONS ON THE BASIS OF BLOCK CONVERSIONS WITH CONTROLLED OPERATIONS USAGE

In article the questions linked to a problematics of construction of proof hash functions on the basis of block cryptography conversions are considered. Controlled operations represent a convenient primitive for designing, both block ciphers, and one-sided conversions. Usage of controlled operations at construction of the main cryptography procedures of a data conversion allows to receive high metrics of hashing and dispersion, with saving of a high speed of conversions.

Секция 2. «Оптимизация, моделирование и разработка систем защиты информации. Подготовка специалистов в области безопасности информационных технологий. Информационные технологии: теоретические и прикладные аспекты»

УДК 65.012.8

С. В. Белим, Н. Ф. Богаченко

ИЕРАРХИЧЕСКИЕ СТРУКТУРЫ РОЛЕВОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА

В работе представлена классификация структур, задающих иерархию ролей в ролевых моделях разграничения доступа, в зависимости от способа распределения полномочий. Рассматриваются преобразования графов, позволяющие произвольную ролевую политику безопасности свести к дереву ролей.

Политика безопасности компьютерных систем в общем случае задает правила разграничения доступа к информационным объектам. Одним из самых распространенных видов политики безопасности является ролевое разграничение доступа [1]. Ролевая политика безопасности, получившая широкое распространение в системах управления базами данных [1, 2], операционных системах [1, 2] и других вычислительных комплексах, допускает моделирование в рамках теории графов. Однако на сегодняшний день при проектировании подсистемы безопасности компьютерной системы иерархия ролей задается в виде ориентированного дерева [1]. Следует заметить, что математические модели, ориентированные на древовидную организацию иерархии ролей являются достаточно развитыми [1]. Целью данной работы ставилось развитие модели ролевой политики безопасности для произвольных графов. Основное внимание уделено отображению RP: $R \to 2^P$, которое каждой роли из множества R сопоставляет набор полномочий из множества прав на действия в системе P.

Иерархия ролей – это отношение частичного нестрогого порядка, заданное на множестве ролей R. При этом если $r_1 \geq r_2$, то r_1 находится в иерархии ролей «выше», чем r_2.

Исходя из определения, иерархию ролей можно представить в виде ориентированного графа $G = (R, E)$. Множество вершин R – это множество ролей. Дуга $(r_1,r_2) \in E$, если в иерархии ролей $r_1 \geq r_2$[2]. Принято считать, что иерархия ролей имеет вид ориентированного дерева [1, 2], в дальнейшем будем называть его *деревом ролей* и обозначать $T = (R, E)$.

При иерархическом отношении ролей важным является вопрос построения отображения RP, а именно, возможно ли назначение одного и того же набора полномочий двум ролям, находящимся в иерархическом подчинении. При этом применяется механизм наследования «снизу – вверх»: назначение полномочий начинается с листовых вершин – *листовое распределение прав доступа*.

Пусть иерархия ролей задана в виде ориентированного дерева $T = (R, E)$. Определим разбиение множества листовых вершин R_L дерева ролей T на k подмножеств:

$$R_L = \bigcup_{i=1}^{k} R_L^{(i)}, \forall i, j \in \{1,\ldots,k\} : R_L^{(i)} \cap R_L^{(j)} = \varnothing .$$

Данное разбиение задает отношение эквивалентности на множестве листовых вершин. Рассмотрим теперь *классовое распределение прав доступа*. Пусть две роли, относящиеся к одному классу эквивалентности листовых вершин, имеют одинаковые права:

---

[2] Если следовать системе обозначений графического языка моделирования UML (Unified Modeling Language), позволяющего представлять различные объектно-ориентированные проекты в единых обозначениях, то дугу надо ориентировать от младшей роли – к старшей. Чтобы сохранить терминологию теории графов, будем считать, что дуги направлены от старших ролей – к младшим. Очевидно, в обоих случаях отношение порядка, задающее иерархию ролей, и соответствующий неориентированный граф останутся неизменными.

$$\forall r_1, r_2 \in R_L : (r_1 \overset{R_L}{\approx} r_2) \Rightarrow (RP(r_1) = RP(r_2)).$$

По аналогии со случаем неклассового ролевого разграничения доступа [1] возможны три подхода к построению отображения *RP*:

1. *Строго таксономический классовый подход*. Разобьем множество *P* на *k* непересекающихся подмножеств по числу классов эквивалентности листовых вершин дерева ролей:

$$P = \bigcup_{i=1}^{k} P_i, \forall i, j \in \{1, \ldots, k\} : P_i \cap P_j = \varnothing .$$

Распределение прав, определяющееся отображением *RP*, зададим для листовых вершин в следующем виде:

$$\forall r \in R_L^{(i)} : RP(r) = P_i .$$

Для нелистовых вершин множество прав будем определять как объединение прав всех вершин, которые являются сыновьями данной вершины:

$$\forall r \notin R_L : RP(r) = \bigcup_{r' \in Ch(r)} RP(r') .$$

Здесь через $Ch(r)$ обозначено множество всех сыновей вершины r.

2. *Нетаксономический классовый подход*. Аналогично предыдущему случаю, распределение прав изначально производится только между листовыми вершинами, но множества прав различных классов эквивалентности листовых вершин могут пересекаться.

3. *Иерархический охватный классовый подход*. Распределение прав производится между классами эквивалентности листовых вершин и передается по иерархическим принципам. Но, кроме того, нелистовые вершины, унаследовавшие одинаковые наборы прав, могут одновременно получать дополнительные права.

За счет иерархической структуры, во всех трех случаях в итоговом наборе полномочий присутствуют все полномочия подчиненных ролей.

Легко показать, что каждый из трех листовых подходов распределения полномочий, определенных в [1], является частным случаем соответствующего классового подхода при условии: $|R_L^{(i)}| = 1$, где $\{R_L^{(i)}\}_{i=1}^{k}$ – начальное разбиение множества листовых вершин, другими словами, каждая листовая вершина образует отдельный класс разбиения.

Разбиение листовых вершин дерева ролей вместе с правилами построения отображения *RP* порождает разбиение всего множества ролей. Будем считать две роли *эквивалентными*, если они наделены одинаковыми правами:

$$\forall r_1, r_2 \in R : (RP(r_1) = RP(r_2)) \Rightarrow (r_1 \overset{RP}{\approx} r_2) .$$

Полученные классы эквивалентности ролей назовем *RP-классами*. Каждому узлу *r* дерева ролей припишем соответствующий данной роли набор полномочий $RP(r)$. Результирующее помеченное дерево ролей назовем *RP-деревом*. Таким образом, в *RP*-дереве в один *RP*-класс попадают вершины, наделенные одним и тем же набором полномочий.

Обозначим число *RP*-классов через *K*, а число классов эквивалентности листовых вершин через *k*. Очевидно, что в случае строгого таксономического классового подхода $K \geq k$. При двух других подходах возможен случай $K < k$ в тех ситуациях, когда несколько классов эквивалентности листовых вершин наделяются одним и тем же набором полномочий.

RP-дерево будем называть *вырожденным*, если на нем существует ровно один *RP*-класс, то есть $K = 1$. *RP*-дерево будем называть *оптимальным*, если количество заданных на нем *RP*-классов совпадает с количеством вершин: $K = |R|$.

Очевидно, что для оптимальности *RP*-дерева необходимо потребовать, чтобы в начальном разбиении множества листовых вершин каждый лист составлял отдельный класс. Далее рассмотрим необходимые и достаточные условия оптимальности.

Теорема 1. При строго таксономическом листовом подходе распределения прав *RP*-дерево является оптимальным тогда и только тогда, когда полустепень исхода (число исходящих дуг) каждой нелистовой вершины не меньше двух:

$$\forall r \notin R_L : d^-(r) \geq 2. \quad (1)$$

Доказательство. Пусть *RP*-дерево является оптимальным. Тогда

$$\forall r_1, r_2 \in R : (r_1 \neq r_2) \Rightarrow (RP(r_1) \neq RP(r_2)). \quad (2)$$

От противного. Пусть $\exists\ r_1 \notin R_L$: $d^-(r_1) < 2$, следовательно, $d^-(r_1) = 1$. Тогда вершина r_1 имеет ровно одного сына, обозначим его r_2. Согласно правилам строго таксономического листового подхода: $RP(r_1) = RP(r_2)$ – противоречие.

Пусть теперь выполнено неравенство (1). Рассмотрим две различные вершины $r_1, r_2 \in R$. Надо показать справедливость условия (2). Заметим, что требование (1) влечет выполнение следующего неравенства:

$$\forall r_1, r_2 \in R : (r_1 \neq r_2) \Rightarrow (R_L(r_1) \neq R_L(r_2)), \quad (3)$$

где $R_L(r_i)$ – потомки вершины r_i, являющиеся листовыми вершинами в случае, когда $r_i \notin R_L$, либо сама вершина r_i, если она листовая. Данное утверждение очевидным образом следует из ацикличности принятой иерархии ролей (T – дерево). Согласно введенной системе обозначений, при строго таксономическом листовом подходе:

$$\forall r \in R : RP(r) = \bigcup_{r' \in R_L(r)} RP(r') \quad (4)$$

и

$$\forall r', r'' \in R_L : (r' \neq r'') \Rightarrow (RP(r') \cap RP(r'') = \varnothing). \quad (5)$$

Из (3) и (5) следует:

$$\forall r_1, r_2 \in R : (r_1 \neq r_2) \Rightarrow \left(\bigcup_{r' \in R_L(r_1)} RP(r') \neq \bigcup_{r' \in R_L(r_2)} RP(r') \right). \quad (6)$$

Принимая во внимание равенство (4), получаем условие (2). Что и требовалось доказать.

Теорема 2. При нетаксономическом листовом подходе распределения прав, *RP*-дерево является оптимальным тогда и только тогда, когда полустепень исхода каждой нелистовой вершины не меньше двух (выполнено условие (1)) и разбиение множества прав P на подмножества P_i произведено таким образом, что

$$\forall j \in \{1, \ldots, k\} : P_j \not\subseteq \bigcup_{i=1, i \neq j}^{k} P_i. \quad (7)$$

Доказательство. Необходимость доказывается аналогично предыдущей теореме. При доказательстве достаточности условие (5) заменяется условием (7). Пусть $I_1, I_2 \subseteq \{1,\ldots,k\}$: $I_1 \neq I_2$, тогда $\exists\ j$: $(j \in I_1) \wedge (j \notin I_2)$. Согласно (7): $P_j \not\subseteq \bigcup_{i \in I_2} P_i$, следовательно $\bigcup_{i \in I_1} P_i \not\subseteq \bigcup_{i \in I_2} P_i$. В результате:

$$\forall I_1, I_2 \subseteq \{1, \ldots, k\} : (I_1 \neq I_2) \Rightarrow \left(\bigcup_{i \in I_1} P_i \neq \bigcup_{i \in I_2} P_i \right). \quad (8)$$

Тогда, принимая во внимание неравенство (3) и то, что $\forall\ r_i \in R_L$: $RP(r_i) = P_i$, получаем (6) и, как следствие, (2). Что и требовалось доказать.

Отметим, что при иерархическом охватном листовом подходе оптимальным может быть *RP*-дерево произвольной структуры (например, ориентированная цепь) за счет того, что нелистовые вершины не только наследуют права, но и получают их непосредственно.

В дальнейшем, выбранный подход к построению отображения *RP* будем указывать в названии *RP*-дерева. Пусть T – *RP*-дерево. *RP-характеристикой* T называется спецификация, указывающая какой именно подход был применен при построении отображения *RP*. Дерево T называется *таксономическим* (или *нетаксономическим*, или *охватным*), если при распределении прав был использован строго таксономический (или нетаксономический, или иерархический охватный) подход. Если важно подчеркнуть, что было использовано листовое (классовое) распределение полномочий, то T – *листовое* (*классовое*) дерево.

Расширение RP-дерева T – это процесс построения *RP*-дерева T' такого, что T является подграфом T' и $\forall\ r \in R_T : RP_T(r) = RP_{T'}(r)$ – множество *RP*-классов T является подмножеством множества *RP*-классов T'.

Теорема 3. Произвольное *RP*-дерево может быть расширено до таксономического (в общем случае классового) *RP*-дерева.

Доказательство. Пусть T – произвольное *RP*-дерево. Построим искомое *RP*-дерево T'. Все вершины, дуги и полномочия дерева T перенесем в дерево T'. Тем самым T' – расширение дерева T.

Пусть каждой листовой вершине r_i сопоставлен набор полномочий $P_i = \{p_{i1}, \ldots, p_{im_i}\}$. Если $|P_i| = m_i > 1$, то в дереве T' к этой вершине присоединим m_i листовых вершин, каждая из которых будет наделена правом p_{ij} ($j \in \{1, \ldots, m_i\}$). Двигаясь по дереву T' от листьев к корню, каждую нелистовую вершину r пополним сыновьями-листьями по числу полномочий из набора $RP(r)$ дерева T, которые не были унаследованы (каждой новой вершине припишем соответствующее право). В результате, в дереве T' каждая нелистовая вершина не получает ни одного полномочия непосредственно, а лишь наследует их от сыновей:

$$\forall r \notin R_L : RP(r) = \bigcup_{r' \in Ch(r)} RP(r').$$

Каждой листовой вершине дерева T' приписано одно единственное полномочие. Объединяя листовые вершины с одним и тем же значением $RP(r) = \{p_i\}$ в один класс разбиения листовых вершин $R_L^{(i)}$, получаем:

$$\forall r \in R_L^{(i)} : RP(r) = \{p_i\} = P_i, \forall i, j\ (i \neq j) : P_i \cap P_j = \varnothing.$$

Итак, отображение *RP* удовлетворяет всем требованиям строго таксономического классового подхода, следовательно, T' – таксономическое *RP*-дерево. Что и требовалось доказать.

Расширяя *RP*-дерево, мы, тем самым, строим новую ролевую политику, наследующую все роли и их иерархию из исходной модели.

Одним из преимуществ классового распределения полномочий является возможность расширения нетаксономических или охватных *RP*-деревьев до строго таксономических классовых, то есть возможна смена произвольной *RP*-характеристики дерева на таксономическую. Но, к сожалению, при таком преобразовании, как правило, увеличивается количество ролей (и *RP*-классов) в системе.

В противовес расширению *RP*-дерева можно рассматривать в некотором смысле обратную операцию. Если в *RP*-дереве найдется хотя бы один *RP*-класс, содержащий несколько ролей, то дерево не *оптимально*, а это свидетельствует о наличии в политике безопасности «дублирующих» ролей. Естественно попытаться преобразовать иерархию ролей так, чтобы результирующее *RP*-дерево стало оптимальным и при этом не изменилось множество *RP*-классов системы.

Два *RP*-дерева T и T' *эквивалентны*, если множества их *RP*-классов совпадают (совпадают различные наборы полномочий, встречающиеся в структуре).

Оптимизация *RP*-дерева *T* – это процесс построения *RP*-дерева *T'* такого, что *T'* эквивалентно *T* и *T'* – оптимальное *RP*-дерево. Заметим, что *RP*-дерево, полученное в результате оптимизации, будет листовым в силу оптимальности.

Попытаемся ответить на следующие вопросы. Любое ли *RP*-дерево поддается оптимизации? Как при этом ведет себя *RP*-характеристика дерева? Если *RP*-дерево является листовым и вершины в пределах одного *RP*-класса не связаны дугами (иначе достаточно произвести попарное *стягивание* таких вершин, как эта операция понимается в теории графов [2]), то добиться оптимальности в ряде случаев можно за счет перестройки древовидной структуры и изменения *RP*-характеристики на охватную. Этот подход не столь интересен, так как, исходя из практических приложений, желательно получить эквивалентное оптимальное таксономическое *RP*-дерево.

Получение эквивалентной оптимальной структуры с той же *RP*-характеристикой представляется возможным за счет отказа от древовидности и построения эквивалентного ориентированного графа, задающего иерархию ролей.

Теорема 4. Ориентированный граф задает иерархию ролей (является орграфом ролей) тогда и только тогда, когда в нем отсутствуют ориентированные циклы.

Доказательство. Отсутствие ориентированных циклов необходимо и достаточно для существования отношения частичного порядка, а именно свойств транзитивности и антисимметричности. Что и требовалось доказать.

Заметим, что в орграфе без ориентированных циклов найдется как минимум один сток (вершина с нулевой полустепенью исхода: $d^-(t) = 0$), и как минимум один источник (вершина с нулевой полустепенью захода: $d^+(s) = 0$). Далее будем рассматривать ориентированные графы с одним источником.

Распределение прав по произвольному орграфу ролей, также как и по дереву ролей, может проводится одним из трех способов. При этом построение отображения *RP* начинается либо со стоков (листовое распределение) либо с классов эквивалентности, на которые разбиты стоки (классовое распределение).

Определения оптимальности, расширяемости, эквивалентности и оптимизации очевидным образом переносятся на случай *RP*-орграфа (помеченного орграфа ролей).

Теорема 5. Произвольное *RP*-дерево может быть оптимизировано до *RP*-орграфа.

Доказательство. В *RP*-дереве достаточно *склеить* вершины, соответствующие эквивалентным ролям, если они не соединены дугами, либо попарно *стянуть*, если такие дуги имеются (операции склейки и стягивания вершин понимаются в соответствии с определениями теории графов [2]). В результате, множество *RP*-классов останется прежним, но орграф будет оптимальным. Что и требовалось доказать.

Следствие 5.1. Из алгоритма построения эквивалентного оптимального *RP*-орграфа *G* непосредственно следует ряд свойств этой структуры:

1. *G* имеет один источник *s*.
2. Число стоков t_i в *G* совпадает с числом классов разбиения $R_L^{(i)}$ листовых вершин исходного *RP*-дерева *T*.
3. Если исходное *RP*-дерево *T* являлось оптимальным, то *G* = *T*.
4. *G* – листовой *RP*-орграф.

Следствие 5.2. Если исходное *RP*-дерево таксономическое, то построенный по предложенному алгоритму эквивалентный оптимальный *RP*-орграф также таксономический.

Доказательство. Стягивание двух вершин, соответствующих эквивалентным ролям, по дуге их соединяющей не изменяет *RP*-характеристику. При склейке вершин из одного *RP*-

класса, результирующий набор сыновей будет распределен по тем же *RP*-классам, что и в исходном *RP*-дереве – тем самым сохранится таксономичность структуры. Что и требовалось доказать.

Следствие 5.3. Если исходное *RP*-дерево нетаксономическое, то построенный по предложенному алгоритму эквивалентный оптимальный *RP*-орграф также нетаксономический.

Следствие 5.4. Если исходное *RP*-дерево охватное, то построенный по предложенному алгоритму эквивалентный оптимальный *RP*-орграф может оказаться охватным, нетаксономическим или таксономическим.

Обобщая вышесказанное, получаем следующую возможную последовательность построения ролевой политики безопасности:

1. Исходя из содержательной постановки задачи, построить *RP*-дерево T_1 (листовое или классовое).
2. Расширить T_1 до таксономического (в общем случае классового) *RP*-дерева T_2 (см. теорему 3).
3. Преобразовать T_2 в эквивалентный оптимальный таксономический *RP*-орграф T_3 (см. теорему 5).

Таким образом, любую ролевую модель распределения полномочий можно расширить до политики, в которой иерархия ролей задана орграфом без ориентированных циклов, роли распределены в соответствии со строго таксономическим листовым подходом и *RP*-структура оптимальна.

Оказывается, предложенный в теореме 5 алгоритм обратим: по произвольному *RP*-орграфу можно построить эквивалентное (но не обязательно оптимальное) *RP*-дерево.

Теорема 6. Для произвольного *RP*-орграфа существует эквивалентное ему *RP*-дерево.

Доказательство. Пусть дан *RP*-орграф *G*. Будем строить эквивалентную ему *RP*-структуру *T*. На первом шаге каждому стоку t_i орграфа *G* сопоставляем $d^+(t_i)$ листьев в *T* («оригинал» и $(d^+(t_i) - 1)$ «дублей»). Эта операция называется *расщеплением* вершины (если полустепень захода равна единице, то имеется только «оригинал»).

Далее, двигаясь по орграфу *G* от нижних ярусов к источнику, последовательно расщепляем все вершины. «Оригинал» и «дубли» наделяем теми же правами, что были у вершины их образующей. К «оригиналу» присоединяем уже существующие вершины структуры *T* из тех, что не имеют входящих дуг, восстанавливая сыновей расщепляемой вершины орграфа *G* (такие вершины в *T* всегда найдутся по построению). К каждому «дублю» добавляем вершины и дуги так, чтобы подграф, порожденный «дублем», представлял собой копию поддерева, порожденного «оригиналом».

Очевидно, что построенная таким образом иерархия *T* является *RP*-деревом и задает те же *RP*-классы, что и исходный *RP*-орграф *G*, то есть ему эквивалентна. Что и требовалось доказать.

Следствие 6.1. Количество вершин *RP*-дерева *T*, эквивалентного *RP*-орграфу *G* и построенного по алгоритму, описанному в теореме, равно

$$\sum_{r \in R_G} \left(1 + (d^+(r) - 1) \mid R_{T(r)} \mid\right),$$

где R_G – множество вершин орграфа *G*, $R_{T(r)}$ – множество вершин поддерева, порожденного той вершиной дерева *T*, которая соответствует вершине *r* орграфа *G*.

Заметим, что теорема 6 дает возможность свести исследование ролевой политики безопасности на произвольном *RP*-орграфе к изучению эквивалентного *RP*-дерева.

Таким, образом, теоремы 5 и 6 позволяют выполнять различные эквивалентные преобразования иерархии ролей в зависимости от того, какой признак более значим: древовидность или оптимальность.

Библиографический список

1. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин. Екатеринбург: Изд-во Урал. ун-та, 2003. – 328 с.

2. Девянин П.Н. Модели безопасности компьютерных систем / П.Н. Девянин. М.: Издательский центр «Академия», 2005. – 144 с.

3. Новиков Ф.А. Дискретная математика для программистов / Ф.А. Новиков. СПб.: Питер, 2001. – 304 с.

S. V. Belim, N. F. Bogachenko

HIERARCHICAL STRUCTURES OF THE ROLE-BASED ACCESS CONTROL MODELS

The classification of the structures setting hierarchy of roles in the role-based access control models, depending on a way of distribution of powers is considered in this article. The graphs transformations allowing any role-based policy to reduce to a roles tree are considered in this article.

УДК 681.142.2

С.С.Валеев, М.Ю. Дьяконов

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ МИКРОЯДЕРНОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В статье предложен подход к определению состояния процессов в микроядерной операционной системе по критерию аномального поведения. Для классификации состояния процессов предлагается использование самоорганизующихся карт Кохонена. Исследуемый прототип классификации состояния процессов основан на микроядерной операционной системе с открытым исходным кодом Minix 3.

Введение

Множество современных средств защиты (антивирусы, межсетевые экраны, системы обнаружения/предотвращения вторжений) используют сигнатурные методы обнаружения вредоносного кода и/или различные эвристики [1-3]. Несмотря на их огромную значимость для задачи эффективной защиты информации, предлагается технология, основанная не на сигнатурных методах обнаружения, а на поведенческом анализе ПО.

Мониторинг поведения процессов

При использовании динамического или статического анализа программного кода возникают два случая, приводящие к затруднениям при мониторинге ПО во время исполнения, а также приводящие к ошибкам классификации:

1) При использовании динамического анализа в режиме обучения возникает сложность построения всех возможных путей исполнения кода ПО. В связи с этим полученное множество является неполным и в режиме мониторинга приводит к значительным ошибкам первого и второго рода.

2) При использовании статического анализа возникают две основные проблемы: недоступность исходного кода ПО, а также обфускационные методы, используемые разработчиками ПО для сокрытия алгоритмов работы.

Первую проблему обычно решают с использованием дизассемблирования кода. Вторая проблема несколько сложнее и решается с использованием интерактивных средств отладки. В этих двух случаях задействован человек-эксперт, причем достаточно высокой квалификации. При этом часть анализа производится вручную даже для сравнительно небольшого объема кода.

Как известно из [4] основной единицей в операционной системе (ОС) является процесс. Процесс для ОС представляется в общем случае как совокупность нескольких составляющих: 1) представление процесса в ОС в виде структур данных, содержащих необходимую информацию для управления потоком исполнения; 2) процесс представлен как бинарный образ программы, располагающийся в оперативной памяти компьютера.

Тем самым, возможен сбор статистики исполнения процесса, которая будет содержать информацию о возможных разрешенных потоках кода ПО, возникающих во время исполнения. Наибольший интерес представляют функции кода, в которых происходит вызов системных служб. При совершении системного вызова формируется контекст вызова C_{ij}, который представляет собой адреса возврата в вызывающие функции. С точки зрения поведения программы интерес представляют переходы, совершаемые при вызове различных служб ядра ОС, т.е. два последовательно совершаемых системных вызова. Ядро ОС управляет системными вызовами и через них предоставляет доступ к различным ресурсам, тем самым возможно осуществлять контроль за поведением программы, анализируя системные вызовы.

В качестве примера можно привести следующую цепочку системных вызовов:

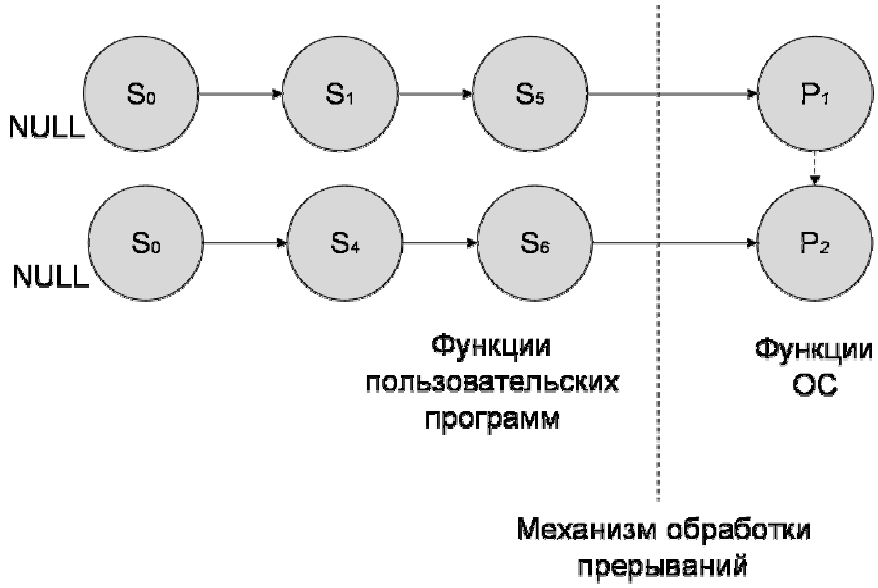

Рис. 1. Цепочка системных вызовов

Таким образом, при последовательном совершении системных вызовов P_1 и P_2, они будут характеризоваться совокупностью контекстов: P_1C_5, C_{51}, C_{10}, C_{04}, C_{46}, C_6P_2.

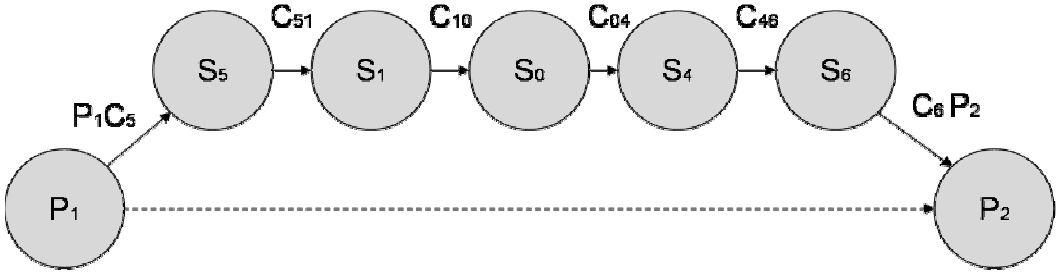

Рис. 2. Совокупность контекстов

В итоге, для двух данных системных вызовов можно получить характерные паттерны поведения. Для примера: на рисунке 2 паттерном будет являться следующее упорядоченное множество:

$$T^{i}_{p1p2} = \langle P_1 C_5, C_{51}, C_{10}, C_{04}, C_{46}, C_6 P_2 \rangle,$$

где $i = 1 \div n$, n - число паттернов при последовательном совершении системных вызовов P_1, а затем P_2.

Совокупность всех возможных паттернов позволяет классифицировать поведение программы на нормальное (обычное) и аномальное – в случае воздействия вредоносного кода на ОС. В качестве классификатора можно использовать самоорганизующиеся карты Кохонена.

Сбор статистики поведения процессов и классификация состояний на основе самоорганизующихся карт Кохонена

Система сбора статистики и классификации состояний представляет собой специально разработанный модуль, встраиваемый в микроядро ОС (прототип модуля встраивается в ОС Minix3). Структура модуля может быть представлена на следующем рисунке:

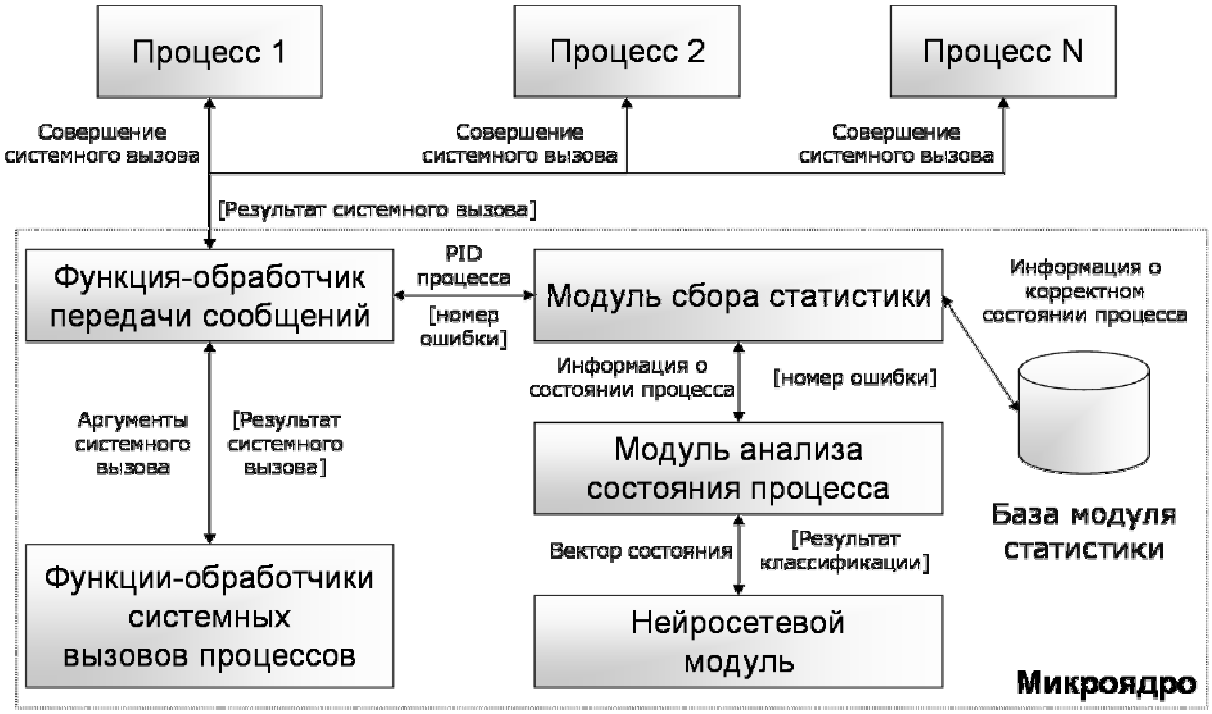

Рис. 3. Структура модуля сбора статистики и классификации

Модуль осуществляет сбор статистики совершения системных вызовов процессами с соответствующими им контекстами. Далее в режиме off-line проводится обучение сети. Моделирование самоорганизующихся карт проводилось в пакете Matlab. Исходные данные для обучения самоорганизующейся сети Кохонена представлены в таблице:

Таблица 1. Исходные данные для обучения сети

Количество кластеров	**Количество входных векторов**	**Размерность вектора**	**Функция окрестности**	**Алгоритм обучения**
4	211	14	Гауссова	Пакетный с указанием меток

Результат моделирования для наглядности приведен в графическом виде на следующем рисунке:

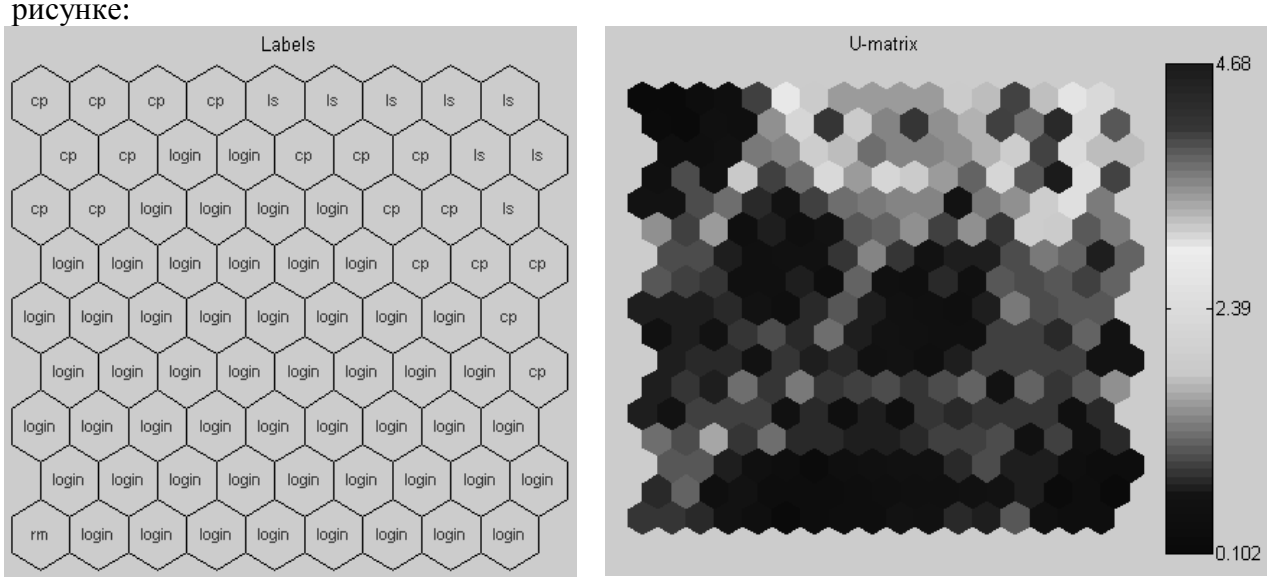

Рис. 4. Результаты обучения сети Кохонена 9x9

Таким образом, результаты можно представить следующей таблицей:

Таблица 2. Итоговые результаты классификации

Наименование процесса	**Количество входных векторов**	**Сеть 9x9**	
		Верно классифицированные, %	**Ошибочно классифицированные, %**
cp	44	92,68	7,32
rm	9	78	22
ls	18	89	11
login	139	100	0
Наименование процесса	**Количество входных векторов**	**Сеть 10x10**	
		Верно классифицированные, %	**Ошибочно классифицированные, %**
cp	44	90,9	9,1
rm	9	88	12
ls	18	94,5	5,5
login	139	100	0
Наименование процесса	**Количество входных векторов**	**Сеть 11x11**	
		Верно классифицированные, %	**Ошибочно классифицированные, %**
cp	44	93,2	6,8
rm	9	88	12
ls	18	94,5	5,5
login	139	100	0

Из таблицы можно сделать вывод, что при достаточном объеме статистики поведения процессов (login, ls), сеть способна различать входные образы процессов.

Выводы

В результате проведения исследований был разработан исследовательский прототип в ОС Minix 3, позволяющий эффективно осуществлять сбор статистики поведения процессов на уровне ядра ОС. Проведено обучение сети на примере поведения нескольких процессов. Результат классификации сетью показал достаточно эффективную работоспособность данного метода.

Основными преимуществами подхода являются: отсутствие необходимости обновления сигнатурных баз; отсутствие каких-либо эмпирических правил для обнаружения аномального поведения; высокая эффективность защиты, связанная со встраиванием системы в ядро ОС.

Основными недостатками на данном этапе являются: для обучения сети требуется достаточно большой объем статистики поведения процессов; обучение нейросетевого классификатора необходимо производить в режиме off-line.

Библиографический список

1. D. Anderson, T. Lunt, H. Javitz, A. Tamaru, A. Valdes, “Detecting unusual program behavior using statistical component of next-generation intrusion detection expert system (NIDES)”, SRI-CSL-95-06, May 1995.

2. S. Han, S. Cho, “Rule-based integration of multiple measure-models for effective intrusion detection”, IEEE International Conference on Systems, Man and Cybernatics, vol. 1, pp. 120-135, 2003.

3. D. Gao, M. Reiter, D. Song, “Gray-box extraction of execution graphs for anomaly detection”, ACM Conference on Computer and Communications Security 2004, pp. 318-329.

4. Таненбаум Э., Вудхалл А. Операционные системы. Разработка и реализация (+CD). Классика CS. 3-е изд. – СПб.: Питер, 2007. – 704 с: ил.

S.S. Valeev, M.Y. Dyakonov

SECURITY ENHANCED OF MICROKERNEL OPERATING SYSTEMS WITH APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS

The approach of detection state of processes state in microkernel operating system by criterion of anomaly of their behaviour is considered. The Kohonen self-organizing maps is used to classified a processes state. The research prototype of state classification system is developed on the basis of microkernel operating system with open source codes Minix 3.

УДК 004.7.056.52

Е.В. Горковенко

РАЗРАБОТКА МОДУЛЬНОЙ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ ОБЩЕГО И ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ

Рассматривается технология защиты данных различной степени конфиденциальности, реализованная в виде взаимосвязанных модулей-подсистем на базе современных методов и механизмов защиты данных.

Известно, что требуемый уровень информационной безопасности достигается только при решении комплекса разноплановых задач защиты информационных ресурсов. Существующие в настоящее время механизмы защиты направлены на реализацию отдельных аспектов обеспечения информационной безопасности (ИБ), что не обеспечивает комплексного решения задач анализа и синтеза систем управления защитой и получения оптимальных проектных решений по созданию защищенных информационных систем и баз данных. Наряду с совершенствованием популярных

средств защиты технической составляющей (ПЭВМ, системы передачи данных и т.д.) информационного взаимодействия, все больше внимания уделяется вопросам защиты самих информационных технологий, в самом широком смысле [1,2]. Основным требованием к технологии защиты является сохранение преемственности и последовательности операций по созданию интегрированной системы защиты при формировании и использовании информационных продуктов, организованных в виде тематических БД. Согласно понятиям и определениям [3,4], ведем понятие информационной технологии защиты.

Определение 1. Под информационной технологией защиты будем понимать процесс, состоящий из последовательности операций по защищенной обработке, хранению и представлению информационных продуктов (баз данных, электронных документов, сообщений и пр.) и способов осуществления таких процессов и методов, ориентированных на современные достижения в области информационной безопасности.

Возможны различные способы формирования технологии процесса защиты и соответственно различные описания самой технологии: начиная с методологии защиты, определяющей методы и механизмы защиты (как защищать?), и заканчивая подходами, базирующимися на выделении и обосновании различных типов объектов защиты (что защищать?). Предлагаемая информационная технология защиты поэтапно реализует процесс защиты данных в виде взаимосвязанных модулей-подсистем на базе современных методов и механизмов защиты, начиная с проектирования защищенных структур баз данных (БД) различных информационных продуктов и заканчивая информационным обслуживанием разнородных пользователей. В большинстве случаев, в БД хранится разнообразная информация не только по форме представления, но и по уровню конфиденциальности. Анализ потенциальных угроз информационной безопасности корпоративным информационным ресурсам общего и ограниченного пользования показал, что для организации системы информационной защиты с учетом требований при работе с документами ограниченного пользования в Республике Казахстан возможна разработка информационной технологии, которая обеспечит многоуровневый контроль доступа к информации, а также оптимальное проектирование структур БД и криптографическую защиту в соответствии с уровнем конфиденциальности.

Определение 2. Многоуровневая защита определяется как свойство самой информационной системы хранить и обрабатывать данные различного уровня и категорий пользования при наличии персонала с различными категориями допуска таким образом, чтобы исключить доступ к информации или ее модификацию лицами, чей допуск не отвечает уровню секретности информации, и разрешить выполнение только разрешенных операций.

Объектом исследования является информация различной степени секретности, хранимая в БД и передаваемая по открытым каналам связи. Предлагаемая технология защиты направлена на решение задачи сохранения *конфиденциальности* для информации ограниченного пользования и задачи поддержания *целостности* для общедоступной информации.

Разработаны модели, методы и инструментальные средства, реализующие предлагаемую технологию защиты (рис.1) информационных ресурсов общего и ограниченного пользования в базах данных однородных тематических направлений (ТБД). Взаимосвязь модулей достигается через взаимное использование результатов решения задач каждого технологического этапа по обеспечению информационной безопасности, которые структурированы и организованы в виде базы метаданных спецификаций защиты (БмДСЗ); базы данных многоуровневой защиты (БДМЗ); базы данных криптографических преобразований (БДКП); базы метаданных предметной области (БмДПрО).

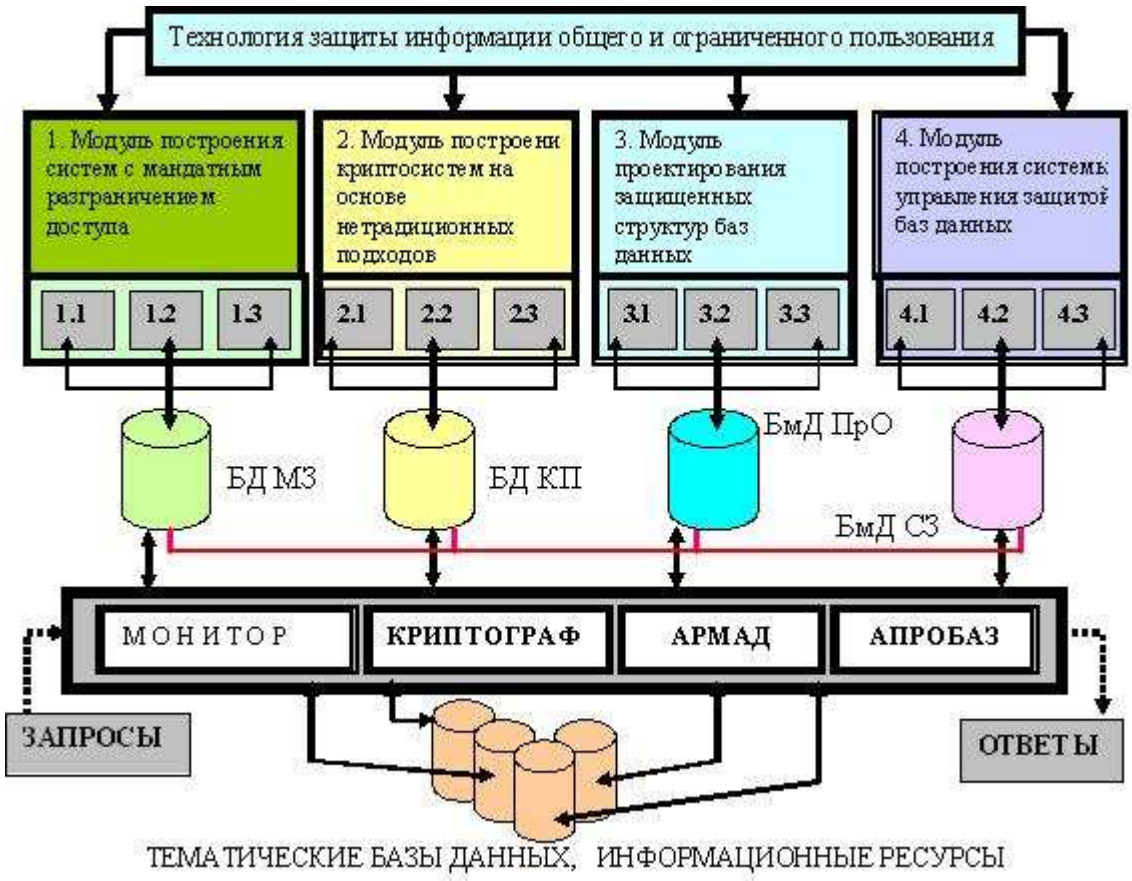

Рис. 1. Взаимосвязь основных компонент технологии защиты информационных ресурсов общего и ограниченного пользования

Обеспечение *конфиденциальности* для интегрированной информации различной степени критичности, хранящейся в БД по различным тематическим направлениям и предназначенной для различных пользовательских групп, достигнуто поэтапным решением следующих задач по управлению защитой информации:

- разработка многоуровневой модели разграничения доступа к данным и алгоритмов, реализующих основные правила мандатного разграничения доступа в соответствии с правилами работы в Республике Казахстан с информацией ограниченного пользования (модуль 1), в том числе спецификация субъектов и объектов (модуль 1.1), контроль и анализ видов прав доступа к ТБД (модуль 1.2), генерация отчетов о попытках НСД (модуль 1.3);
- разработка отдельных компонент криптографической защиты информации повышенной надежности на основе нетрадиционных подходов в системах с мандатным разграничением доступа (модуль 2), в том числе шифрование данных с заданными характеристиками надежности (модуль 2.1), аутентификация пользователей и информационных сообщений (модуль 2.2), генерация и распределение ключей (модуль 2.3);
- анализ предметной области пользователей ТБД, построение спецификаций защиты по обработке и хранению данных ограниченного и общего пользования, моделирование оптимальных структур ТБД при помощи инструментального средства «АПРОБАЗ» (модуль 3.1);
- моделирование структур баз метаданных и построение защищенных структур ТБД по выделенным критериям достоверности и безопасности данных (модуль 3.2);
- моделирование комплекса задач управления системой защиты баз данных от НСД (модуль 4), в том числе моделирование ресурсов защиты (модуль 4.1) и вариантов защиты (модуль 4.2) например - выбор оптимальной СУБД по критериям полноты

покрытия информационных потребностей пользователей и классу защищенности ИВС, формирование комплекса методик аттестации информационных технологий (модуль 4.3)

Контроль целостности данных (модуль 3.3) осуществляется по таким критериям «качества», как полнота данных (контроль неполного или неверного описания значений данных, проверка полного описания структур данных); непротиворечивость данных (проверка логических связей между данными, выявление избыточных и противоречивых описаний, контроль границ диапазона значений и правдоподобия самих значений); актуальность данных (контроль одновременного и своевременного внесения изменений в тематические БД и базы метаданных). Методы и способы контроля базируются на анализе вводимых данных и описаний требований к данным, принятым стандартам СУБД и функциональным потребностям пользователей, зафиксированных в базах метаданных и реализованных в инструментальном средстве «АРМАД».

В разработанной модели мандатного разграничения доступа реализованы расширенный список прав доступа и управление доступом с учетом права реализации, соответствующие принятым в нашей стране нормам и правилам обработки критичной информации в распределенных БД организационного типа. Система криптографической защиты, интегрированная с мандатным разграничением доступа, позволяет при использовании непозиционных систем счисления задавать характеристики надежности криптопреобразований в соответствии со степенью секретности хранимой или передаваемой информации. Высокая криптостойкость предложенных алгоритмов позволяет обеспечить конфиденциальность и целостность информации ограниченного пользования. Спроектированные оптимальные системы защиты БД от несанкционированного доступа позволяют формализовать, алгоритмизировать и в большинстве случаев автоматизировать процесс проектирования оптимальных механизмов и систем защиты БД. Разработанные модели и методы учитывают особенности предметных областей пользователей БД, требования к уровню секретности информационных ресурсов, права пользователей на доступ к конфиденциальной информации и характеристики аппаратно-программной платформы. Оптимизация структур тематических баз данных по критериям надежности и достоверности дает дополнительную защиту от НСД.

В настоящее время разработан комплекс программ в виде монитора безопасного доступа [5], который может быть применен для систем управления государственными органами с древовидной структурой субъектов и объектов защиты информации, в которых функционирует информация различной степени чувствительности. Эффективность разработанной системы с мандатной политикой информационной безопасности продемонстрирована при обеспечении многоуровневого разграничения доступа к тематическим информационным ресурсам в спутниковой информационно-телекоммуникационной системе, создаваемой в Республике Казахстан [6].

Рассмотренная технология защиты направлена на создание интегрированной системы защиты, начиная от проектирования тематических БД, содержащих информацию различной степени конфиденциальности, и заканчивая организацией доступа к подобным информационным ресурсам пользователей различных уровнем полномочий. Мандатное разграничение доступа позволяет автоматизировать обработку требований, определяемых Инструкцией по обеспечению режима секретности в Республике Казахстан (Астана, 2000). Использование непозиционной полиномиальной системы счисления для криптопреобразований информации повышает производительность вычислительных средств за счет распараллеливания арифметических операций. При этом следует отметить простоту реализации и возможность обеспечить необходимую криптостойкость при меньших длинах ключей шифрования. Проектирование оптимальных структур ТБД, с точки зрения защиты от несанкционированного доступа, направленно на уменьшение времени реакции при обработке информации и формировании ответов на запросы пользователей за счет сокращения времени выборки из ТБД.

Библиографический список

1. Конявский В.А., Гадасин В.А. Основы понимания феномена электронного обмена информацией. - Минск: Беллифонд, 2004. – 282 с.
2. Конявский В.А. Информационные технологии как объект защиты и классификация антивирусных программ. // Журнал «Управление защитой информации», Том 11, №4. - М: ВНИИПВТИ, 2007, с.433-436.
3. Защита от несанкционированно доступа к информации. Термины и определения: Руководящий документ // Сборник руководящих документов по защите информации от несанкционированно доступа. - М.: Гостехкоммисия, России, 1998.
4. Об информации, информационных технологиях и о защите информации // Федеральный закон Российской Федерации. Москва, Кремль, 27 июля 2006 года, N 149-ФЗ.
5. Горковенко Е.В., Горбунова Т.В. Программное обеспечение для обработки запросов в информационных системах с мандатным управлением доступа (программа для ЭВМ). // Свидетельство о государственной регистрации объекта интеллектуальной собственности. Запись в реестре Комитета по правам интеллектуальной собственности Республики Казахстан №109 от 25.03.2008, ИС 03499
6. Горковенко Е.В. Организация защиты тематических информационных ресурсов в корпоративной сети космической инфраструктуры. // Материалы XII международной научно-практической конференцию «Решетневские чтения», посвященной памяти ген. конструктора ракетно-космических систем акад. М.Ф. Решетнева.- Красноярск: Сиб.гос. аэрокосмический университет, 2008, с.396-397

E.V.Gorkovenko

DEVELOPMENT OF MODULAR INFORMATION TECHNOLOGY OF DATA PROTECTION OF THE GENERAL AND LIMITED USING

The technology of data protection of various degree of the confidentiality, realized as the interconnected modules - subsystems is considered on the basis of modern methods and mechanisms of data protection.

УДК 004.056

В. Г. Жуков, М. Н. Жукова, А. П. Стефаров

ПОСТРОЕНИЕ МОДЕЛИ СИСТЕМЫ РЕАГИРОВАНИЯ ДЛЯ СЕТЕВЫХ СИСТЕМ ОБНАРУЖЕНИЯ АТАК[3]

Одной из главных проблем систем обнаружения атак является их склонность к большому числу ложных срабатываний. В свете этого актуальной задачей является уменьшение числа ложных срабатываний и повышение достоверности результатов работы СОА. В данной статье предлагается решение этой задачи путем построения модели системы реагирования для сетевых систем обнаружения атак.

Ввиду необходимости использования информационно-телекоммуникационных систем вопрос информационной безопасности становится особо актуальным. Число организаций в мире попавших под воздействие атак безостановочно растёт; ущерб, наносимый вредоносным программным обеспечением: шпионскими и троянскими программами, вирусами, сетевыми червями и т.д. увеличивается. Традиционные средства защиты, такие

[3] Работа поддержана грантом Президента молодым кандидатам наук МК-4294.2008.9

как межсетевые экраны, не могут обеспечить должный уровень безопасности. Зачастую они борются лишь с последствиями атак, в то время как актуальным является работа средств защиты на опережение, то есть определение атаки еще до ее начала, например, при попытке поиска уязвимостей в системе злоумышленником, либо, как минимум, в режиме реального времени. Отсюда следует необходимость использования СОА.

Системами обнаружения атак (IDS – Intrusion Detection Systems) называют множество различных программных и аппаратных средств, объединяемых одним общим свойством – они занимаются анализом использования вверенных им ресурсов и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способны предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин.

СОА контролируют циркулирующую по сети информацию и сравнивают её с заданным набором шаблонов запрещённых типов трафика или действий пользователей (сигнатур).

Одной из главных проблем систем обнаружения атак является их склонность к большому числу ложных срабатываний [1]. У большинства СОА имеются обширные используемые по умолчанию базы данных из тысяч сигнатур возможной подозрительной активности. Производители систем обнаружения атак не могут знать характер сетевого трафика пользователя, что приводит к большому числу ложных срабатываний.

В свете этого актуальной задачей является уменьшение числа ложных срабатываний и повышение достоверности результатов работы СОА.

Уменьшить число ложных срабатываний представляется возможным при помощи построения модели системы реагирования для сетевых систем обнаружения атак.

Адекватный уровень информационной безопасности в организации может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективных политик безопасности. Такие политики определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски информационной безопасности до приемлемой величины [2].

Политика СОА играет важную роль в реализации политики безопасности организации. Вместе с развитием информационных систем должны развиваться и системы безопасности для поддержания своей эффективности. Использование распределенных систем привело к появлению большого числа уязвимых мест, требуются безопасные условия для информационного обмена в телекоммуникационной среде.

СОА выполняет две важные функции в защите информационных ресурсов. Во-первых, она является обратной связью, позволяющей уведомить сотрудников отдела информационной безопасности об эффективности компонент системы безопасности. Отсутствие обнаруженных вторжений при наличии надежной и эффективной системы обнаружения атак является свидетельством того, что система ИБ организации надежна. Во-вторых, она является индикатором, приводящим в действие запланированные ответные меры безопасности.

Безопасность обычно реализуется с помощью комбинации технических и организационных методов [3].

Политика СОА должна определить, какой подход должен использоваться сотрудниками организации в ходе ответных мер при подозрении на атаку. Организация должна иметь специальную группу для расследования инцидентов ИБ.

На основании политики СОА, в АС организации должна быть установлена СОА, сигналы тревоги должны быть проанализированы, политика СОА и локальные инструкции должны изменяться для повышения достоверности работы системы ИБ организации. Следовательно, следует контролировать настройки активного сетевого оборудования, четко классифицировать нарушителя в соответствии с его действиями, сами атаки и настраивать правила СОА.

Таким образом, для построения модели системы реагирования следует учитывать анализируемый трафик, классификацию сигнатур и приоритеты классов сигнатур,

классификацию атак и уязвимостей с соответствующим значением приоритета [4, 5], классификацию компетентности нарушителя [4, 5, 6].

Все сигнатуры СОА классифицируются на группы в соответствии с характером действий и уязвимостями системы, используемых при атаке, каждая из которых имеет свой приоритет по степени риска атаки и определенное количество правил.

Классификация атак строится в соответствии с политикой СОА. Специалист по ИБ оценивает атаки в соответствии со структурой сети, классификацией ценности информации, циркулирующей в системе.

Классификацию атак можно разделить на грубую и тонкую [7].

Под грубой классификацией понимается отключение классов сигнатур, реагирующих на события, которые не могут произойти в данной АС в виду отсутствия того или иного ресурса.

Тонкая классификация подразумевает под собой настройку правил в классах правил в соответствии с политикой СОА, структурой сети.

Для построения модели нарушителя используется информация от служб безопасности и аналитических групп о существующих средствах доступа к информации и ее обработки, о возможных способах перехвата данных на стадии передачи, обработки и хранении, об обстановке в коллективе и на объекте защиты, сведения о конкурентах и ситуации на рынке, об имевших место свершившихся случаях хищения информации и т. п.

Кроме этого, оцениваются реальные оперативные технические возможности злоумышленника для воздействия на систему защиты или на защищаемый объект. Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать злоумышленник в процессе совершения действий, направленных против системы информационной безопасности организации.

При разделении нарушителей по классам можно исходить из его принадлежности определенным категориям лиц, мотивов действий и преследуемых целей, характера методов достижения поставленных целей, квалификации, технической оснащенности и знаний о атакуемой АС.

Создание модели нарушителя или определения значений параметров нарушителя в большей мере субъективно. Модель необходимо строить с учетом технологий обработки информации и особенностей предметной области.

Учитывая вышеизложенное, следует, что модель реагирования должна позволять адекватно и оперативно реагировать на атаки, повышать производительность системы ИБ, при этом число ложных срабатываний СОА должно быть незначительным.

Модель реагирования будет иметь следующий вид (рисунок 1).

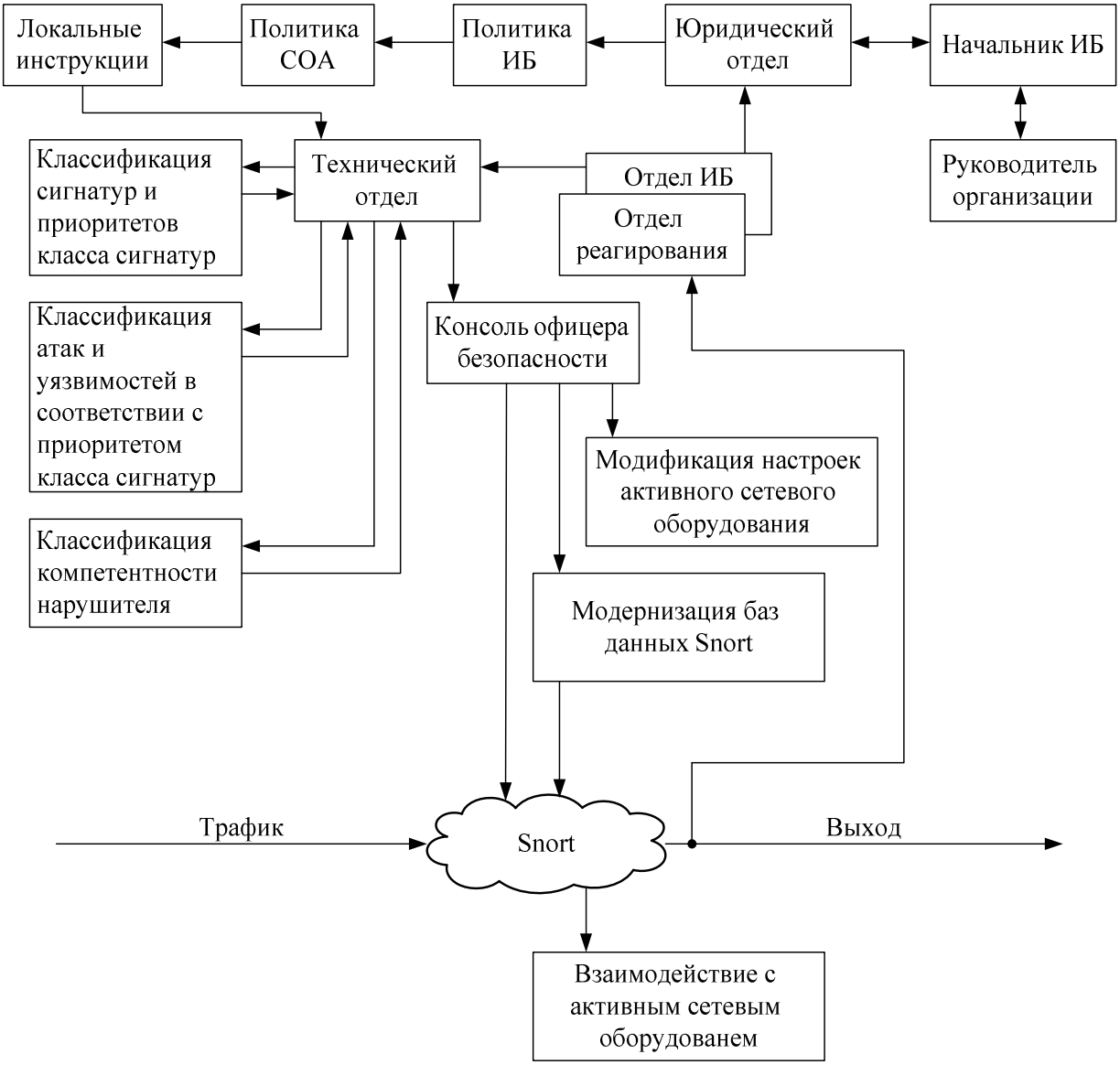

Рисунок 1 – Модель реагирования

Достигнутый уровень развития вычислительной и коммуникационной техники, позволяет построить законченную сеть СОА с множеством сенсоров, протоколирующих инциденты в базу данных, информацию которой можно применять для анализа данных и генерации отчетов. Это поможет лучше использовать данные об обнаруженных вторжениях, получить максимальную отдачу от усилий по обеспечению безопасности и получить наглядные отчеты и графики для демонстрации статистических данных СОА.

Данная модель позволит оптимально применить специалисту по защите информации систему обнаружения атак как один из компонентов обеспечения безопасности сети в многоуровневой стратегии её защиты, в частности позволит решать следующие задачи: создавать новые правила, производить настройку существующих правил на основе политики СОА, тесно взаимодействовать с активным сетевым оборудованием, модернизировать БД Snort, что позволит уменьшить число ложных срабатываний и эффективно применять данные зарегистрированных инцидентов ИБ в качестве доказательной базы при расследовании инцидентов ИБ.

Библиографический список

1. Тихомиров М.М. Безопасность сетей Windows: опыт профессионалов. / М.М. Тихомиров. – СПб.: Икар, 2004. – 271 с.

2. Галатенко А. Активный аудит // InfoSec. – 2006. – № 1. – с. 5-18.
3. Шарков А., Сердюк В. Защита информационных систем от угроз "пятой колонны" // InfoSec. – 2003. – № 8. – С. 7-18.
4. Стефаров А.П. Применение теории игр при оценке систем защиты информации. / А.П. Стефаров, М.Н. Жукова. Сборник публикаций тезисов статей XI международной научной конференции «Решетневские чтения». Направление «Методы и средства защиты информации» – Красноярск: Сибирский государственный аэрокосмический. университет, 2007. – с. 74-75.
5. Стефаров А.П. Оценка системы защиты информации на основе теоретико-игровых моделей. / А.П. Стефаров, М.Н. Жукова. Сборник публикаций тезисов статей IV всероссийской конференции творческой молодежи «Актуальные проблемы авиации и космонавтики». Направление «Методы и средства защиты информации» – Красноярск: Сибирский государственный аэрокосмический. университет, 2008. – с. 52-55.
6. Стефаров А.П. Социальный агент как элемент системы защиты информации. / А.П. Стефаров, М.Н. Жукова, Н.В. Шкроб. Сборник публикаций тезисов статей XII международной научной конференции «Решетневские чтения». Направление «Методы и средства защиты информации» – Красноярск: Сибирский государственный аэрокосмический. университет, 2008. – с. 67-69.
7. Загоруйко Н.Г. Прикладные методы анализа данных и знаний. / Н.Г. Загоруйко. – Новосибирск: Изд-во Института математики, 1999. – 279 с.

V.G. Zhukov, M.N. Zhukova, A.P. Stefarov.

CREATION OF REACTIVE SYSTEM MODEL FOR NETWORK INTRUSION DETECTION SYSTEM

One of the main problems of Intrusion detection systems is high level of false positives. In this case an actual goal is decreasing of false positives` level and increasing of reliability of IDS results. In this article we introduce the way to solve this problem by means of creation of reactive system model for network intrusion detection systems.

УДК 621.396.96.001(07)

В. Г. Жуков, Н. Ю. Паротькин

ПРИМЕНЕНИЕ МОДИФИЦИРОВАННОГО ГЕНЕТИЧЕСКОГО АЛГОРИТМА ДЛЯ ОПТИМИЗАЦИИ СТРУКТУРЫ СЕТИ WI-FI[4]

Рассматривается нахождение оптимальных параметров беспроводной сети Wi-Fi с целью обеспечения соответствия уровня сигнала вне здания государственным нормам и контроля подключений к сети вне периметра помещения.

Для предотвращения несанкционированного подключения к сети Wi-Fi стандартными методами применяется шифрование трафика и скрытие идентификатора сети. Другой способ противостоять данной проблеме является ослабление сигнала до уровня недостаточного для работы с сетью при использовании стандартного оборудования.

Согласно нормативным актам [1, 2] допускается использование на вторичной основе радиочастот в пределах полосы радиочастот 2400 – 2483,5 МГц для эксплуатации внутриофисных систем передачи данных на территории Российской Федерации без оформления разрешений на использование радиочастот, при выполнении следующих условий:

[4] Работа поддержана грантом Президента молодым кандидатам наук МК-4294.2008.9

1) эксплуатации радиоэлектронных средств внутриофисных систем передачи данных только внутри зданий, закрытых складских помещений и производственных территорий;

2) регистрации радиоэлектронных средств внутриофисных систем передачи данных установленным в Российской Федерации порядком.

Выполнение второго пункта возлагается на производителя оборудования, а первого непосредственно на лицо или организацию его эксплуатирующую, при этом в данном пункте подразумевается, что мощность сигнала от точек доступа вне здания не должна превышать установленного уровня. При несоблюдении данных условий согласно статье 68 Федерального закона «О связи» «Ответственность за нарушение законодательства Российской Федерации в области связи» наступает уголовная, административная и гражданско-правовая ответственность в случаях и порядке установленном законодательством Российской Федерации.

Для решения обозначенных проблем необходимо уменьшить мощность сигнала от точек доступа вне помещений, в которых предполагается санкционированная работа с сетью, до определённого уровня.

Данная задача может быть решена двумя способами:

1) экранированием стен помещения;

2) перекомпоновкой размещения активного сетевого оборудования и настройкой его параметров.

Первый вариант предполагает значительные затраты на материалы и установку, кроме того он будет препятствовать прохождению радиоволн других частот, что не всегда желательно. Поэтому подробнее рассмотрим второй вариант решения. Для применения его на практике необходимо подобрать оптимальное соотношение совокупности следующих параметров:

1) Выбор модели точки доступа и места её размещения.
2) Выбор модели сетевых карт.
3) Мощность сигнала активного сетевого оборудования (точки доступа и беспроводных сетевых карт).
4) Выбор типа используемых антенн и их ориентация в пространстве.

В итоге получается 8 параметров, оптимальное соотношение которых должно определить заданную скорость работы беспроводной сети внутри помещения и минимальную мощность сигнала вне его. Данная задача может быть решена как практическими методами, так и аналитическими. Практическое решение потребует значительных временных затрат и договорённости на аренду различного оборудования. Кроме того, исследование мощности сигнала за периметром помещения может быть сложной задачей, если внешняя стена цельная. Для аналитического решения подобной задачи необходимо использовать методы оптимизации, но использование средств численной оптимизации неоправданно, т.к. исследуемая функция имеет 8 аргументов и имеет множество экстремумов. Следовательно, для решения данной задачи целесообразно использовать специальные алгоритмы, предназначенные для решения сложных задач оптимизации, например генетические алгоритмы. Таким образом, необходимо разработать программное средство, которое на основании плана помещения с указанием размещения рабочих мест, материалов стен и уровня допустимого сигнала вне помещения, подбирало оптимальные параметры для сети.

В качестве генетического алгоритма был выбран разработанный ранее модифицированный генетический алгоритм [3]. Данный выбор обусловлен тем, что он даёт лучшие характеристики, чем классический генетический алгоритм по следующим параметрам:

1) эффективность работы алгоритма мало зависит от его первоначальных настроек;

2) выше эффективность поиска экстремумов для многоэкстремальных функций и функций с проблемой плато;

3) наличие дополнительной характеристики, позволяющей отслеживать эффективность работы алгоритма в реальном времени;

4) сравнительная простота внедрения альтернативной целевой функции.

Для расчёта параметров сети был использован типовой метод расчета беспроводных сетей, при котором определялось не расстояние при заданных характеристиках системы, а мощность сигнала в точке, находящейся на определённом расстоянии от точки доступа. Для этого были использованы следующие соотношения. Во-первых, рассчитывались потери в свободном пространстве (1):

$$FSL = 33 + 20(\lg F + \lg D) \quad (1)$$

где FSL (Free Space Loss) – потери в свободном пространстве (*дБ*); F – центральная частота канала, на котором работает система связи (*МГц*); D – расстояние между двумя точками (км).

С другой стороны FSL равен следующему выражению (2):

$$FSL = Y_{дБ} - SOM \quad (2)$$

где SOM – запас в энергетике радиосвязи, для инженерных расчетов обычно принимается равным 10 *дБ*; $Y_{дБ}$ - суммарное усиление системы (*дБ*). L_0 – суммарное затухание сигнала при прохождении через преграды (*дБ*).

Далее необходимо выразить мощность сигнала в точке из формулы для суммарного усиления системы (3). Она будет равна чувствительности приёмника.

$$P_{i,дБмВт} = P_{t,дБмВт} + G_{r,дБи} + G_{r,дБи} - Y_{дБ} - L_{SUM} \quad (3)$$

где $P_{t,дБмВт}$ – мощность передатчика; $G_{t,дБи}$ – коэффициент усиления передающей антенны; $G_{r,дБи}$ – коэффициент усиления приёмной антенны; $P_{i,дБмВт}$ – чувствительность приёмника на данной скорости; L_{SUM} – суммарные потери при распространении радиоволн (*дБ*).

Для нахождения мощности сигнала по периметру помещения из формулы (3) необходимо исключить коэффициент усиления приёмной антенны. При использовании на точках доступа направленных антенн учитывается угол между направлением на точку, в которой необходимо определить мощность сигнала, и направлением главного лепестка антенны. В соответствии с полученным углом выбирается коэффициент усиления передающей антенны по её диаграмме направленности.

Для расчёта суммарных потерь при распространении радиоволн применяется следующее выражение (4):

$$L_{SUM} = L_t + L_r + L_{доп} \quad (4)$$

где L_t – затухание в передающем тракте (*дБ*); L_r – затухание в приёмном тракте (*дБ*); $L_{доп}$ – дополнительные потери в радиоканале (*дБ*).

Потери в приёмном тракте будут равны 0, т.к. во внутриофисных сетях Wi-Fi антенны практически всегда подключаются напрямую к сетевым картам. Параметр $L_{доп}$ определяется видом и толщиной материала, который необходимо преодолеть сигналу по прямой линии от точки, в которой вычисляется мощность сигнала, до передающего устройства.

В качестве целевой функции была использована суммирующая функция, отражающая меру достижения параметров сети, указанных пользователем. Данные параметры определяются совокупностью отклонений уровня сигнала от заданного по периметру помещения и отклонением скорости передачи данных от заданной для указанных точек внутри помещения. В результате данные требования могут быть выражены формулой (5). Штраф для мощности сигнала по периметру вычисляется как нормированное отклонение мощности сигнала умноженного на коэффициент важности соблюдения указанного уровня. При отклонении скорости от требуемой в точках внутри помещения целевой функции назначается штраф, размер которого так же пропорционален величине отклонения.

$$F(x) = \sum_{j=1}^{4} \sum_{i=1}^{N_j} (P_i - P_j) / P_j \cdot k_j - \sum_{i=1}^{R} 0{,}1 \cdot (\exp(V - v_i) - 1) \quad (5)$$

где N_j – номер участка на j-ой стене; P_i – мощность сигнала в точке; P_j – требуемы уровень сигнала на j-ой стене; k_j – коэффициент, отражающий критичность превышения мощности сигнала на j стене (0;1); R – количество работающих сетевых карт; V – требуемая скорость передачи данных для сетевой карты, изменяется дискретно, имеет всего 9 значений от 0 Мбит/с до 54 Мбит/с; V_i – скорость i-ой сетевой карты при данных настройках сети.

Для целевой функции, определённой таким образом, необходимо найти абсолютный максимум, поскольку она представляет собой сумму элементов, положительных в случае соответствия требуемым параметрам и отрицательных в противном случае.

На основании модифицированного генетического алгоритма и приведённых выше аналитических зависимостей было разработано программное средство, решающее поставленную проблему. Главное окно программы представлено на рис.1.

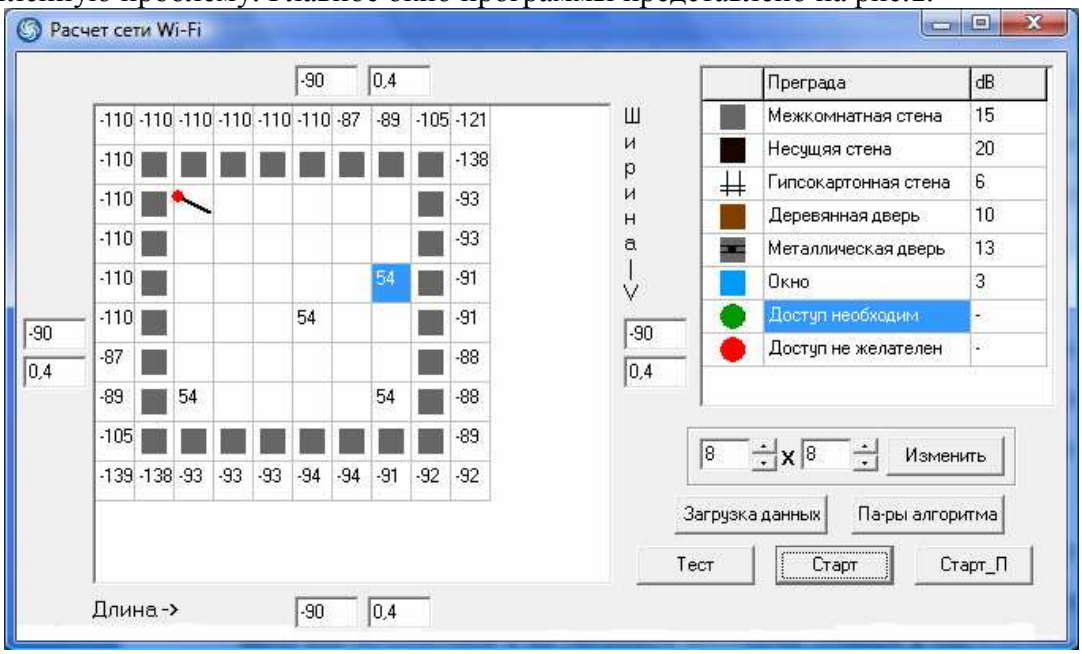

Рис. 1 Главное окно программы

Для работы программы необходимо загрузить базы данных точек доступа, сетевых карт и антенн, в которых указываются параметры оборудования, необходимые для расчёта сети, например, мощность излучаемого сигнала, чувствительность приёмника, диаграмма направленности антенн. При этом в базы данных добавляются только устройства, удовлетворяющие ограничениям по стоимости и функционалу. Для тестирования программы были использованы характеристики оборудования компании D-Link. Вся информация хранится в текстовых файлах, что позволяет редактировать списки оборудования, но при этом необходимо соблюдать формат файла для корректной работы программы.

В левом верхнем углу строится план помещения с указанием материалов стен, выбираемых из списка справа. Пользователь может изменять значения затухания для каждого материала, что позволяет моделировать практически любые помещения. На плане отмечаются зелёными маркерами точки внутри помещения, где предполагается размещение пользователей сети. Требуемая скорость доступа для данных пользователей составляет 48 – 54 Мбит/с. По периметру плана расположены поля для указания уровня мощности сигнала, который не должен превышаться за пределами помещения, рядом указывается коэффициент, отражающий критичность превышения установленного уровня для данной стены.

Кнопки управления, расположенные на форме, позволяют загружать данные характеристик оборудования, вызывать окна для настройки параметров генетического алгоритма, расчёта характеристик сети с указанием всех параметров размещения оборудования и его модели. Кнопки «Старт» и «Старт_П» позволяют запускать алгоритм нахождения оптимальных параметров сети, т.е. нахождения генетическим алгоритмом максимума целевой функции. Параметром завершения поиска экстремума является достижение числа поколений указанного в параметрах ГА. При запуске алгоритма кнопкой «Старт_П» имеется возможность остановить работу алгоритма до достижения указанного числа поколений и его выполнение осуществляется в потоке отдельном от графической формы программы.

В процессе работы алгоритма на график выводится статистическая информация по его работе. При завершении вычислений происходит переход на вкладку информация, где отображается полная информация об использованном оборудовании и его настройках. На план сети выводиться мощность сигнала в *дБмВт* по периметру помещения и скорость сети для указанных точек внутри помещения. Местоположение и направление антенны точки доступа указывается символом ◄—, причем за ось поворота берётся утолщение на линии.

Разработанное программное средство способно рассчитать параметры беспроводной сети Wi-Fi с соблюдением ограничений, устанавливаемых на мощность сигнала вне помещения и на скорость передачи данных в определённых точках внутри него, поэтому можно говорить об успешном решении проблемы конфигурации сети в соответствии с требованиями законодательства и безопасности. Это даёт возможность его применения при построении внутриофисных беспроводных сетей. Данное программное средство не имеет прямых аналогов. В сходном по предназначению программном средстве Ekahau Site Survey (стоимостью около 900$) рассматриваются вопросы обеспечения требуемой скорости и радиуса действия сети, без расчёта уровня мощности сигнала вне помещения.

Библиографический список

1. Федеральный закон "О связи": федер. закон от 07.07.2003 №126-ФЗ // Рос. газ. – 2003. – 10 июля

2. Об использовании полосы радиочастот 2400 - 2483,5 МГц для внутриофисных систем передачи данных: решение ГКРЧ от 6 декабря 2004 г. №04-03-04-003

3. Паротькин Н. Ю. Разработка модифицированного генетического алгоритма для решения сложных задач оптимизации в сфере ИБ // Актуальные проблемы авиации и космонавтики: тез. Всерос. науч.-практ. конф. студентов, аспирантов и молодых специалистов (6–10 апреля 2009, г. Красноярск) : в 2 т. Т. 1. Технические науки. Информационные технологии. Сообщения школьников / под общ. ред. И. В. Ковалева ; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2009.

4. Беспроводные сети Wi-Fi: учебное пособие / А. В. Пролетарский, И. В. Баскаков, Д. Н. Чирков и др. – М.: БИНОМ. Лаборатория знания, 2007. – 215 с.

V. G. Zhukov, N. Y. Parot’kin

THE USE OF A MODIFIED GENETIC ALGORITHM TO OPTIMIZE THE STRUCTURE OF THE NETWORK WI-FI

It is covered the finding of optimum parameters of wireless network Wi-Fi for the purpose of maintenance of conformity of level of a signal out of a building to the state norms and the control of connections to a network the out of a perimeter of room.

УДК 004.056

В. В. Золотарев, Н.С. Заблоцкая

ПРИМЕНЕНИЕ ФАКТОРНОГО АНАЛИЗА ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В работе представлен подход к управлению информационными рисками для системы электронного документооборота с использованием факторного анализа. Показаны способ оценки и оптимизации затрат на информационную безопасность, а также базовая модель факторной оценки информационного риска.

Введение

Факторный анализ представляет собой метод оценки влияния отдельных факторов, действующих на исследуемый объект, на его состояние, свойства и характеристики. В информационной безопасности, как правило, факторный анализ применяется достаточно редко, поскольку при его использовании возникает ряд смежных задач, обладающих собственной сложностью. Такими задачами являются определение и доказательство полноты исходного набора факторов, исследование взаимозависимости действующих факторов, оценка пригодности полученного результата для управления информационной безопасностью. В работе показан подход, позволяющий провести с использованием факторного анализа оценку, оптимизацию и процедуру управления информационными рисками для систем электронного документооборота.

Факторы и целевая функция

Риск системы электронного документооборота в целом определяется как значение целевой функции, зависящей от факторов.

К формированию целевой функции и выбору факторов оценки информационных рисков системы электронного документооборота, можно подходить с двух сторон:

- факторы определяют, насколько хорошо и полно выполняются требования, государственных стандартов, руководящих документов и федеральных законов, предъявляемые к системе электронного документооборота;
- факторы определяют, насколько составные элементы системы электронного документооборота находятся в безопасности, какие существуют уязвимости, и ценность самих элементов.

В данной работе был выбран второй метод оценки. Система электронного документооборота состоит из элементов, ее образующих. Для каждого элемента системы находится значение целевой функции. Суммирование значений по всем требованиям дает значение риска для системы электронного документооборота (СЭД) в целом.

В дальнейшем же планируется разработать и первый метод оценки, подобрать соответствующие факторы, требования нормативно-правовой части, спроектировать целевую функцию. Предполагается, что целевые функции как для первого, так и для второго методов будут несильно отличаться друг от друга, и в дальнейшем можно будет производить комплексную оценку по обоим методам.

При выборе факторов риска для выбранного метода оценки можно руководствоваться ГОСТ Р 51275-2006 «Объекты информатизации. Факторы, воздействующие на информацию». В соответствии с данным стандартом объектом информатизации (ОИ) является совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а

также средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров. Как можно заметить, это определение довольно емкое, и оно включает в себя понятие системы электронного документооборота [1].

Полнота и достоверность выявленных факторов, воздействующих или могущих воздействовать на информацию, достигается путем рассмотрения множества факторов, воздействующих на все элементы объекта информатизации и на всех этапах обработки информации.

В данном случае проводится оценка рисков по десяти факторам. Было взято более 3 факторов (в отличие от существующих методик) по той причине, чтобы детально со всех сторон оценить СЭД и сократить количество вопросов, на которые должны ответить лица, принимающие решение, для получения результата (в данном случае элементов системы, подвергаемых оценке). Число факторов, равное десяти, получилось в результате анализа и обобщения факторов, воздействующих на информацию, взятых из стандарта.

Итак, были выбраны следующие факторы:

1. ценность анализируемого элемента системы электронного документооборота (Ф1);
2. дефекты, сбои и отказы, аварии технических систем и систем объекта информатизации (под объектом информатизации понимается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены) (Ф2);
3. дефекты, сбои и отказы программного обеспечения объекта информатизации (Ф3);
4. угроза от явлений техногенного характера (Ф4):
   - непреднамеренные электромагнитные облучения объекта информатизации;
   - радиационные облучения объекта информатизации;
   - сбои, отказы и аварии систем обеспечения объекта информатизации;
5. угроза от действий криминальных групп и отдельных преступных субъектов (Ф5):
   - диверсия в отношении объекта информатизации;
   - диверсия в отношении элементов объекта информатизации;
6. недостатки организационного обеспечения защиты информации (Ф6):
   - при задании требований по защите информации (требования противоречивы, не обеспечивают эффективную защиту информации);
   - при несоблюдении требований по защите информации;
   - при контроле эффективности защиты информации;
7. ошибки обслуживающего персонала объекта информатизации (Ф7):
   - при эксплуатации технических систем;
   - при эксплуатации программных средств;
   - при эксплуатации средств и систем защиты информации;
8. несанкционированный доступ к защищаемой информации (Ф8):
   - путем подключения к техническим средствам и системам объекта информатизации;
   - путем использования закладочных средств;
   - путем использования программного обеспечения технических средств объекта информатизации;
   - путем хищения носителя защищаемой информации;
   - путем нарушения функционирования технических систем обработки информации;
9. разглашение защищаемой информации лицами, имеющими к ней право доступа (Ф9):
   - через лиц, не имеющих право доступа к защищаемой информации;
   - через передачу информации по открытым линиям связи;

- через обработку информации на незащищенных технических системах обработки информации;
- через опубликование информации в открытой печати и других средствах массовой информации;
- через копирование информации на незарегистрированный носитель информации;
- через передачу носителя информации лицам, не имеющим право доступа к ней;
- через утрату носителя информации;

10. частота совершаемых несанкционированных доступов по отношению к данному элементу СЭД (Ф10).

Функцию риска можно получить путем применения подходов математической логики. Можно заметить, что при полученных факторах итоговый риск СЭД прямо зависит от них: чем выше уровень фактора, тем выше уровень риска, и наоборот.

Исследовав зависимости выбранных факторов друг от друга, формируем целевую функцию риска:

$$F=Ф1 \vee Ф2 \vee Ф3 \cap Ф2 \vee Ф4 \vee Ф5 \vee Ф6 \vee Ф7 \vee Ф8 \vee Ф9 \vee Ф10 \cap (Ф8 \vee Ф9),$$

где F – функция риска,

Ф1,Ф2,…Ф10 – факторы, выбранные для данной методики,

∩ – символ пересечения (если между факторами есть зависимость),

V – символ объединения (если между факторами нет явной зависимости),

Упростив данную функцию, используя методы математической логики, получаем:

$F=Ф1 \vee Ф2 \cap (1 \vee Ф3) \vee Ф4 \vee Ф5 \vee Ф6 \vee Ф7 \vee (Ф10 \vee 1) \cap (Ф8 \vee Ф9)$.

Если осуществить переход на количественные характеристики, то функцию модно представить следующим образом:

$$F=Ф1 + Ф2 * (1 + Ф3) + Ф4 + Ф5 + Ф6 + Ф7 + (Ф10 + 1) * (Ф8 + Ф9).$$

Исследуя качественные характеристики предлагаемого подхода, можно отметить, что формирование целевой функции является достаточно трудоемкой задачей. Авторам представляется, что решение этой задачи во многом определяет успешность дальнейшей оценки; вместе с тем целевая функция часто уникальна для каждой рассматриваемой системы. Методы формирования целевых функций задач такого вида авторы планируют подробно рассмотреть в других работах, в то время как данная функция была получена экспертным путем с применением итеративных методов опроса (метода парных согласований, метода Дельфи).

Принцип ранжирования

Обычно количественные показатели используются там, где это допустимо и оправдано, а качественные – где количественные оценки по ряду причин затруднены. Количественные показатели существующих или предлагаемых ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса, а также при помощи определения затрат на их приобретение.

В данном случае не для всех элементов системы обмена электронными документами приемлемо количественное выражение, либо оно затруднено. Поэтому выбор был сделан в пользу качественной оценки факторов.

Для каждого составного элемента системы электронного документооборота, исследуемой на предмет наличия информационных рисков, производится оценка факторов. Оценки для факторов выставляются лицами, принимающими решение по 5-уровневой шкале {Очень низкий; Низкий; Средний; Высокий; Очень высокий}.

Для удобства программной реализации необходимо получить шкалу оценки факторов риска – переводом качественных показателей в количественные. При определении количественной характеристики показателей были приняты во внимание следующие замечания [2]:

– значения факторов лежат в пределах (0;1);

– очень низкий фактор не означает его отсутствие;
– очень высокий фактор не означает его 100% выполнение;
– показатели факторов равномерно удалены друг от друга (равный шаг).

Было получено следующее соответствие количественных и качественных показателей:
Очень низкий – 0,1;
Низкий – 0,3;
Средний – 0,5;
Высокий – 0,7;
Очень высокий – 0,9.

Шаг был выбран равный величине 0,2.

Целевая функция имеет минимум в точке (0.1,0.1,…,0.1), когда все факторы принимают минимальное значение, и максимум в точке (0.9,0.9,…,0.9), когда все факторы риска принимают максимальное значение.

Произведя обследование функции риска таким образом, были получены интервалы, при попадании в которые система электронного документооборота имеет очень низкий, низкий, средний, высокий или очень высокий уровень риска (таблица 1).

Таблица 1 – Уровни риска

Уровень риска	Интервал значений
Очень низкий	0,83 – 2,3
Низкий	2,4 – 4,2
Средний	4,21 – 6,01
Высокий	6,02 – 7,82
Очень высокий	7,83 – 9,63

Можно заметить, что в данном соотношении расстояние между границами интервалов для всех уровней разные, причем они увеличиваются с возрастанием уровня. Это объясняется тем, что чем больше значение отдельного фактора, тем больше его влияние на уровень риска (например, ценность информации).

Формирование рекомендаций

Очевидно, что целью применяемого метода, помимо оценки информационного риска, является формирование рекомендаций по управлению риском для заданной ситуации. Необходимо получить оптимальные (условно оптимальные) значения факторов, чтобы предложить мероприятия по достижению требуемого уровня риска. Данные задачи рассматривает теория оптимизации технических систем.

В общем виде задача оптимизации может быть записана следующим образом:

$$F(X) \to \underset{X \in D \subseteq S}{opt}.$$

Здесь $F=\{f_1, f_2, \ldots, f_k\}$ – оптимизируемая функция, численно выражает степень достижения целей функционирования оптимизируемого объекта. $X=(x_1, x_2, \ldots, x_n)$ называется вектором независимых переменных, его компоненты – неизвестными в задаче оптимизации. D – множество допустимых значений неизвестных, определяемое налагаемыми на неизвестные ограничениями. D по другому называется допустимой областью. S – пространство оптимизации. В данном случае оптимальным будет минимальное при заданных ограничениях значение.

Для данной задачи оптимизируемой функцией является целевая функция риска; неизвестными в задаче оптимизации – факторы риска; D – интервал (0; 1); S определяется следующими ограничениями: факторы принимают только конкретные дискретные значения: {0,1; 0,3; 0,5; 0,7; 0,9}. Данная задача является однокритериальной (так как k=1) и многомерной (так как n=10) задачей оптимизации. Так как $D \subset S$ и в задаче не все

значения переменных допустимы, т.е. имеются некоторые ограничения на них, то такая задача является условной задачей оптимизации или задачей с ограничениями.

При анализе существующих методов условной оптимизации было замечено, что для решения данной задачи подходят как методы нелинейного программирования, так и дискретной оптимизации. Окончательно был выбран метод локального поиска для оптимизации на дискретной решетке без существенных ограничений.

Задача формулируется таким образом: необходимо найти факторы, которые приведут целевую функцию к требуемому уровню риска за минимальное количество шагов. На функцию и факторы накладываются ограничения:

для целевой функции задан интервал значений;
шаг фактора;
максимальное количество шагов;
стоимость операции перехода на следующий качественный уровень;
максимальная суммарная стоимость всех операций перехода.

При этом учитывается также исходное состояние функции, т.е. во внимание принимаются значения факторов, полученных после процедуры согласования, характеризующие текущее состояние системы электронного документооборота. На выходе данного алгоритма получаем значения факторов, при которых система имеет требуемый (чаще всего низкий) уровень риска.

Оптимальная стоимость рекомендаций

Для обеспечения адекватности предлагаемых мероприятий в системе задается стоимость перехода – затраты на изменение в положительную сторону качественного уровня воздействия факторов. В качестве ограничения, обусловливающего переход с одного уровня на другой – стоимость мероприятий, обеспечивающих данный переход, либо количество операций, затрачиваемых на данный переход. Максимальную стоимость определяет Заказчик перед проведением оценки рисков.

В этом случае задача оптимизации формулируется следующим образом: требуется определить минимально затратный способ достижения заданного уровня информационного риска для системы электронного документооборота. Исследуется как общая стоимость (обозначенная как C) всех операций по изменению качественного уровня, так и непревышение заданной максимальной суммарной стоимости всех операций.

Формулируя задачу окончательно, можно указать ее общий вид:

$$F(X) \to \min_{X \in D \subseteq S},$$

$$\sum_{i=1}^{N} C_i \geq C_{\max},$$

$$\sum_{i=1}^{N} C_i \to \min.$$

При этом необходимо отметить некоторые особенности расчета стоимости каждой операции. Учитывая, что противодействие каждому фактору имеет свою усредненную стоимость операции перехода на следующий качественный уровень, при общем количестве операций N требуется дифференцировать стоимость операций для каждого фактора. Вместе с тем, несмотря на внутренние отличия, закон увеличения стоимости таких операций, по-видимому, имеет общий вид. Авторами предлагается в данном случае декларировать экспоненциальное увеличение стоимости операций с каждым шагом, что соответствует принятым в области анализа информационных риском положениям основных литературных источников [например, см. 3], но требует широкого экспериментального подтверждения.

Выводы

Предлагаемый авторами подход может быть использован в рамках проведения базового экспертного анализа информационных рисков и управления риском для систем электронного документооборота. Достоинством предлагаемого подхода является простота используемых экспертных подходов, что снижает влияние эксперта на итоговый результат оценки, а также возможность использования стандартных методов оптимизации для доказательства оптимальности применяемых мер по противодействию конкретным дестабилизирующим факторам и снижению уровня информационного риска для системы в целом.

Библиографический список

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информации. – Введ. 01.02.2008. – М.: Стандартинформ, 2007 г.
2. Золотарев В.В., Ширкова Е.А. Фундаментальные основы методик базового экспертного анализа информационных рисков // Прикладная дискретная математика, 2008, №2 – Томск: Изд-во Томского гос. ун-та – с.71-76
3. Петренко С.А., Симонов С.В. Управление информационным риском. Экономически оправданная безопасность. – М.: Компания АйТи, ДМК-Пресс, 2004. – 384 с.

V. V. Zolotarev, N.S. Zablotskaya

INFORMATION RISK MANAGEMENT ON COMPONENT ANALYSIS BASE FOR ELECTRONIC DOCUMENT CIRCULATION SYSTEMS

Here is presented the approach of information risk management for electronic document circulation system with component analysis usage. The way of estimation and optimization of expenses for information security, and also base model of information risk factor estimation are shown.

УДК 004.056

А. А. Калинин

СЛОГОВОЙ МЕТОД ГЕНЕРАЦИИ ПАРОЛЕЙ

Статья повествует об алгоритме генерации легкозапоминающихся паролей, близких по структуре к словам естественного языка, на основе порождения случайных слогов.

Проблема ограничения доступа к информации является актуальные массового внедрения информационных технологий в современном обществе; наряду с ростом значимости информации в мире эволюционируют и методы несанкционированного доступа к ней. Соответственно в процессе этого антагонизма появились и совершенствуются инструменты информационной защиты. Наиболее распространенными, простым во внедрением, но, в тоже время, и малонадежным средством является защита паролем.

Пароль (фр. *parole* — слово) — это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий. Пароли часто используются для защиты от несанкционированного доступа. информации

Для того чтобы обеспечивать эффективную защиту пароль должен соответствовать следующим критериям:

- пароль должен быть максимально возможной длины;
- использовать максимальное количество символов;

- исключать комбинации символов, которые можно подобрать по словарю.

Также для обеспечения надлежащей защиты необходима как можно более частая смена пароля и невозможность попадания символьной комбинации к третьим лицам.

Генераторы паролей, выдающие случайную комбинацию символов, оказываются очень полезным, когда нужно создать случайный пароль, который можно подобрать лишь машинным перебором, и удобны для сколько угодно частой генерации таких паролей.

Примеры генерируемых паролей:

bnppXztZ

Jhz9Rx7ahN

bzPaYcOfiG

Эти пароли хороши с точки зрения сложности их подбора машиной, однако они очень плохи в плане их запоминания человеком. Ситуация многократно усложняется, если используется режим частой смены паролей, что побуждает пользователя такого случайного пароля хранить его в записях на бумаге, электронных носителях и т.д. Это в свою очередь повышает риск попадания пароля к третьим лицам, что делает информацию очень уязвимой.

Таким образом, часто меняющийся пароль должен 1) быть случайной комбинацией символов 2) быть легким для запоминания.

Первая проблема легко решается с помощью использования генераторов случайных чисел. Сложность же восприятия случайных паролей состоит в том, что человеку нужно запомнить дискретную последовательность символов, т.е. запомнить каждый символ и его место в отдельности, что безусловно сложнее запоминания естественных слов, представляющих собой символьное единство, и поэтому легко удерживаемых в памяти и воспроизводимых при необходимости. Поэтому хороший для запоминания, и в тоже время надежный пароль должен быть случайным и одновременно напоминать слово на естественном языке.

Данная проблема может быть решена, если мы представим слово как последовательность не просто символов, но как последовательность слогов — супра-символов, включающих элементарные символы.

Например, возьмем следующие пароли:

slwk3cn4ix и erftumvak5 — статистическая вероятность появления таких слов в естественном языке примерно одинаково маловероятна, однако второй проще запомнить, т.к. он обладает слоговой структурой в отличие от первого. Наличие слоговой структуры «erf-tum-vak-5» позволяет пользователю проговаривать про себя пароль, задействую не только отделы мозга отвечающие за абстрактное мышление, но также и более глубокие нейронные уровни, связанные с артикуляцией, что существенно закрепляет связь между символьной комбинацией и ее образом в памяти пользователя.

Поэтому, «словоподобные» пароли, построенные на основе слогов, наиболее подходят для использования, особенно при частой смене парольных комбинаций.

Итак, для создания таких паролей нам необходима эксплицитная модель слога, которая может быть использована машиной.

В лингвистике слог, согласно сонорной теории слога, - это отрезок речи, ограниченный звуками с наименьшей звучностью, между которыми находится слоговой звук, звук с наибольшей звучностью, т.е. гласный звук, факультативно окруженный согласными. Соответственно, если принять множество гласных звуков за V (vocals) , а согласных за C (consonants), то слог может принимать следующие типы: V, CV, VC, CVC. Разумеется, возможны и другие варианты слогов вроде CCV, CCVCC, а также слоговой вершиной может являться и согласный звук, но данные явления не являются языковыми универсалиями и поэтому в данной модели засматриваться не будут.

Таким образом, из элементарных символов, букв, порождаются супра-символы, слоги, из которых в свою очередь и строится слово, пароль.

Теперь перейдем к тому, как можно эту модель использовать в алгоритме генерации

паролей и к рандомизации этого алгоритма.

Алгоритм будет представлен на языке программирования PHP:

Задаем массивы гласных и согласных букв:

$vowels = array ("a","e","i","o","u",);

$consonants = array ("b","c","d","f","g","h","j","k","l","m","n","p","r","s","t","v","z");

Буквы *q,x* исключены из массивов, т.к. они могу порождать плохочитаемые комбинации. Буква *q* не может быть использована без буквы *u*, а буква *x* состоит из двух фонем, что может вызвать затруднение в артикуляции при длинной цепочке согласных звуков, и, следовательно, в запоминании.

Также добавим массив цифр от 0 до 9

$digits = array ("0","1","2","3","4","5","6","7","8","9");

Итак, инвентарь символов перечислен. Теперь зададим инвентарь супра-символов — слогов. Они в рамках данного алгоритма насчитывают 5 типов:

V, CV, VC, CVC, D («цифровой» слог).

Теперь смоделируем процесс случайной генерации одного слога: присвоим переменным $v, $c, $c1 и $d случайные значения из соответствующих массивов с помощью оператора *rand*:

$v = $vowels [rand (0,4)];

$c = $consonants [rand (0,17)];

$c1 = $consonants [rand (0,17)];

$d = $digits [rand (0,9)];

Таким образом, мы имеем ряд возможных элементов для генерации любого из 5 типов слога. После того, как каждая возможная переменная приняла случайное значение из соответствующего ей массива, мы задаем множество возможных типов слога:

$sylltype = array ("$v","cv","vc","cv$c1","$d");

и теперь после случайного выбора типа слога, из случайных элементов генерируется и выводится случайный слог:

$syll = $sylltype [rand (0,4)];

echo $syll;

Длина слога от 1 до 3 символов. Для генерации более длинных паролей необходимо произвести ряд итераций данного алгоритма.

При проведении 3 итераций, получаются следующие пароли длиной от 3 до 9 символов:

0ruza

rorilnet

nibuh4

5dodlug

Эти пароли являются набором совершенно случайных символов, но в отличии от «чисто случайно» сгененрированных паролей, они обладают слоговой структурой, что позволяет проще хранить их в памяти.

Выводы

Недостатком этого алгоритма является, то что наряду с хорошо запоминаемыми паролями, он может генерировать плохозапоминаемые пароли вроде *34de7u*, а также короткие пароли вроде *a3g*. Данный недостатки могут быть решены за счет включения в алгоритм условия на ограничение определенного количества символов (регламент длины пароля), а также ограничение количества тех или иных символов, например цифр, до 1.

Также алгоритм генерации «словоподобных» паролей может быть улучшен за счет включения в модель согласных сонорных звуков в качестве слоговой вершины, моделирование слога на основе более сложной линвистической модели «инициаль — медиаль — финаль», а также применение правил дистрибуции тех или иных букв при генерации случайных слогов.

A.A. Kalinin
SYLLABIC-BASED PASSWORD GENERATION

The artcicle is about producing easy-to-remember passwords possessing natural syllabic structure based on the method of random syllables generation.

УДК 004.056

Ф.Ю. Кулишов
АЛГОРИТМЫ СИГНАТУРНОГО АНТИВИРУСНОГО ПОИСКА ДЛЯ СОВМЕРЕННЫХ SIMD-ПРОЦЕССОРОВ

Рассматриваются алгоритмы поиска регулярных выражений для применения в сетевом поиске вредоносных объектов. Предлагается SIMD-реализация поиска регулярных выражений, способная более полно задействовать вычислительную мощность современных процессоров. В качестве платформы для реализации был выбран процессор Cell Broadband Engine.

Введение

В связи с бурным развитием Интернета и ростом его значимости как бизнес-инструмента все выше становится цена простоев IT-инфраструктуры, многие из которых вызываются вредоносным программного обеспечения: вирусов, червей и троянских программ. Дополнительную проблему представляют растущие скорости передачи данных по сетям. Современные сетевые антивирусные решения, даже основанные на узкоспециализированных ASIC-вычислителях, с трудом успевают за этим ростом [1]. К тому же, добавление нового функционала для таких устройств невозможно, разработчиков под такие платформы крайне мало, а весь цикл разработки очень дорог.

Таким образом, задача создания быстродействующих и гибких программно-аппаратных комплексов с функциями эффективного сетевого обнаружения вредоносного ПО представляется в данный момент актуальной. Также актуальным являеся поиск заранее известных вредоносных объектов (т.н. сигнатурный поиск), т.к. он имеет предсказуемое быстродействие и допустим для сетевой обработки данных.

Данная работа представляет реализацию алгоритмов поиска регулярных выражений (РВ), являющихся основой производительного сетевого поиска, для SIMD-процессора Cell BE. Рассматриваются детерминированные (ДКА) и недетерминированные конечные автоматы (НКА), их оптимальная реализация на Cell BE, а также SIMD-оптимизация алгоритма выполнения НКА.

Современные методы поиска регулярных выражений

Главным преимуществом ДКА является фиксированное время поиска, не зависящее от сложности и длины РВ, т.е. 1 входной символ обрабатывается за время $O(1)$. При этом затраты на размещение ДКА данного РВ в памяти могут составить в худшем случае до $O(2^m)$, где m — длина РВ. В отличие от ДКА, НКА требуют для размещения всего $O(m)$ памяти, но при этом время на 1 входнй символ составляет до $O(m^2)$. [2,3]

В последние годы при разработке новых алгоритмов поиска РВ упор делался в основном на внесение различных дополнительных сущностей в классический ДКА: как правило, ребра и вершины автоматного графа несли некоторую дополнительную информацию. Это позволяет значительно снизить расходы памяти для худшего случая, не допуская заметной потери производительности. Примерами являются D^2FA [4], XFA [5,6],

delta-FA [7], HFA [8], H-cFA [8]. Такое усложнение алгоритма сравнения допустимо, если он выполняется на специально разработанной аппаратной архитектуре, но, как правило, приводит к заметному снижению быстродействия на процессорах общего назначения, как показано в [5,6]. Кроме того, эти алгоритмы не используют SIMD-инструкции.

Другой подход состоит в том, чтобы ДКА - затратный по памяти, но быстрый алгоритм — выполнял бы поиск по части РВ, а именно по префиксам, и при совпадении данных с префиксом РВ отправлял бы этот поток на дальнейший анализ [8,9. Такие автоматы называют префиксными. Это оправдано в случае, когда большинство анализируемых данных не является вредоносным, что справедливо для большинства сетевых потоков, кроме почтовых [10].

Процессор Cell BE представляет интерес главным образом за счет очень производительного интерфейса взаимодействия с памятью, а также большого количиства (128) SIMD-регистров по 128 бит каждый. В первую очередь его используют для сложных научных расчетов и трехмерного моделирования. У него есть свои особенности программирования, например, крайняя нежелательность ветвлений, а также сравнительно малый объем быстрой кэш-памяти [11]. Таким образом, двухступенчатый анализ можно признать предпочтительным.

Реализация поиска регулярных выражений для процессора Cell BE

Работа обычного ДКА на РВ в программном коде обычно производится по принципу:

```
state = DFA[state][inputSymbol];
```

где *DFA* — двумерный массив таблицы переходов, *state* — номер состояния, *inputSymbol* — входной символ, приводящий к изменению состояния. Для некоторых процессорных архитектур быстрее выполнится конструкция вида:

```
S = *(S + c*sizeof(S));
```

В этом случае состояние является указателем на его строку переходов — то есть на массив, каждый элемент которого является указателем на следующую строку переходов.

ДКА-варианту нужна всего одна инструкция Cell для совершения перехода:

```
lqx $(state_R), $(state_R), $(symbol_R)
```

при выполнении которой указатель на текущую строку состояния обновляется на основе поступающего на вход символа.

Как было отмечено выше, в худшем случае выполнение РВ-поиска при помощи НКА займет до $O(m^2)$ операций. Однако, если длина РВ меньше, чем разрядность процессора, то существует эффективный способ выполнения НКА, основанный на алгоритме СДВИГ-ИЛИ [12]. В виде строки программы на С это выглядит как:

```
D = (D << 1) | B[c]
```

где *D* — состояние автомата, *c* — входной символ, *B* — массив заранее сформированных битовых масок.

Этот алгоритм легко расширяется на случай простых регулярных выражений [13], при этом позволяя выполнять поиск в SIMD-режиме, когда в длинный процессорный регистр загружено сразу несколько автоматов для РВ. Упрощенная поддержка РВ допустима для построения префиксного автомата, а высокая скорость работы (за счет SIMD) позволяет использовать такой алгоритм при обнаружении потенциально опасных объектов.

Для дальнейшего анализа уже отобранных потенциально опасных объектов будет применяться SIMD-версия СДВИГ-ИЛИ с полной поддержкой РВ, имеющая быстродействие примерно в 3 раза ниже вышеупомянутой [13], однако вызываться она будет только по запросу для обработки очень малой части трафика.

Длина SIMD-регистра вычислительного ядра Cell BE (называемого SPE) равна 128 бит, что позволяет за один такт обрабатывать 1 выражение из 128 символов, или 4 по 32 бита, или 8 по 16, или 16 по 8. Сравнение одного символа с этим набором РВ потребует 4 или 5 инструкции (5 для 8-битовых РВ). При полной поддерже РВ на 1 символ тратится до 15

инструкций.

Полученные результаты

Несмотря на то, что первое поколение процессоров Cell вышло в 2005 году, есть крайне ограниченное количество работ по использованию его для строкового поиска. Цикл работ, сведенный воедино в [14], описывает ДКА для алгоритма Ахо-Корасик. В открытых источниках не встречалось информации о реализации алгоритмов поиска РВ на платформе Cell, так что предлагаемые алгоритмы претендуют на инженерную новизну.

Ввиду отсутствия прямых аналогов сравнение результатов ведется с двумя вариантами реализации алгоритма Ахо-Корасик, первый из которых, AC-LS, рассчитан на работу с сигнатурами из локального кэша SPE-ядер, а второй, AC-HD (HD = Heavy Duty, высокая нагрузка), может работать с сигнатурами из оперативной памяти (ценой заметного уменьшения производительности). Оба варианта используют имеющую ограниченные возможности SIMD-версию табличных перестановок (table lookups), что оправдано для взятого там 32-символьного входного алфавита и специальной схемы группировки 16 входных потоков, при которой один 16-байтный регистр входного буфера содержит по 1 байту из каждого потока. Такое сложное преобразование требует дополнительного сетевого устройства (названного там преобразователем сессий, sessionizer), что вместе с крайне малым размером входного алфавита существенно ограничивает применение предложенного метода.

Характерно, что авторы работы [14] не стали использовать многочисленные усовершенствования классического алгоритма Ахо-Корасик (сжатие пути, слияние состояний и т.п.), т.к. их введение не позволит воспользоваться всеми преимуществами SIMD-архитектуры. Кроме того, программа для процессора Cell должна по возможности избегать ветвлений ([11]), часто использующихся в новых версиях алгоритмов сравнения.

Указанные реализации можно сравнить на основе *таблицы 1* ниже; жирным шрифтом выделены преимущества того или другого варианта.

Таблица 1. Сравнительная характеристика AC-LS, AC-HD, ДКА и НКА на Cell BE

Критерий	**AC-LS**	**AC-HD**	**ДКА**	**НКА**
Поддержка РВ	Нет	Нет	**Полная**	Простая
Размер алфавита	32	32	**256**	**256**
Входных потоков	16	16	7	**1**
Преобразование входного потока (на 1 SPE)	Выбор по одному байту из 16 потоков	Выбор по одному байту из 16 потоков	Подача на вход 7 потоков одновременно	**Не требуется**
Производительность на 1 SPE	5.1 Гбит/с	0.28 Гбит/с	**7.5 Гбит/с**	1.3 Гбит/с
Использование SIMD	**Есть**	**Есть**	Нет	**Есть**
Состояний на 1 SPE	1700	**1700 + ОЗУ**	60	7000
Из них одновременно используются	1700	**1700 + ОЗУ**	60	512

В представляемой работе сложно привести сравнение с РВ-поиском на процессорах семейства x86. В данный момент происходит смена поколений флагманских процессоров Intel, например, новые образцы оснащены встроенным контроллером памяти, что положительно повлияет на быстродействие РВ-поиска. На старых образцах (одноядерные Pentium4 2.4 ГГц) быстродействие алгоритма Бойера-Мура (поиск фиксированных строк) достигало не более 400 Мбит/сек на 5000 шаблонов. Соответственно, можно ожидать от современнных 4-ядерных процессоров не более 2 Гбит/с, в то время как Cell-реализация обеспечивает как минимум 10 Гбит/с на процессор из 8 SPE-ядер. Производительность

современных 4- и 8-ядерных процессоров Intel будет детально проанализирована в дальнейших работах.

Заключение

Представленный в данной работе алгоритм поиск регулярных выражений может выполняться в SIMD-режиме на современных процессорах (как универсальных, так и графических), его реализация для Cell BE имеет высокую производительность по сравнению с традиционными x86-решениями. Применение данного алгортма представляется перспективным на сетевых шлюзах безопасности, а также для поиска среди больших объемов неструктурированной информации.

Библиографический список

1. Линейка продукта SourceFire IPS. - http://www.sourcefire.com/products/3D/ips
2. М. Мозговой. Классика программирования: алгоритмы, языки, автоматы, компиляторы. Практический подход. - СПб: Наука и техника, 2006.
3. R. Cox. Regular Expression Matching Can Be Simple And Fast — http://swtch.com/~rsc/regexp/, 2007
4. S. Kumar, F. Yu, P. Crowley, J. Turner. Algorithms to Accelerate Multiple Regular Expressions Matching for Deep Packet Inspection. In proc. of SIGCOMM, 2006
5. R. Smith, C. Estan, S. Jha. XFA: Faster Signature Matching With Extended Automata. - In IEEE Simposium on Security and Privacy, 2008
6. N. Goyal, J. Ormont, R. Smith, C. Estan. Signature Matching in Network Processing Using SIMD/GPU Architectures. - 2008
7. D. Ficara, S. Giordano, G. Procissi. An Improved DFA for Fast Regular Expression Matching. - ACM SIGCOMM Computer Communication Review, Vol. 38, Number 5, 2008
8. S. Kumar, J. Turner, G. Varghese. Curing Regular Expressions Matching Algorithms from Insomnia. Amnesia, and Acalculia. In proc. of ANCS, 2007
9. M. Becchi, P. Crowley. «A Hybrid Finite Automaton for Practical Deep Packet Inspection». - CoNEXT, 2007
10. Материалы антивирусного интернет-портала www.viruslist.ru
11. Руководство «Cell Broadband Engine Programming Handbook». - www.ibm.com, 2007
12. Baeza-Yates R., Gonnet R. A new approach to text searching. Communications of the ACM, 35(10):74{82), 1992
13. Navarro G. Pattern Matching. Technical Report. Department of Computer Science, University of Chile, 2003
14. D. Scarpazza, и др.. Exact Multi-pattern String Matching on CellBE Processor. - 2008.

F.Y. Kulishov

SIMD REGULAR EXPRESSION MATCHING ALGORITHM FOR FAST ANTIVIRUS SEARCH

The parer is devoted to fast regular expression search for network-based malware detection. A SIMD algorithm of regexp search is proposed, its implementation on Cell BE processor outperforms both an existing Aho-Corasick Cell BE variant and traditional regular expression implementation on x86.

УДК 004.056.53

И. А. Лубкин, К. В. Якименко

ОБЗОР МЕТОДОВ ЗАЩИТЫ ПРОГРАММ И ИХ ПРЕОДОЛЕНИЯ

В статье приведен обзор методов защиты программ от несанкционированного использования и модификации. Приведены методы атак на технологии защиты.

В настоящее время большую актуальность получила проблема защиты авторских прав. В сети Internet можно найти множество так называемых «взломанных» программ, система защиты от незаконного использования (далее – СЗНИ) которых была отключена либо изменена таким образом, что это позволяет использовать программу неправомочно. Естественной ответной мерой в такой ситуации является совершенствование СЗНИ программ.

Зачастую авторы СЗНИ в качестве обоснования стойкости своих разработок используют свой авторитет, указания используемых стойких (с криптографической точки зрения) алгоритмов и технологий противодействия исследованию и модификации программ. Упускается момент корректности реализации и использования механизмов защиты. Между тем известно множество случаев, когда атакующим удавалось преодолеть качественно спроектированные системы защиты вследствие некорректного их использования.

В данной статье приведен обзор существующих методов защиты программ предназначенных для работы в ОС Microsoft Windows NT от несанкционированного использования и модификации. Также заложена основа для дальнейшего исследования СЗНИ программ с целью получения оценки сложности их преодоления.

В ходе подготовки статьи рассмотрено более 40 примеров атак на СЗНИ программ. На основании этого осуществлена попытка обобщения общедоступной информации о системах защиты и способах их преодоления.

Не рассматривается ситуация, когда атакующий на основании анализа алгоритмов проверки имеет возможность сформировать поддельную корректную информацию о правомерности использования. Такая ситуация соответствует использованию криптографически слабых алгоритмов.

Актуальность данной работы в том, что формализация процесса преодоления СЗНИ позволит выявить слабые стороны систем защит и на этом основании усовершенствовать существующие СЗНИ. Большинство работ в рассмотренных авторами открытых источниках являются описательными, а рекомендации носят рецептурный характер.

Опишем рассматриваемую модель преодоления системы защиты. Пусть могут быть выполнены все функции защищаемой программы. Причина данного условия в том, что злоумышленник тем или иным способом может заполучить полнофункциональную копию программы. Обратное предположение наивно и приводит к потенциальному снижению безопасности.

Вследствие того, что процессор ЭВМ может выполнить программу только в открытом виде, то при любой организации защиты существует возможность получить полный перечень выполненных процессором инструкций и за конечное время преодолеть систему защиты. При использовании для защиты технологии виртуальных машин код самой виртуальной машины выполняется процессором. А это значит, что за конечное время можно получить описание набора команд виртуального процессора. Если мы рассмотрим выполнение защищенной части программы относительно виртуального процессора, то мы приходим к описанному ранее случаю, когда защищаемая программа должна быть выполнена в открытом виде. Следует вывод, что вместо вопроса о возможности преодоления системы защиты ставится вопрос о времени и экономических затратах такого преодоления.

Процесс преодоления систем защиты можно разделить на две компоненты – методологическую (т.е. использование неких стандартных путей решения, которые позволяют за конечное время добиться желаемого результата) и творческую (трудно формализуемая компонента, связанная с использованием злоумышленником своего предшествующего опыта и догадок для формирования эффективного способа преодоления системы защиты). Наиболее просто оценивать методологическую компоненту, но полученные оценки характеризуют только верхнюю границу времени и затрат преодоления системы защиты. В первую очередь в статье будет рассматриваться методологическая компонента атак на систему защиты.

Цель работы – совершенствование систем защит программ от неправомерного использования.

Исходя из этого ставятся задачи:

1. Качественный анализ существующих современных методов защиты.
2. Качественный анализ существующих методов преодоления систем защиты
3. Формализовать процесс преодоления систем защиты.
4. Сформировать методику оценки стойкости существующих систем защит программ от несанкционированного использования.
5. Выдача рекомендаций по повышению стойкости защит.

В статье рассматривается решение 1 – 2 задач.

Будем исходить из следующих предположений о возможностях атакующего:

- имеет максимально возможные права в системе;
- умеет и при необходимости пользуется всеми доступными наборами программ для исследования и преодоления систем защиты;
- владеет навыками программирования и при необходимости может разрабатывать собственные средства исследования и преодоления систем защиты;
- имеет общие представления о используемом методе защиты;
- зачастую разработчиком программы ставится условие запуска защищенной программы (в том числе и атакующим) с правами администратора системы, а также включением ее фрагментов в ядро системы. Зачастую данное условие повышает уязвимость и нестабильность системы в целом и не всегда может быть выполнено.

Качественный анализ методов защиты и их преодоления

СЗНИ решает три основные задачи: проверка правомерности использования, противодействие исследованию и защита от изменения алгоритмов работы программы. Рассмотрим, как решаются эти задачи и какие атаки возможны на эти системы.

Типовым решением задачи установления правомерности использования является проверка некой ключевой информации (часто называемой «ключом», «серийным номером») на соответствие некоторым критериям. Зачастую ключевая информация после преобразования сравнивается с содержащимся в программе эталоном. Иногда ключевая информации связана с аппаратным обеспечением ЭВМ, системным временем или является ключом расшифрования для фрагментов программы. То есть полноценная работа программы без ключевой информации или без атаки на систему защиты невозможна.

В работе предлагается следующая классификация методов решения задачи защиты от исследования и модификации:

1. Статическая защита, т.е. противодействующая атакам до этапа выполнения.

1.1 Усложнение структуры программы для затруднения автоматизированного исследования. Для преодоления применяется отладка. Если для незапущенной программы сложно указать, как будет происходить выполнение в динамике, то при пошаговом

выполнении появляется возможность получить исчерпывающие сведения о работе программы.

1.2 Изменение системы команд, из которых состоит программа для невозможности прямого исследования (технология виртуальной машины).

При преодолении защиты, основанной на технологии виртуальной машины, первым этапом является сбор сведений о системе команд виртуального процессора. Для этого используется отладка и мониторы обращений к операционной системе. После получения сведений о командах виртуальной машины осуществляется исследование защищенной части программы с дальнейшей модификацией. Данная технология превосходит по стойкости 1.1, так как анализ команд виртуальной машины трудно поддается оптимизации и делает маловероятным преобразование программы до исходного вида. Возможным выходом является извлечение кода виртуальной машины из системы защиты с дальнейшим удалением самой СЗНИ.

2. Динамическая защита (взаимодействующая с окружением программы при выполнении).

2.1 Основанная на использовании сервисов операционной системы

Так как возможное количество пар «запрос-ответ» к операционной системе конечно и невелико, то возможно за сравнительно небольшое время написать программное средство, которое будет подменять ответы операционной системы на запросы защищенной программы. При этом модификации будет подвергаться операционная система, а не защищенная программа.

2.2 Операции с адресным пространством программы. Использование данного принципа затрудняет наиболее распространенный метод атаки через модификацию программы.

2.2.1 Операции чтения (используется при проверке целостности участков памяти).

2.2.2 Операции записи (основа для самомодифицирующихся кодов, кодогенераторов, модулей шифрования).

При активной модификации системой защиты ВАП программы, которое включает в себя сам образ, системные библиотеки и данные, атака на СЗНИ в незапущенном состоянии потребует значительных усилий и времени для достижения результата. Это вызвано тем, что эмулирующие отладчики работают значительно медленнее реального процессора и не всегда корректно эмулируют отклики операционной системы [1. с. 140].

Данный принцип защиты используется в технологии на основании шифрования («крипторы») и самомодифицирующихся кодов (СМК). Отличие двух технологий в том, что после расшифровки фрагменты программы представлены в незащищенном виде, тогда как СМК являются трудно отделяемой частью программы, т.к. программа формируется на этапе выполнения. Серьезной проблемой крипторов является необходимость наличия ключа для расшифровки в операционной системе на момент выполнения программы. Сложности с использованием СМК вызваны трудностью проектирования использующих их систем защит.

При атаках на динамическую защиту аналогично атаке на (1.2) действиям по снятию СЗНИ предшествует длительная фаза (более половины от затрачиваемого на взлом времени) исследования.

Первым этапом процесса преодоления СЗПИ можно выделить пассивную атаку – сбор максимально возможного объема информации об атакуемом программном средстве. В частности, анализируется информация, содержащаяся в образе программы (данные, отладочная информация, секции импорта и экспорта).

В ходе второго этапа происходит выявление кода СЗНИ. Типовым способом обнаружения является поиск данных и функций ОС, используемых в ходе работы защиты (например, строк, выводимых в случае неправомерного использования программы). На основании выясненных адресов осуществляется переход к участкам программы, использующих эти данные или функции.

Не менее эффективным является поиск СЗНИ на основании анализа стека программы при использовании обращений к операционной системе. Это обусловлено тем, что системные функции и запросы однотипны и существуют эффективные методы отслеживания их использования.

Завершающим этапом является для преодоления большинства «навесных» защит является снятие слепка памяти («дампа») в тот момент, когда программа уже расшифрована или распакована. После этого формируется образ программы уже без системы защиты.

Обычно подразумевается, что атакующий будет пытаться для зашифрованной программы внести изменения именно в зашифрованный текст. Типовой является ситуация, когда цель атакующего – расшифровать программу и только потом вносить изменения.

В результате может быть сформирована программа для автоматического или автоматизированного преодоления защиты. В противном случае манипуляции осуществляются вручную. Данная технология защиты требует от атакующего длительного и алгоритмически трудного анализа, что делает ее предпочтительной для использования. Какой либо унифицированной методики преодоления не существует.

Обзор технологий защиты

Можно выделить следующие технологии защиты. Каждая технология может основываться на нескольких принципах защиты (указаны в скобках). В силу ограниченности объема статьи не приводятся нюансы работы систем защиты и атак на них.

Защита от дизассемблирования. Предназначена для затруднения анализа алгоритмов защиты человеком.

- Нестандартный формат программы (1.1).
- Использование технологии виртуальных машин (1.2).
- Скрытие данных, используемых системой защиты программы (2.2.1).
- Формирование эффективного кода (т.е. такого, который будет выполнен процессором) программы в процессе работы (2.2.2) [2. с. 45].

Защита от отладки. Варианты реализации:

- Обнаружение конкретных программ-отладчиков. Осуществляется поиск следов работы отладчика в операционной системе (2.1). Проверка выполняется на конечное и, обычно, небольшое количество показателей наличия отладчиков. Состав проверяемых показателей не изменяется со временем.
- Противодействие отладке на основании особенностей операционной системы (2.1).
- Выявление факта отладки программы на основании на основании анализа виртуального адресного пространства программы (ВАП) (2.2.1);
- Противодействие процессу отладки программы с использованием особенностей аппаратного обеспечения. Данная технология является нестабильной вследствие регулярного изменения аппаратной составляющей ПЭВМ [3. с. 267].
- Защита от эмулирующих отладчиков. Основана на выявлении разности поведения реальной и виртуальной среды. Решается посредством динамической защиты (2).

Зачастую способы преодоления защит программ основаны на поиске уязвимостей и ошибок в работе алгоритма защиты, а не на атаках на конкретные технологии. Именно эта особенность приводит к появлению непредсказуемой, «творческой» составляющей преодоления защиты, т.к. в случае корректного проектирования системы защиты и реализации защитных механизмов время преодоления будет определяться скоростью изучения исполнимого кода программы.

В качестве примера рассмотрим ситуацию, когда разработчик программы построил защиту на проверке возвращаемого функцией значения и не добавил в программу средств

контроля целостности. В такой ситуации преодоление будет сводиться к модификации программы так, чтобы проверяющая функция всегда возвращала значение, соответствующее состоянию зарегистрированной программы.

В случае использования криптографических методов защиты кроме стойкости алгоритма необходимо также рассматривать протокол и реализацию. Например, вследствие нахождения способа поиска коллизий для алгоритма MD5 ряд защит, основанных на сравнении хеш-сверток ключа с неким эталоном перестал быть безопасным. При этом никаких модификаций защищенной программы не требуется.

Представляются разумными следующие общие рекомендации для повышения стойкости:

- СЗНИ не должна быть статична. Наиболее эффективными средствами защиты являются виртуальные машины и защиты, активно модифицирующие память.
- СЗНИ должна быть распределена по программе, желательно – равномерно.
- «Развязка» по времени и пространству проверки и действий, выполняемых в результате проверки.
- СЗНИ не должна использовать тривиальные алгоритмы преобразования данных.
- СЗНИ не должна строиться на основании предположений об используемых средствах атак, архитектурах ЭВМ и операционных системах.
- Защищаемая программа не должна присутствовать в памяти в виде, пригодном для снятия копии с памяти программы.

Выводы

В статье произведена классификация СЗНИ и приведены общие методы их преодоления. Приведены общие рекомендации по построению систем защиты.

В дальнейшем планируется рассмотреть «творческую» компоненту атак на систему защиты и формализовать процесс преодоления систем защит.

Библиографический список

1. Касперски, К. Техника и философия хакерских атак / К. Касперски. – М.: СОЛОН - Р, 2004 г. – 272 с.

2. Пирогов В.Ю. Ассемблер и дизассемблирование.— СПб.:БХВ-Петербург, 2006.— 464с.: ил.

3. Бурдаев О.В., Иванов М.А., Тетерин И.И. Ассемблер в задачах защиты информации / Под ред. И. Ю. Жукова — М.: КУДИЦ-ОБРАЗ, 2002. — 320с.

УДК 681.322

А.Н. Мироненко, С.В. Белим

ВЫЯВЛЕНИЕ СПАМ-СООБЩЕНИЙ В ПОТОКЕ ЭЛЕКТРОННОЙ ПОЧТЫ

Разработан алгоритм и реализована система фильтрации почтовых сообщений на основе двухслойной нейронной сети. Проведено исследование влияния величины входного слоя нейронов и функции отклика на эффективность определения спам-сообщений.

В настоящее время проблема нежелательных массовых рассылок является наиболее актуальной в связи с возросшей долей спама в почтовом трафике. По данным «Лаборатории Касперского», в апреле 2009 года доля спама составила в среднем 83,4%.

В данной работе реализован модуль фильтрации почтовых сообщений на основе двухслойной сети формальных нейронов (рис.1).

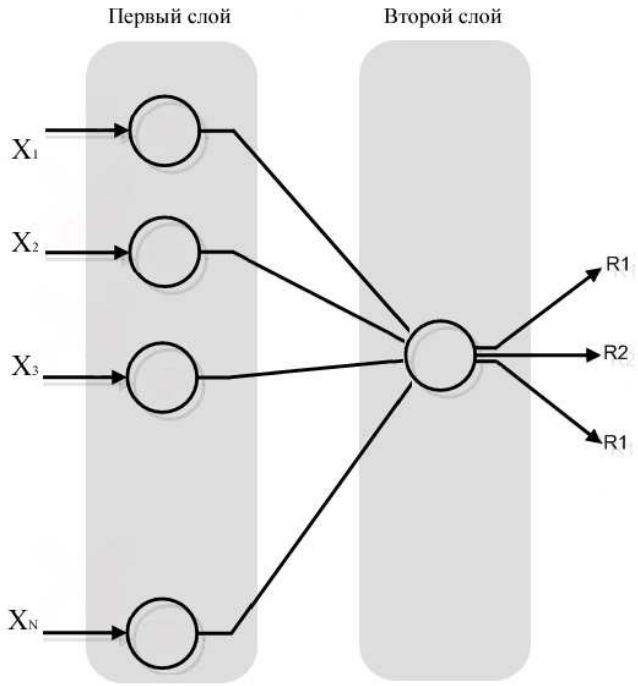

Рис.1

Сам процесс фильтрации, при этом, производится по содержимому сообщения. Первичная обработка письма состоит в выборе N наиболее часто встречающихся в нем слов. Величина N является константой системы и выбирается на основе компьютерного эксперимента до начала построения нейронной сети. А именно, первоначально при увеличении N эффективность фильтрации возрастает, но при достижении некоторого порогового значения меняется слабо. В качестве рабочей величины N было выбрано значение близкое к пороговому.

Первый слой нейронной сети содержит N нейронов, на входные синапсы которых подаются слова и частота их встречаемости в обрабатываемом сообщении. Каждый нейрон производит сравнение частоты встречаемости данного слова с табличным значением частоты встречаемости этого слова в спам-сообщениях и частотой встречаемости в легитимных сообщениях и вырабатывает число в интервале от 0 до 1, показывающее вероятность признания данного сообщения спамом. Все выходные сигналы подаются на вход второго слоя, состоящего из одного нейрона, который принимает одно из трех решений: сообщение является спамом (R1), сообщение не является спамом (R2), невозможно определить является ли сообщение спамом или нет(R3).

Математически функционирование нейронной сети описывается следующим образом:

$x_1,...,x_N$ – значения, поступающие на входы (синапсы) нейронов первого слоя сети.

Состояние нейрона определяется по формуле:

$$W_i = {(x_i k_i)}/{A_i}, \quad (1)$$

где x_i– значение i-го входа нейрона, k_i - количество, раз слово встречалось в предыдущих сообщениях (табличное значение), A_i – некоторый коэффициент, так же хранящийся во внутренней таблице сети. Коэффициент будет увеличиваться, если сообщение будет признанно легитимным.

Полученное значение W_i преобразуется в выходной сигнал, функцией активации нейрона F:

$$y = F(W_i). \quad (2)$$

В качестве функции активации используется логистическая или сигмоидальная функция, показанная на рис. 2. Эта функция математически выражается как:

$$y = F\left(W_i\right) = \frac{1}{1+e^{W}}. \quad (3)$$

Выбор данного вида функции определяют следующие ее ценные свойства:

1. монотонность и дифференцируемость на всей оси абсцисс;
2. простое выражение для ее производной.

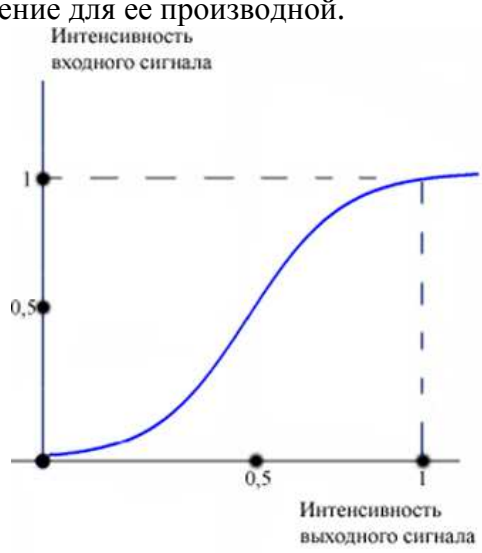

Рис. 2

На втором слое сети находиться лишь один нейрон, на вход которого поступают сигналы y_i, i =1..N от нейронов первого слоя. Они преобразуются по формуле:

$$S = \sum_{i=1}^{N} y_i \ , \quad (4)$$

где yi– значение i-го входа нейрона.

В качестве функции активации, так же как и на первом слое, используется логистическая или сигмоидальная функция, показанная на рис. 2.

$$y = F\left(S\right) = \frac{1}{1+e^{s}}. \quad (5)$$

На этом слое принимается решение насколько уверенно можно принять решение, о принадлежности сообщения к спаму. Решение принемаеться исходя из полученного числа, лежащего в интервале от 0 до 1. Чем ближе получившееся число к одному из этих значений, тем с большей уверенностью можно сказать является сообщение спамом или нет.

Формирование внутренней таблицы нейронной сети осуществляется в два этапа. Первоначально производится обучение с учителем. То есть первые N_0 сообщений классифицирует пользователь. В дальнейшем применяется смешанное обучение. Если сообщение попало в категорию R1 или R2, то соответствующие поправки в таблицу вносятся автоматически. Для писем из категории R3 решение принимает пользователь, и, на основе его решения вносятся изменения во внутреннюю таблицу.

Библиографический список

1. Уоссермен Ф. Нейрокомпьютерная техника: теория и практика. — М.: Мир, 1992.

2. С.Короткий Нейронные сети: основные положения, 1996г. // http://www.gotai.net
3. Андреев А.М. Автоматическая классификация текстовых документов с использованием нейросетевых алгоритмов и семантического анализа / Андреев А.М., Березкин Д.В., Морозов В.В., Симаков К.В.// http://www.inteltec.ru

A.N. Mironenko, S.V. Belim

SPAM DETECTION IN ELECTRONIC MAIL FLOW

The algorithm is developed and mail messages filtering system on the basis of a two-layer neural network is realised. Research of influence of an entry layer neurons value and functions of the response to efficiency spams-messages definition is conducted.

УДК 004.056

А.П. Никитин, С.С. Валеев, В.В. Озеров

СИСТЕМА ОГРАНИЧЕНИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНТЕРНЕТ-САЙТАМ

В настоящее время все больше организаций используют ресурсы Интернета в работе. На некоторых сайта содержится программы, способные привести, к разглашению, искажению или уничтожению служебной информации. Существующие способы классификации Интернет-сайтов не обладают достаточной гибкостью настройки и необходимой точностью классификации. Предлагается представлять текстовое содержимое запрашиваемой страницы в виде семантического графа, частично отражающего семантику. Для классификации текстового фрагмента предлагается использовать нейросетевой ассоциатор, обладающий большой скоростью обучения.

В связи с повсеместным распространением дешевого широкополосного доступа в Интернет, всё больше организаций используют его в работе. Большой популярностью пользуются следующие ресурсы:

- электронная почта;
- системы обмена мгновенными сообщениями (ICQ, Jabber, MSN, Google-Talk, Mail.Ru-Агент, Yandex-Online и др.);
- новостные ленты;
- всемирная паутина (World Wide Web).

Часто сотрудники организаций в рабочее время посещают Интернет-сайты, содержащие следующие нежелательные материалы:

- развлекательные материалы;
- пиратское программное обеспечение;
- нелицензионные аудио и видео материалы;
- эротические и порнографические материалы.

Подобные действия сотрудников могут привести к следующим негативным для организации последствиям:

- снижение продуктивность их работы;
- уменьшение пропускной способности канала связи организации с Интернет-провайдером, что может привести к снижению доступности информации, расположенной в сети Интернет и необходимой другим сотрудника;
- проникновения на рабочую станцию, а затем и на другие узлы корпоративной локальной вычислительной сети компьютерных вирусов, сетевых червей и троянских программ, что может служить причиной несанкционированного ознакомления злоумышленников с конфиденциальной информацией, а также к искажению или уничтожения служебной информации.

Соответственно встаёт задача ограничения перечня Интернет-сайтов, доступных сотрудникам с их рабочих мест.

Наиболее простым методом ограничения доступа сотрудников организации к Интернет-сайтам является фильтрация по адресам Интернет-сайтов (URL). Некоторые компании предлагают доступ к своим базам категорий Интернет-сайтов, как платным – например, ISS Orange Web Filter или SurfControl, так и бесплатным – например, Yahoo! SafeSearch. Администратор безопасности локальной вычислительной сети организации может иметь возможность вручную вносить в корпоративную базу данных адреса конкретных нежелательных Интернет-сайтов, например http://www.rapidshare.com или http://www.udaff.com, а также слова, встречающие в адресах нежелательных Интернет-сайтов, например adult, porno, crack, keygen. Однако создатели подобных сайтов, заинтересованные в увеличении показа рекламы, для привлечения посетителей создают зеркала основных сайтов, которые не сразу попадают в базы данных. Преимуществом фильтрации по адресам Интернет-сайтов является блокировка доступа сотрудника организации к сайту до его скачивания.

Достаточно большую группу методов ограничения доступа сотрудников организации к Интернет-сайтам образуют методы контентной фильтрации или фильтрации по содержимому. Данные методы потребляют больше аппаратных ресурсов системы ограничения доступа, они сложнее в реализации, но позволяют фильтровать вновь созданные Интернет-сайты. Недостатком методов контентной категоризации Интернет-сайтов является необходимость загрузки содержимого страницы, запрашиваемой сотрудником организации для анализа ее содержимого и определения категории Интернет-сайта. Использование proxy-серверов, работающих по зашифрованному протоколу HTTP Secure, делает контентную фильтрацию бесполезной, поскольку система ограничения доступа сотрудников к Интернет-сайтам может фиксировать только факт доступа определенного сотрудника к неизвестному Интернет-сайту.

Фильтрация по ключевым словам является простым, но неточным методом ограничения доступа сотрудников к Интернет-сайтам. Байесовский классификатор позволяет точнее определять категорию страницы, запрашиваемой пользователем. По сравнению с фильтрацией по ключевым словам, данный подход требует ещё больше вычислительных ресурсов, он ещё сложнее в реализации. Недостатком Байесовской фильтрации является ориентация на английский язык, в котором значение слова зависит от места, занимаемое этим словом в рамках предложения. В русском же языке значения слов в зависимости от их взаимного расположения в предложении и от контекста использования.

Предлагается в качестве упрощенной модели текстового содержимого страницы, запрашиваемой сотрудником организации, использовать представление минимальной семантической единицы – предложения – в виде семантического графа. Данная модель позволяет быстро построить простую структуру, частично отражающую семантику текстового содержимого страницы Интернет-сайта.

На первом этапе анализа текстового содержимого страницы, запрашиваемой сотрудником организации, из него формируется множество $F = \{f_k\}$, где f_k – заданная для системы ограничения доступа сотрудников к Интернет-сайтам минимальная семантическая структура, $i=1\ldots m$, при этом из структуры удаляются избыточные элементы. В результате структура f_k может быть представлена в виде семантического графа S_k, определяющего связь L лексем V в f_k. При оценке силы связи между лексемами учитывается лексикографический порядок в f_k. После обработки всего текстового содержимого получаем семантический граф $G = < V, L > = \bigcup_1^n V_k$ - упрощенную семантическую модель текстового фрагмента.

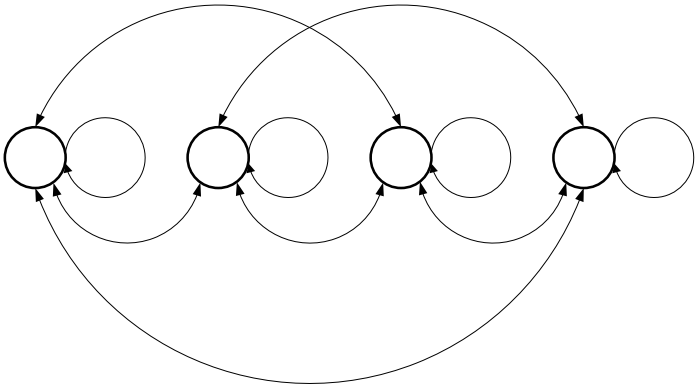

Рисунок 1 – Семантический граф

Далее граф *G* представляется матрицей смежности *Z*, представляющей собой семантическую матрицу. Матрица *Z* имеет четко выраженную структуру, что позволяет использовать ее для повышения эффективности процедуры запрошенной при решении задачи фильтрации.

Таблица 1

Пример матрицы смежности

	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8	V_9	V_{10}	V_{11}	V_{12}	V_{13}	V_{14}	V_{15}
V_1	***4***	***3***	***1***	0	***2***	0	***2***	0	0	0	***1***	0	***1***	0	0
V_2	***3***	***6***	0	***3***	0	0	***5***	***4***	0	0	***5***	0	0	***2***	0
V_3	***1***	0	***5***	0	***4***	0	0	0	0	0	***4***	0	0	0	0
V_4	0	***3***	0	***4***	***3***	0	***3***	0	***3***	***3***	***2***	***3***	***2***	***1***	0
V_5	***2***	0	***4***	***3***	***6***	0	0	***3***	0	0	***5***	***3***	0	0	0
V_6	0	0	0	0	0	***7***	0	0	0	***3***	0	0	0	***2***	0
V_7	***2***	***5***	0	***3***	0	0	***6***	***5***	***3***	0	***1***	0	0	0	***3***
V_8	0	***4***	0	0	***3***	0	***5***	9	***3***	0	***6***	0	***4***	0	0
V_9	0	0	0	***3***	0	0	***3***	***3***	***4***	0	0	0	0	***3***	***2***
V_{10}	0	0	0	***3***	0	***3***	0	0	0	***5***	***4***	***2***	0	0	0
V_{11}	***1***	***5***	***4***	***2***	***5***	0	***1***	***6***	0	***4***	***7***	0	***5***	***2***	0
V_{12}	0	0	0	***3***	***3***	0	0	0	0	***2***	0	***4***	0	0	***3***
V_{13}	***1***	0	0	***2***	0	0	0	***4***	0	0	***5***	0	***6***	0	***3***
V_{14}	0	***2***	0	***1***	0	***2***	0	0	***3***	0	***2***	0	0	***4***	0
V_{15}	0	0	0	0	0	0	***3***	0	***2***	0	0	***3***	***3***	0	***4***

Для классификации текстового содержимого страниц Интернет-сайтов был выбран линейный ассоциатор, обладающей большой скоростью работы. Предложенный способ включает в себя следующие этапы:

1. Построение матрицы *M* весов анализируемого текстового содержимого страницы, запрашиваемой сотрудником организации.

$$M = \begin{bmatrix} m_{2,3} & m_{2,5} & m_{2,9} \\ m_{6,3} & m_{6,5} & m_{6,9} \\ m_{7,3} & m_{7,5} & m_{7,9} \end{bmatrix}.$$

2. Построение сжатой матрицы весов текстовых фрагментов нежелательного *S'* и желательного *H'* Интернет-сайтов путем удаления из матрицы весов текстовых фрагментов нежелательного *S* и текстовых фрагментов желательного *H* Интернет-сайта лексем, отсутствующих в анализируемом текстовом содержимом страницы, запрошенной пользователем организации.

$$S' = \begin{bmatrix} s_{2,3} & s_{2,5} & s_{2,9} \\ s_{6,3} & s_{6,5} & s_{6,9} \\ s_{7,3} & s_{7,5} & s_{7,9} \end{bmatrix}, \quad H' = \begin{bmatrix} h_{2,3} & h_{2,5} & h_{2,9} \\ h_{6,3} & h_{6,5} & h_{6,9} \\ h_{7,3} & h_{7,5} & h_{7,9} \end{bmatrix},$$

$$S = \begin{bmatrix} s_{1,1} & s_{1,2} & \dots & s_{1,n} \\ s_{2,1} & s_{2,2} & \dots & s_{2,n} \\ \dots & \dots & \dots & \dots \\ s_{n,1} & s_{n,2} & \dots & s_{n,n} \end{bmatrix}, \quad H = \begin{bmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,l} \\ h_{2,1} & h_{2,2} & \dots & h_{2,l} \\ \dots & \dots & \dots & \dots \\ h_{l,1} & h_{l,2} & \dots & h_{l,l} \end{bmatrix},$$

3. Формирование вектора V_S, составленного из элементов сжатой весовой матрицы текстового содержимого нежелательного, вектора V_H, составленного из элементов сжатой весовой матрицы текстового содержимого желательного Интернет-сайта и вектора V_M, составленного из элементов весовой матрицы анализируемого текстового содержимого страницы, к которой сотрудник организации пытается получить доступ.

$$V_S = \begin{bmatrix} s_{2,3} \\ s_{2,5} \\ s_{2,9} \\ s_{6,3} \\ s_{6,5} \\ s_{6,9} \\ s_{7,3} \\ s_{7,5} \\ s_{7,9} \end{bmatrix}, \quad V_H = \begin{bmatrix} h_{2,3} \\ h_{2,5} \\ h_{2,9} \\ h_{6,3} \\ h_{6,5} \\ h_{6,9} \\ h_{7,3} \\ h_{7,5} \\ h_{7,9} \end{bmatrix}, \quad V_M = \begin{bmatrix} m_{2,3} \\ m_{2,5} \\ m_{2,9} \\ m_{6,3} \\ m_{6,5} \\ m_{6,9} \\ m_{7,3} \\ m_{7,5} \\ m_{7,9} \end{bmatrix}$$

4. Формирование матриц X и Y для обучения линейного ассоциатора.

$$X = \begin{bmatrix} s_{2,3}\, h_{2,3} \\ s_{2,5}\, h_{2,5} \\ s_{2,9}\, h_{2,9} \\ s_{6,3}\, h_{6,3} \\ s_{6,5}\, h_{6,5} \\ s_{6,9}\, h_{6,9} \\ s_{7,3}\, h_{7,3} \\ s_{7,5}\, h_{7,5} \\ s_{7,9}\, h_{7,9} \end{bmatrix}, \quad Y = \begin{bmatrix} y_S \\ y_H \end{bmatrix}$$

5. Настройка весов W линейного ассоциатора.

$$W = Y \times X^{+} = Y \times \left(X^{T} \times X \right)^{-1} \times X^{T}$$

6. Определение класса анализируемого текстового фрагмента.

$$y = W \times V_M$$

Результаты сравнительного анализа классификации текстовых фрагментов показали,

что практически во всех случаях разработанный метод категоризации точнее определяет категорию Интернет-сайта, доступ на который попытался получить сотрудник организации, чем байесовский классификатор.

A.P.Nikitin, S.S.Valeev, V.V. Ozerov

SYSTEM OF ACCESS LIMITATION OF USERS TO INTERNET SITES

Many organizations use Internet resources in job now. On some site contains programs which can cause disclosure, distortions or to destruction of the confidential information. Existing discriminatory analyses of Internet sites do not possess flexibility of customization and necessary accuracy of classification. It is offered to represent text contents of required page in the form of the semantic count partially mirroring semantics. For classification of a text fragment it is offered to use the neural qualifier possessing in the big speed of training.

УДК 004.056

А.П. Никитин, В.В. Озеров

ИЕРАРХИЧЕСКОЕ ФОРМИРОВАНИЕ БАЗ ЗНАНИЙ СИСТЕМЫ СПАМ-ФИЛЬТРАЦИИ

В настоящее время остро стоит проблема спама. Существующие архитектуры используемых систем спам-фильтрации обладают существенными недостатками. Применяемы подходы к формированию баз знаний систем спам-фильтрации не позволяют в полной мере учитывать области интересов всех пользователей. Предлагается новый подход к формированию базы знаний системы спам-фильтрации, вобравший в себя основные преимущества существующих подходов.

В Правилах оказания телематических услуг связи (Постановление Правительства Российской Федерации от 10.08.2007 № 575) отмечается, что оператор связи должен принимать меры для воспрепятствования распространению спама. Несмотря на использование различных систем спам-фильтрации, доля спама в почтовом трафике все еще достаточно высока. По мнению экспертов компании Microsoft, в 2009 году объём спама превысит отметку в 95% всего почтового трафика.

В ходе анализа архитектурных особенностей серверных систем спам-фильтрации (рис. 1 а) была выявлена их неспособность адаптации к области служебных интересов конкретного пользователя, что снижает точность классификации, в результате чего нарушается целостность информации, обрабатываемой системой электронной почтовой связи.

В ходе анализа архитектурных особенностей персональных систем спам-фильтрации (рис. 1 б) было выявлено, что необходимость раздельной настройки каждого спам-фильтра снижает размер и достоверность базы знаний системы спам-фильтрации, что негативно сказывается на точности классификации электронных писем, в результате чего также нарушается целостность информации, обрабатываемой системе электронной почтовой связи. Расположение персонального фильтра на компьютере конечного пользователя негативно сказывается на доступности информации, обрабатываемой системой электронной почтовой связи, в случае, если пропускной способности канала связи с Интернет-провайдером не хватит для своевременного скачивания электронных писем (например, если сотрудник организации проверяет корпоративный почтовый ящик, находясь дома или в командировке).

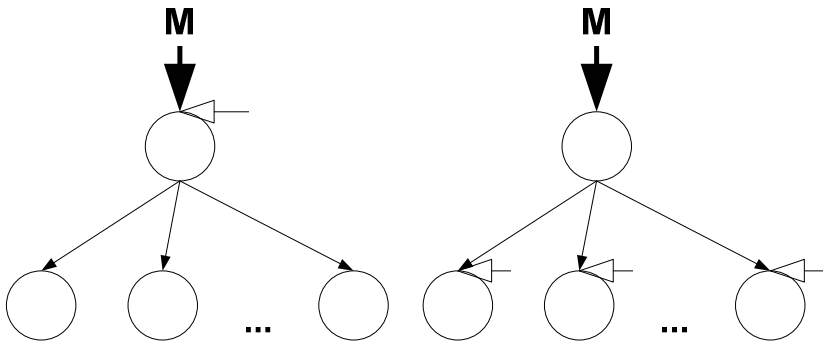

Рисунок 1 – Различные архитектуры систем фильтрации почтовых сообщений

Способы формирования баз знаний серверных систем спам-фильтрации подразделяются на три вида.

Простое пересечение, когда для формирования базы знаний используются электронные письма, помеченные как спам всеми пользователями. В этом случае база знаний получается достаточно маленькой, а вероятность попадания в неё ошибочно классифицированных электронных писем крайне мала. Данный способ можно выразить следующим образом:

$$B = b_1 \cap b_2 \cap ... \cap b_n = \bigcap_{k=1}^{n} b_k \ , \tag{1}$$

где B – база знаний организации; b_k – база знаний k-го пользователя; n – количество пользователей. Пример процедуры формирования базы знаний методом простого пересечения показан на рис. 2.

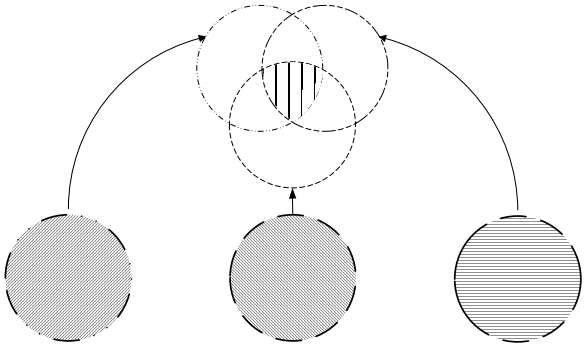

Рисунок 2 - Пример процедуры формирования базы знаний методом простого пересечения

Сложное пересечение, когда система спам-фильтрации принимает решение, включать ли письмо, помеченное пользователем как спам, в свою базу знаний, на основе рейтинга пользователя, который зависит количества писем, верно классифицированных данным пользователем с точки зрения других пользователей. В этом случае размер базы знаний увеличивается, как и вероятность попадания в неё неверно классифицированных электронных писем. В упрощенном виде, данный способ формирования базы знаний можно выразить следующим образом:

$$\begin{aligned} B = (b_1 \cap b_2) \cup (b_1 \cap b_3) \cup ... \cup (b_1 \cap b_n) \cup (b_2 \cap b_3) \cup ... \\ ... \cup (b_2 \cap b_n) \cup ... \cup (b_{n-1} \cap b_n) = \bigcup_{k=1,\, j=1}^{k=n,\, j=n,\, k \neq j} (b_k \cap b_j) \end{aligned} \tag{2}$$

Пример процедуры формирования базы знаний методом сложного пересечения показан на рис. 3.

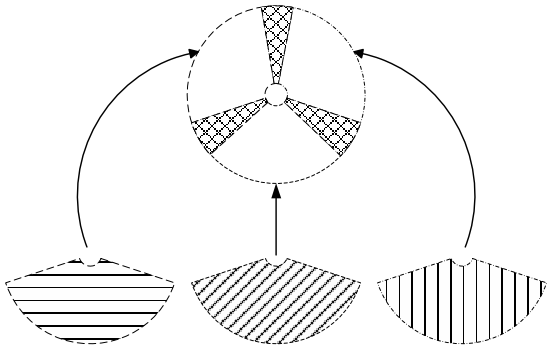

Рисунок 3 - Пример процедуры формирования базы знаний методом сложного пересечения

Объединение, когда для формирования базы знаний системы спам-фильтрации используются электронные письма, помеченные как спам хотя бы одним пользователем. В этом случае размер базы знаний резко увеличивается, однако в неё с большой долей вероятности могут попасть неверно классифицированные письма. Данный способ формирования базы знаний можно выразить следующим образом:

$$B = b_1 \cup b_2 \cup ... \cup b_n = \bigcup_{k=1}^{n} b_k \qquad (3)$$

Пример процедуры формирования базы знаний системы спам-фильтрации методом объединения показа на рис. 4.

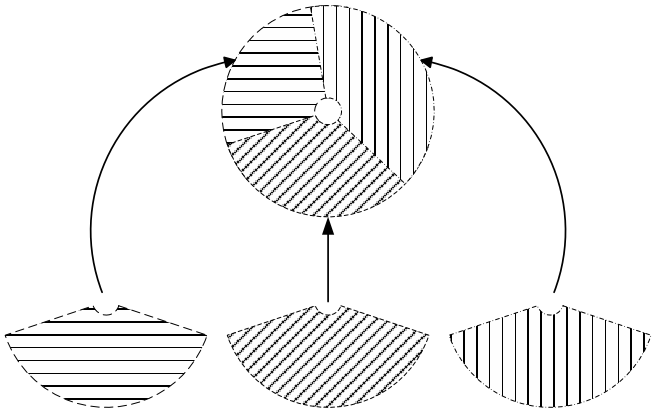

Рисунок 4 - Пример процедуры формирования базы знаний системы спам-фильтрации методом объединения

Предлагается процедура иерархического формирования базы знаний системы спам-фильтрации, объединяющая в себе все преимущества серверных и персональных систем. На каждом уровне используется собственная база знаний.

На нижнем уровне используется база знаний, сформированная из писем, классифицированных конечным пользователем.

На уровне отдела используется база знаний, сформированная из писем, классифицированных хотя бы одним пользователем. Письма, по-разному классифицированные разными пользователями, не вносятся в базу знаний. Учитывая, что области интересов пользователей одного отдела совпадают, данный подход позволяет строить более репрезентативную (по сравнению с нижним уровнем) базу знаний без повышения вероятности попадания в неё неверно классифицированных писем.

На верхнем уровне используется база знаний, сформированная из писем, одинаково классифицированных каждым отделом организации, что позволяет получить базу знаний, небольшую по размеру и с очень низкой вероятностью попадания в неё неверно классифицированных писем. Разработанный иерархический подход к формированию баз

знаний позволяет повысить целостность информации, обрабатываемой системой электронной почтовой связи за счет снижения уровня ошибок первого и второго рода. Данный способ формирования базы знаний можно представить следующим образом:

$$B_1 = b_{11} \cup b_{12} \cup ... \cup b_{1n} = \bigcup_{k=1}^{n} b_{1k} \ , \tag{4}$$

$$Base = B_1 \cap B_2 \cap ... \cap B_p = \bigcap_{k=1}^{p} B_k \ . \tag{5}$$

Учитывая (4) и (5) можно получить описание процедуры формирования БЗ:

$$Base = \left(b_{11} \cup b_{12} \cup ... \cup b_{1n}\right) \cap \left(b_{21} \cup b_{22} \cup ... \cup b_{2m}\right) \cap ... \cap \left(b_{p1} \cup b_{p2} \cup ... \cup b_{po}\right) = \\ = \bigcap_{k=1}^{p} \left(\bigcup_{j=1}^{r} b_{k,j} \right). \tag{6}$$

где p – количество отделов; n, m и l – количество сотрудников в первом, втором и p-ом отделе; b_{pl} – база знаний, сформированная l-ым сотрудником p-го отдела; B_k – база знаний уровня k-го отдела организации; *Base* – база знаний уровня организации.

Пример процедуры иерархического формирования базы знаний системы спам-фильтрации почтовых сообщений показан на рис. 5.

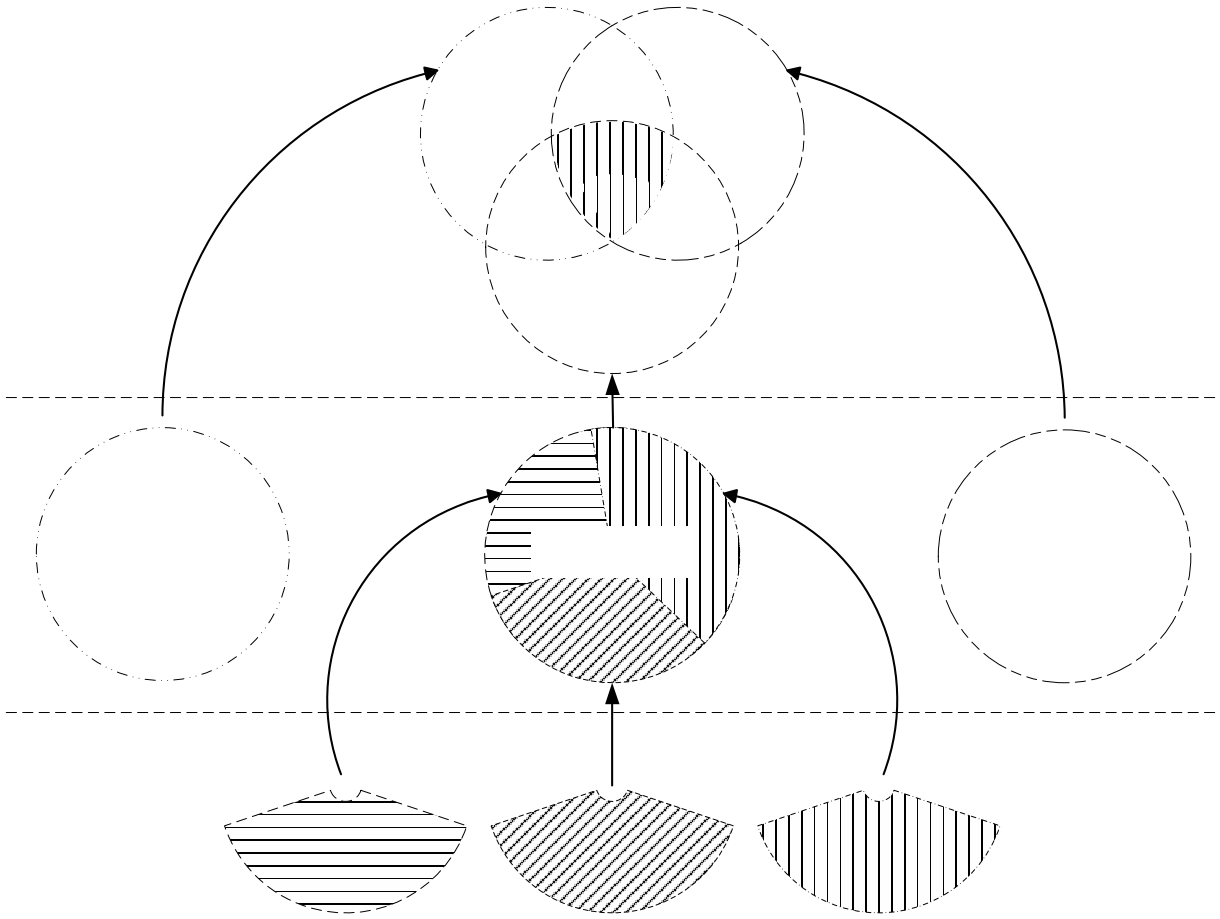

Рисунок 5 - Процедуры иерархического формирования базы знаний системы спам-фильтрации

Как показали результаты имитационное моделирование при переходе с классической

процедуры формирования базы знаний к разработанной иерархической процедуре, точность классификации электронных почтовых сообщений увеличилась на 3-4%.

A.P.Nikitin, V.V. Ozerov

HIERARCHICAL FORMATION OF KNOWLEDGE BASES OF SPAM-FILTRATION SYSTEM

The spam problem costs sharply now. Architecture of used systems of a spam-filtration possess essential lacks. Approaches to formation of knowledge bases of systems of a spam-filtration are applied do not allow to consider area of interests of all users to the full. The new approach to formation of the knowledge base of system of a spam-filtration which has incorporated the basic advantages of existing approaches, is offered.

УДК 65.012.810(075.8)

Ракицкий Ю.С., Белим С.В.

МОДЕЛИРОВАНИЕ РОЛЕВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ СО СТАНДАРТОМ СТО БР ИББС-1.0-2008

Рассматривается дополнение ролевой политики безопасности, в результате которого построенная политика безопасности будет удовлетворять требованиям стандарта СТО БР ИББС-1.0-2008

Введение

Анализ различных организационно-управленческих и организационно-технологических схем показывает, что, в реальной жизни сотрудники предприятий, учреждений выполняют определенные функциональные обязанности не от своего личного имени, а в рамках некоторой должности. Должность, которую можно трактовать как определенную роль, представляет некоторую абстрактную, точнее обобщенную сущность, выражающую определенный тип функций и тип положения работника (подчиненность, права и полномочия). Таким образом, в реальной жизни в большинстве организационно-технологических схем права и полномочия предоставляются конкретному сотруднику не лично (непосредственно), а через назначение его на определенную должность (роль), с которой он и получает некоторый типовой набор прав и полномочий. Ролевое разграничение доступа является развитием политики дискреционного разграничения доступа, при этом права доступа субъектов системы (т.е. сотрудников предприятия, занимающих определенную должность) на объекты с учетом специфики их применения, образуя роли.

Ярким примером описанных предприятий являются коммерческие банки. Учитывая законодательство в области банковской деятельности (ст. 26 «Банковская тайна» закона «О банках и банковской деятельности» и закон «О персональных данных»), проблема обеспечения информационной безопасности компьютерных систем в организациях банковской системы является весьма актуальной. Центральный Банк Российской Федерации (Банк России) выпустил серию документов, посвященных обеспечению информационной безопасности организаций банковской системы. Одним из таких документов является стандарт Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». Авторы данного стандарта предлагают при построении политики информационной безопасности определить и разграничить роли сотрудников банка.

Согласно пункту стандарта 7.2.1 «Роль – это заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом, например, сотрудником организации, и объектом, например, программно-аппаратным средством. Для эффективного выполнения целей организации и задач по управлению активами должны быть выделены и определены соответствующие роли персонала организации». Таким образом, в любой автоматизированной компьютерной системе предоставление доступа должно осуществляться в соответствии с ролевой моделью разграничения доступа.

Согласно пункту стандарта 7.2.3 «Не рекомендуется, чтобы одна персональная роль целиком отражала цель, например, включала все правила, требуемые для реализации бизнес-процесса. Совокупность правил, составляющих роли, не должна быть критичной для организации с точки зрения последствий успешного нападения на ее исполнителя. Не следует совмещать в одном лице (в любой комбинации) роли разработки, сопровождения, исполнения, администрирования или контроля, например, исполнителя и администратора, администратора и контролера или других комбинаций». Таким образом, выделяются роли исполнителей, контролеров, администраторов и сопровождения, которые должны в какой-либо комбинации присутствовать в любом процессе в каждой автоматизированной компьютерной системе.

Согласно пункту стандарта 7.2.4 «Роль должна быть обеспечена ресурсами, необходимыми и достаточными для ее исполнения». Следовательно, любая роль не должна содержать избыточных прав доступа в автоматизированной компьютерной системе, то есть не должна обладать доступом к объектам, которые не используются при исполнении данной роли. Например, сотрудник банка, оформляющий в автоматизированной системе заявки на выдачу кредита клиенту банка не должен иметь доступ к информации о принятии вкладов от населения, но при этом должен обладать правами доступа на просмотр и редактирование анкетных данных клиентов, подавших заявку на получение кредита.

Приведенные выше требования являются частью общих требований по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу. На основании этих требований можно сформулировать формальную модель ролевой политики безопасности, в соответствии со стандартом СТО БР ИББС-1.0-2008.

Формализация политики безопасности

Базовая модель ролевого разграничения доступа включает в себя следующие множества: U – множество пользователей, R – множество ролей, P - множество прав на работу в системе. Важную роль играет отображение PA: $R \to 2^P$, определяющее множество прав доступа для заданной роли, при этом для каждого $p \in P$ существует $r \in R$ такая что $p \in PA(r)$.

Для введения в модель контролирующих функций необходимо множество ролей R, которые в дальнейшем будем называть исполнительскими, дополнить множеством административных ролей ACR и множеством контролирующих ролей CR. При этом

$$R \cap ACR = \varnothing,\ ACR \cap CR = \varnothing,\ R \cap CR = \varnothing. \quad (1)$$

Также введем дополнительные множества: ACP – множество прав для административных ролей, CP – множество прав для контролирующих ролей. Множества P, CP и ACP также не имеют общих элементов. ACR осуществляют администрирование контролирующих ролей.

Для каждого права $p \in P$ должно быть определено множество контролирующих прав, обладание которыми необходимо для контроля над p. Введем соответствующее отображение

$$\text{Control\_right: } P \rightarrow 2^{CP} \quad (2)$$

при этом $\forall\, p \in P$ Control_right(p)$\neq\varnothing$.

Также для любой роли должен существовать набор, контролирующих ролей, осуществляющих контроль над ней. Введем отображение

$$\text{Control\_Role: } R \rightarrow 2^{CR}, \quad (3)$$

при этом $PA(r)=\{p_{i1},p_{i2},\ldots,p_{in}\} \Rightarrow PA(\text{Control\_Role}(r))=\cup\text{Control\_right}(p_{ij})$.

Определение: В системе выполняются функции контроля, если в любой момент времени для любого $p \in P$ существует $\{cp_{i1},cp_{i2},\ldots,cp_{in}\} \subseteq CP$ такое, что $\{cp_{i1},cp_{i2},\ldots,cp_{in}\} \subseteq$ Control_right(p), а для любой $r \in R$ существует $\{cr_{l1},cr_{l2},\ldots,cr_{lm}\} \subseteq CR$ такие, что $\{cr_{l1},cr_{l2},\ldots,cr_{lm}\} \subseteq$ Control_Role(r).

Аналогично, введем отображение

$$\text{Admin\_right: } CP \rightarrow 2^{ACP} \quad (4)$$

при этом $\forall\, p \in CP$ Admin_right(p)$\neq\varnothing$.

Введем отображение

$$\text{Admin\_Role: } CR \rightarrow 2^{ACR} \quad (5)$$

при этом $PA(cr)=\{cp_{i1}, cp_{i2},\ldots, cp_{in}\} \Rightarrow PA(\text{Admin\_Role}(ar))=\{ap_1, ap_2,\ldots, ap_m\}$.

Определение: В системе выполняются функции администрирования, если в любой момент времени для любого $cp \in CP$ существует $\{ap_{i1},ap_{i2},\ldots,ap_{in}\} \subseteq ACP$ такое, что $\{ap_{i1},ap_{i2},\ldots,ap_{in}\} \subseteq$ Admin_right(cp), а для любой $cr \in CR$ существует $\{ar_{l1},ar_{l2},\ldots,ar_{lm}\} \subseteq ACR$ такие, что $\{ar_{l1},ar_{l2},\ldots,ar_{lm}\} \subseteq$ Admin_Role(cr).

Аналогичным образом можно выделить в системе роли разработки и сопровождения.

Соответствие модели стандарту СТО БР ИББС-1.0-2008

Теперь покажем, что построенная модель соответствует требованиям стандарта СТО БР ИББС-1.0-2008.

Теорема. Построенная модель удовлетворяет требованиям стандарта СТО БР ИББС-1.0-2008.

Доказательство.

Для доказательства теоремы необходимо показать, что введенные отображения соответствуют требованиям стандарта, и, наоборот, для каждого требования стандарта существует соответствующее отображение. Как было показано в пункте 2, в стандарте ролевой политике безопасности посвящено три пункта.

Согласно пункту 7.2.1 разграничение доступа должно производиться по ролевому принципу, что очевидно выполняется.

Согласно пункту 7.2.3 должны существовать исполнительские, административные, контролирующие роли, а также роли сопровождения, которые не должны совмещаться в одном лице. Это задается соотношением (1).

Согласно пункту 7.2.4 любая роль должна обладать необходимыми и достаточными правами на свое исполнение, что задается соотношениями (2), (3), (4) и (5), согласно которым для любой роли существует контролирующая и административная роль, обладающая достаточными правами для исполнения своих функций. В то же время административная и контролирующая роли не обладают правами на исполнение других функций, что обозначено соотношением (1).

Теорема доказана.

Библиографический список

1. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации / А. А.Грушо, Е. Е.Тимонина. М: Издательство Агенства Яхтсмен, 1996.

2. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. М.: Горячая линия Телеком, 2000.

3. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности / А. Ю. Щербаков. М.: Издатель Молгачева С.В., 2001.

Rakitskij J.S., Belim S.V.

MODELLING OF THE ROLE SECURITY POLICY ACCORDING TO THE STANDARD СТО БР ИББС-1.0-2008

Addition of a role security policy in which result the constructed security policy will meet requirements of the standard СТО БР ИББС-1.0-2008 is considered

УДК 002.53

Е. Ю. Федорова, Т. А. Чалкин

РАЗРАБОТКА АЛГОРИТМА АВТОМАТИЧЕСКОЙ КЛАССИФИКАЦИИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Описывается алгоритм классификации электронных документов в области защиты информации, основанный на теоретико-множественном подходе к анализу ключевых слов документов.

Нормативная база является основой при создании любой системы защиты информации. Специалисту приходится просматривать большое количество различной документации при проектировании системы, что существенно затрудняет работу, занимает немало времени, а также может привести к неверному или же неполному подбору документации. Поэтому возникла необходимость классификации документов в области защиты информации по заданным параметрам в качестве помощи специалисту или проверки правильности его работы.

Объектом исследования настоящей работы является специальная нормативная документация по защите информации. Предметом исследования являются алгоритмы автоматической классификации электронных документов.

Разработка автоматизированных средств классификации массивов документов для специфических областей также необходима для дальнейшего развития систем поддержки принятия решений и экспертных систем, которые приносят существенную временную и экономическую выгоду менеджерам в процессе принятия решений.

Общее описание схемы классификации электронных нормативных документов в области защиты информации, проблемы и пути их решения представлены в статье [1].

В качестве продолжения исследования алгоритмов классификации предлагается использовать теоретико-множественный подход к анализу ключевых слов классифицируемых документов.

Постановка задачи

Пусть имеется глобальное множество ключевых слов $K = \{k_1, k_2, \dots, k_n\}$. Определим документ как объект, однозначно описываемый множеством его ключевых слов $K' \subset K, K' \neq \emptyset$. Множество всех возможных документов обозначим $D = \{K' \subset K\}$. Также определено глобальное множество классов документов $C = \{c_1, c_2, \dots, c_m\}$.

Дано «обучающее» множество документов $D_0 = \{d_1, d_2, \dots, d_k\}$, для каждого элемента $d_i \in D_0$ которого однозначно определен соответствующий ему класс $c_i \in C$, то есть задано (таблично) отображение $F_0: D_0 \to C$, причем для любого класса $c_i \in C$ существует хотя бы один документ из «обучающего» множества D_0, относящийся к этому классу: $\forall c \in C \; \exists d \in D_0: F_0(d) = c$.

Исходные данные можно представить в виде таблицы:

$$d_1 = K_1' = \{k_1^1, \dots, k_{n_1}^1\} \quad c_{i_1}$$
$$\vdots \qquad\qquad \vdots$$
$$d_k = K_k' = \{k_1^k, \dots, k_{n_k}^k\} \quad c_{i_k}$$

Пример

$K = \{\text{защита, информация, алгоритм, шифрование, программа, риск}\}$

$C = \{\text{общие документы, криптография}\}$

$d_1 = K_1' = \{\text{защита, алгоритм, шифрование}\}$ криптография

$d_2 = K_2' = \{\text{защита, информация, алгоритм}\}$ общие документы

$d_3 = K_3' = \{\text{защита, информация, программа}\}$ общие документы

Требуется: построить (аналитически или алгоритмически) отображение $F: D \to C$ (расширение отображения F_0), то есть правило, определяющее принцип отнесения документа к определенному классу на основе сведений о его ключевых словах. То есть правило F для документа с любым набором ключевых слов должно однозначно указывать соответствующий ему класс документов.

Базовое требование к отображению F: для любого $d_i \in D_0$ должно выполняться $F(d_i) = F_0(d_i)$, то есть расширение отображения не должно изменять исходного отображения F_0, иными словами, для «обучающего» множества искомое отображение F должно давать корректные (соответствующие изначально заданным) классы. Назовем отображение F, для которого это условие выполняется, состоятельным.

Пусть существует $k \in K$, такой что $\nexists d = K' \in D_0: k \in K'$. Иными словами, в глобальном множестве существует ключевое слово, которое не является ключевым ни для одного из документов «обучающего» множества. Тогда, очевидно, $F(K') = F(K' \backslash k)$ для любого $K' \subset K$, то есть добавление или удаление из глобального множества ключевых слов элемента, который не является ключевым ни для одного из документов «обучающего» множества, не влияет на результат классификации, так как она основывается только на данных о ключевых словах документов из «обучающего» множества.

Процедурой редукции глобального множества $K \to K^0$ назовем процедуру удаления из K всех таких ключевых слов, то есть $K^0 = \{k \in K: \exists d = K' \in D_0: k \in K'\}$.

В дальнейшем будем рассуждать исходя из того, что над множеством K проведена процедура редукции и строится отображение $F: D \to C$, где $D = \{K' \subset K^0\}$, то есть в документах в качестве ключевых присутствуют только те слова, которые встречаются в качестве ключевых в документах «обучающего» множества.

Для редуцированного множества K^0 справедливо $K^0 = \bigcup_{i=1}^{k} K_i'$, $K_i' \in D_0$, то есть множество ключевых слов есть объединение множеств ключевых слов документов «обучающего» множества.

Возможные подходы к построению алгоритма

Основываясь на приведенной выше теоретико-множественной интерпретации задачи, предлагается строить значение отображения $F(K')$ на основе значений мощности множеств $K' \cap K_i'$, где $K_i' \in D_0$. Иными словами, предлагается искать число ключевых слов, общих у документа, требующего классификации, и различных документов из «обучающего» множества.

Построить таким образом отображение F можно, например, следующим образом:

$$F(K') = c_j: \sum_{K_i' \in D_0: F_0(K_i') = c_j} |K' \cap K_i'| = \max_{c_j}$$

То есть в качестве класса для документа с множеством ключевых слов K' выбирается такой класс c_j, для которого число ключевых слов, общих у документов из «обучающего» множества, отнесенных к классу c_j, и данного документа, максимально.

Пример 1 (исходные данные см. в примере выше)

Пусть требуется классифицировать документ

$d = K' = \{\text{информация, шифрование, программа}\}$

Ищем мощности пересечений K' с K_1', K_2', K_3':

$K' \cap K_1' = \{\text{шифрование}\}$ $|K' \cap K_1'| = 1$

$K' \cap K_2' = \{\text{информация}\}$ $|K' \cap K_2'| = 1$

$K' \cap K_3' = \{\text{информация, программа}\}$ $|K' \cap K_3'| = 2$

Суммируем мощности по классам:

криптография $|K' \cap K_1'| = 1$

общие документы $|K' \cap K_2'| + |K' \cap K_3'| = 1 + 2 = 3$

Таким образом, результатом классификации будет отнесение документа к классу «общие документы».

Нетрудно показать на примере, что отображение F, построенное описанным выше образом, не является состоятельным.

Пример 2

Пусть

$K = \{\text{защита, информация, алгоритм, шифрование, программа}\}$

$C = \{\text{общие документы, криптография}\}$

$d_1 = K_1' = \{\text{защита, алгоритм, шифрование}\}$ криптография

$d_2 = K_2' = \{\text{защита, информация, алгоритм}\}$ общие документы

$d_3 = K_3' = \{\text{защита, алгоритм, программа}\}$ общие документы

Тогда $F(d_1) = \text{криптография}$, то есть документ d_1 из обучающего множества классифицируется таким отображением неправильно (поскольку $|K_1' \cap K_1'| = 3$, но $|K_1' \cap K_2'| + |K_1' \cap K_3'| = 4$).

В связи с этим предлагается доработать алгоритм следующим образом:

$$F(K') = c_j : \left| K' \cap \bigcup_{K_i' \in D_0 : F_0(K_i') = c_j} K_i' \right| = \max_{c_j}$$

В данном случае мы считаем число общих ключевых слов не для каждого документа из «обучающего» множества в отдельности, а для объединения множеств ключевых слов всех документов, отнесенных к определенному классу. Тогда ключевые слова, которые повторяются в разных документах из «обучающего» множества, отнесенных к одному классу, будут учитываться только один раз, а не столько раз, сколько они встречаются в разных документах, как в предыдущем случае.

Предположение о том, что построенное таким образом классифицирующее отображение является состоятельным, требует дальнейшего исследования.

Итак, перечислим основные достоинства описанного теоретико-множественного подхода к задаче автоматической классификации документов на основе ключевых слов:

1) Простота программной реализации.

2) Возможность теоретического обоснования состоятельности и строгого математического анализа эффективности и надежности алгоритма.

3) Высокое быстродействие при большом объеме документов и ключевых слов.

К недостаткам относятся:

1) Зависимость от числа документов «обучающего» множества, отнесенных к определенному классу – их должно быть для каждого класса примерно поровну.

2) Зависимость от числа ключевых слов, определенных для каждого документа – их также должно быть примерно поровну.

3) Возможность (и достаточно высокая вероятность, особенно при малом числе классов и ключевых слов в документах) ситуации неопределенности, когда мощности пересечений множеств ключевых слов для разных классов совпадают.

Для устранения вышеперечисленных недостатков предлагается подход с использованием теории нечетких множеств: вместо детерминированных множеств ключевых слов в документах определяется степень соответствия каждого ключевого слова из K тексту данного документа в виде вещественного числа от 0 до 1. Тогда характеристикой документа, являющейся основой для классификации, будет вектор, состоящий из n чисел от 0 до 1 (n - число ключевых слов в глобальном множестве K), а в качестве операции пересечения таких «нечетких» множеств в самом простом случае можно взять операцию поэлементного определения минимума из составляющих вектора. В данном случае удастся устранить все 3 вышеописанных недостатка, используя математический аппарат теории нечетких множеств.

В результате исследования была описана схема реализации программы классификации и разработан алгоритм ее осуществления. Следующим этапом является программная реализация алгоритма, оценка результатов классификации, разработка дальнейшей стратегии улучшения и применения других алгоритмов. В дальнейшем планируется использовать этот алгоритм при создании экспертной системы согласования нормативных документов для разработчиков систем защиты информации.

Библиографический список

1. Федорова Е. Ю. Автоматизированная классификация электронных документов в области защиты информации // Актуальные проблемы авиации и космонавтики : тез. Всерос. науч.-практ. конф. студентов, аспирантов и молодых специалистов (6–10 апреля 2009, г. Красноярск) : в 2 т. Т. 1. / под общ. ред. И. В. Ковалева ; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2009.

E. Y. Fyodorova, T. A. Chalkin

DEVELOPMENT OF ELECTRONIC DOCUMENTS AUTOMATIC CLASSIFICATION ALGORITHM FOR APPLICATION IN THE SPHERE OF INFORMATION SECURITY

In this paper it is described the electronic documents classification algorithm for application in the sphere of information security which is based on set-theoretical approach to documents keywords analysis.

УДК 517. 91

Т.К. Юлдашев

НЕЯВНОЕ ЭВОЛЮЦИОННОЕ ИНТЕГРАЛЬНОЕ УРАВНЕНИЕ ВОЛЬТЕРРА ПЕРВОГО РОДА

Изучается однозначная разрешимость и устойчивость решения неявного интегрального уравнения Вольтерра при заданных начальном и конечном условиях. Доказывается теорема о существовании и единственности непрерывного решения уравнения на рассматриваемом отрезке. При этом применяется метод последовательных приближений в сочетании его с методом сжимающих отображений.

В данной работе рассматривается уравнение

$$f\left(t,\ \int_{-\infty}^{\alpha(t)} K(t,s)u(s)\,ds\right)=0\ ,\quad t\in T_1 \tag{1}$$

с начальным

$$u(t)=g_1(t)\ ,\ \ t\in E_0\equiv\left(-\infty;t_1\right] \tag{2}$$

и конечным

$$u(t) = g_2(t),\ t \in E_T \equiv [T;\infty) \tag{3}$$

условиями, где $K(t,s) \in C\left(T_{-\infty}^2\right)$, $f(t,x) \in C\left(T_1 \times R\right)$, $T_1 \equiv [t_1;T]$, $0 < t_1 < T < \infty$, $T_{-\infty} \equiv E_0 \cup T_1 \equiv (-\infty;T]$, $t < \alpha(t) \in C(T_{-\infty} \cup E_T)$, $g_1(t) \in C(E_0)$, $g_2(t) \in C(E_T)$, .

Подчеркнем, что начальная и конечная функции (2) и (3) помогают нам в преобразовании уравнения (1) к специальному виду нелинейного интегрального уравнения Вольтерра второго рода.

Отметим, что в работе [1] рассмотрен вопрос об однозначной разрешимости нелинейного интегрального уравнения Вольтерра первого рода вида

$$\int_{t_0}^{t} K(t,s)\,u(s)\,ds = f\left(t,\,u(t)\right),\ t \in \left[t_1, T\right]. \tag{a}$$

Далее в работах [2 - 4] были развиты и обобщены идеи работы [1]. А в работе [5] рассматривается дискретный аналог уравнения (а).

Доказывается теорема о существовании, единственности и устойчивости по начальной функции (2) решения уравнения (1) на отрезке T_1.

На отрезке $T_0 \equiv [t_0,T]$, $0 < t_0 < t_1$ вводим новую функцию $K_0(t)$ такую, что

$$K_0(t) \in C(T_0^2),\ 0 < K_0(t).$$

Примем обозначения

$$\varphi(t,s) = \int_{s}^{t} K_0(\tau)\,d\tau,\ \varphi(t,t_0) = \varphi(t),\ t \in T_0 \equiv \lfloor t_0;T \rfloor.$$

Ясно, что $\varphi(t,s) = \varphi(t) - \varphi(s)$.

Под решением уравнения (1) мы понимаем непрерывную на отрезке T_1 функцию $u(t)$, удовлетворяющую уравнение (1) при начальном (2) и конечном (3) условий.

Здесь используем интеграл

$$\int_{t_0}^{t} K_0(s)\,u(s)\,ds,$$

который понимается в смысле суммы двух следующих интегралов

$$\int_{t_0}^{t} K_0(s)\,u(s)\,ds = \int_{t_0}^{t_1} K_0(s)\,g(s)\,ds + \int_{t_1}^{t} K_0(s)\,u(s)\,ds,$$

где $u(s)$ - неизвестная функция.

Тогда уравнение (1) при начальном (2) и конечном (3) условий запишем в виде

$$u(t) + \int_{t_0}^{t} K_0(s)u(s)\,ds = u(t) + \int_{t_0}^{t} K_0(s)u(s)\,ds +$$

$$+ f\left(t,\ \int_{-\infty}^{\alpha(t)} K(t,s)u(s)\,ds\right),\ t \in T_1.$$

Отсюда, используя резольвенту ядра $[-K_0(s)]$, имеем

$$u(t)=\int_{t_0}^{t}K_0(s)u(s)\,ds+u(t)+$$

$$+f\left(t,\int_{-\infty}^{\alpha(t)}K(t,s)\,u(s)\,ds\right)+$$

$$+\int_{t_0}^{t}K_0(s)\exp\{-\varphi(t,s)\}\cdot\left\{-u(s)-\int_{t_0}^{s}K_0(\tau)\,u(\tau)\,d\tau-\right.$$

$$\left.-f\left(s,\int_{-\infty}^{\alpha(s)}K(s,\tau)u(\tau)\,d\tau\right)\right\}ds,\ \ t\in T_1. \qquad (4)$$

Применяя к (4) формулу Дирихле, получаем

$$u(t)=\int_{t_0}^{t}H(t,s)u(s)\,ds+\left[u(t)+f\left(t,\int_{-\infty}^{\alpha(t)}K(t,s)u(s)\,ds\right)\right]\times$$

$$\times\exp\{-\varphi(t)\}+\int_{t_0}^{t}K_0(s)\cdot\exp\{-\varphi(t,s)\}\times\{u(t)-u(s)+$$

$$+f\left(t,\int_{-\infty}^{\alpha(t)}K(t,s)u(s)\,ds\right)-$$

$$\left.-f\left(s,\int_{-\infty}^{\alpha(s)}K(s,\tau)u(\tau)\,d\tau\right)\right\}ds,\ \ t\in T_1, \qquad (5)$$

где

$$H(t,s)\equiv K_0(s)\exp\{-\varphi(t,s)\}-$$

$$-\int_{s}^{t}K_0(\tau)\cdot\exp\{-\varphi(t,\tau)\}\cdot K_0(\tau,s)\,d\tau\,. \qquad (6)$$

Уравнение (1) при условиях (2) и (3) эквивалентно уравнению (5).

Теорема. Пусть выполняются следующие условия:

$$f(t,x)\in Bnd(M)\cap Lip\{L(t)_{|x}\},\ \ 0<M=const,\ \ 0<L(t)\in C(T_1).$$

Тогда уравнение (1) при условиях (2) и (3) имеет единственное решение на отрезке T_1. Это решение устойчиво по начальной функции (2).

Доказательство. Итерационный процесс Пикара определим следующим образом:

$$\begin{cases}u_0(t)=g(t),\ t\in E_0,\\ u_0(t)=f(t,0)\cdot\exp\{-\varphi(t)\}+\int_{t_0}^{t}K_0(s)\cdot\exp\{-\varphi(t,s)\}\times\\ \qquad\times\{f(t,0)-f(s,0)\}\,ds,\ \ t\in T_1,\end{cases} \qquad (7)$$

$$\begin{cases} u_{k+1}(t) = g(t),\ t \in E_0, \\ u_{k+1}(t) = \int\limits_{t_0}^{t} H(t,s)\,u_k(s)\,ds + \end{cases}$$

$$+\left(u_k(t) + f\left(t,\ \int\limits_{-\infty}^{\alpha(t)} K(t,s)\,u_k(s)\,ds \right) \right) \times$$

$$\times exp\{-\varphi(t)\} + \int\limits_{t_0}^{t} K_0(s) \cdot exp\{-\varphi(t,s)\} \times \Big\{ u_k(t) - u_k(s) +$$

$$+ f\left(t,\ \int\limits_{-\infty}^{\alpha(t)} K(t,s)\,u_k(s)\,ds \right) -$$

$$- f\left(s,\ \int\limits_{-\infty}^{\alpha(s)} K(s,\tau)\,u_k(\tau)\,d\tau \right) \Big\} ds,\quad t \in T_1. \tag{8}$$

Для нулевого приближения $u_0(t)$ в силу условия теоремы из (7) получим оценку

$$\|u_0(t)\| \le \|f(t,0)\| exp\{-\varphi(t)\} +$$

$$+ \int\limits_{t_1}^{t} K_0(s)\,exp\{-\varphi(t,s)\} \cdot \|f(t,0) - f(s,0)\|\,ds \le M \cdot P(t,t_1),\ t \in T_1, \tag{9}$$

где $P(t,s) \equiv exp\{-\varphi(t)\} + 2\int\limits_{s}^{t} K_0(\tau)\,exp\{-\varphi(t,\tau)\}d\tau$.

Для функции $H(t,s)$ из (6) справедлива оценка

$$\|H(t,s)\| \le \|K_0(t,s)\| exp\{-\varphi(t,s)\} +$$

$$+ \int\limits_{s}^{t} K_0(\tau) \|K_0(t,\tau)\|\, exp\{-\varphi(t,\tau)\}d\tau \le \|K_0(t,s)\| \cdot N(t,s),\ \ (t,s) \in T_1^2\ . \tag{10}$$

где $N(t,s) \equiv exp\{-\varphi(t,s)\} + \int\limits_{s}^{t} K_0(\tau)\,exp\{-\varphi(t,\tau)\}d\tau$.

Тогда с учетом (10) в силу условия теоремы из (8) получаем, что для произвольного натурального числа k справедлива оценка

$$\|u_{k+1}(t) - u_k(t)\| \le \int\limits_{t_1}^{t} \|H(t,s)\| \cdot \|u_k(s) - u_{k-1}(s)\|\,ds + \Big[\|u_k(t) - u_{k-1}(t)\| +$$

$$+ L(t) \cdot \int\limits_{t_1}^{t} \|K(t,s)\| \cdot \|u_k(s) - u_{k-1}(s)\|\,ds \Big] \cdot P(t,t_1) \le$$

$$\le \rho(t,t_1) \cdot \|u_k(t) - u_{k-1}(t)\|,\quad t \in T_1, \tag{11}$$

где $\rho(t,t_1)$ определяется из следующей формулы

$$\rho(t,\,s)\equiv\int_s^t\left\|K_0(t,\tau)\right\|\cdot N(t,\tau)\,d\tau+$$

$$+\left\{1+L(t)\cdot\int_s^t\left\|K(t,\xi)\right\|d\xi\right\}\cdot P(t,s).$$

Функция $0<K_0(\xi)$ выбирается таким образом, чтобы было

$$\varphi(t,s)=\int_s^t K_0(\xi)\,d\xi>>1\ .$$

А это значит

$$\exp\{-\varphi(t)\}<<1.$$

Итак, функции $N(t,s)$ и $P(t,s)$ малые. Тогда $L_i(t)$, $(i=\overline{1,3})$ можно выбрать так, чтобы было $\rho(t,s)<1$.

Отсюда в силу оценок (9) и (11) следует, что оператор в правой части (5) является сжимающим. Следовательно, согласно принципу Шаудера о неподвижной точке существует на отрезке T_1 единственное решение уравнения (1) с условиями (2) и (3).

Теперь покажем устойчивость решения уравнения (1) по начальной функции (2). Пусть $g_{11}(t)$ и $g_{12}(t)$ две начальные функции на начальном отрезке E_0. Тогда на отрезке T_1 им соответствуют два решения $u_1(t)$ и $u_2(t)$ уравнения (1).

Положим $\|p(t)\|\equiv\|g_{11}(t)-g_{12}(t)\|<\delta$, где $0<\delta$ - малое число.

Тогда из (5) получаем

$$\|u_1(t)-u_2(t)\|\le\rho(t_1,t_0)\cdot\|p(t)\|+\rho(t,t_1)\cdot\|u_1(t)-u_2(t)\|\ . \qquad (12)$$

Так как $\rho(t,s)<1$ для всех $(t,s)\in T_0^2$, то из (12) окончательно имеем

$$\|u_1(t)-u_2(t)\|<\varepsilon,\ \varepsilon=\delta\cdot\left(1-\rho(t,t_1)\right)^{-1}.$$

Библиографический список

1. Юлдашев Т.К., Артыкова Ж.А. Интегральное уравнение Вольтерра первого рода с нелинейной правой частью // Складні системи і процеси. - №1,2. – 2005. – С. 3-5.

2. Юлдашев Т.К., Артыкова Ж.А. Интегральные уравнения Вольтерра первого рода с нелинейной правой частью и сложным отклонением // Тезисы межд. семинара «Геометрия в Одессе - 2005. Дифференц. геометрия и ее приложения» (23-29 мая 2005 г.). – Одесса, 2005. – С. 112-113.

3. Yuldashev T.K., Artykova J.A. Volterra functional integral equation of the first kind with nonlinear right-hand side and variable limits of integration // Укр. мат. журн. – 2006. – Т. 58. - № 9. – С.1285-1288.

4. Юлдашев Т.К., Артыкова Ж.А. Эволюционное интегральное уравнение Вольтерра с интегральными отклонениями // Вестник УлГТУ. - № 3. – 2006. – С. 18-20.

5. Yuldashev T.K. On a summary equation with weak nonlinear right-hand side // Advanced stud. in contemp. math. – V. 15. – N 1. – 2007. – P. 95-98.

T.K. Yuldashev

NONEXPLICIT EVOLUTION VOLTERRA INTEGRAL EQUATION OF THE FIRST KIND

We prove a theorem of existence, uniqueness and stability of solution of the nonexplicit evolution Volterra integral equation with respect to the initial value condition on the given finite segment. Here we use the method of successive approximation in combination it with the method of compressing mapping.

УДК 004. 4’244

Т.К. Юлдашев, Ж.К. Акматалиев

ПРАВОВЫЕ НОРМЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ: НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Рассматриваются проблемы правового обоснования противодействия компьютерной преступности, в случае неправомерного доступа к компьютерной информации

Научно-техническое достижение обусловливает не только коренные прогрессивные изменения в составе факторов экономического развития Кыргызстана, но и стимулирует негативные тенденции развития преступного мира, приводит к появлению новых форм и видов преступных посягательств.

Преступные сообщества создают системы конспирации и связи, принимают меры по оказанию активного противодействия сотрудникам правоохранительных органов, используя современные технологии и специальную технику, в том числе и новые информационно-обрабатывающие технологии. Для достижения корыстных целей все чаще применяют системных при планировании своих действий, разрабатывают оптимальные варианты проведения и обеспечения криминальных "операций", создают системы скрытой связи [1].

Особую тревогу в этом плане вызывает факт появления и развития в странах СНГ нового вида преступных посягательств, связанных с использованием средств компьютерной техники. Такой вид преступности называется компьютерной.

Под компьютерным преступлением Бекбоев А.З. понимает запрещенное уголовным законом общественно опасное деяние, посягающее на нормальный порядок развития отношений в сфере компьютерной информации и безопасное функционирование ЭВМ, системы ЭВМ или их сети, причиняющее при этом вред личным правам и интересам, а также правам и интересам общественной и государственной безопасности [2].

При рассмотрении компьютерных преступлений особое внимание уделяется преступлениям, совершаемым через Интернет.

Интернет как новое средство общения, обмена информацией, моментального производства платежей, сегодня представляет собой глобальную компьютерную сеть, охватывающий весь мир. Чтобы оценить криминогенный потенциал «Всемирной паутины» достаточно просмотреть уголовный кодекс Кыргызской Республики (УК КР) [3].

Несмотря на принимаемые меры по законодательному закреплению прав и свобод в информационной сфере, остается немало пробелов, помогающих избегать ответственности за совершения действий, наносящих ущерб в сфере информации.

В.В. Крылов выделяет следующие группы способов совершения компьютерных преступлений [4]:

1) Способы непосредственного доступа к компьютерной информации;

2) Способы удаленного доступа к компьютерной информации;

3) Способы распространения технических носителей информации, содержащих вредоносные программы для ЭВМ, систем и компьютерных сетей.

Для предотвращения преступлений с использованием компьютерных технологий в нашей республике создается законодательная база противодействия такой преступности. Здесь можно перечислить:

1) Конституцию КР от 5 мая 1993 г.;
2) Закон КР «О гарантиях и доступе к информации» от 11 ноября 1997 г.;
3) Закон КР «О правовой охране программ для ЭВМ и баз данных» от 2 марта 1998 г.;
4) Указ президента КР «О концепции развития правовой информатизации в Кыргызской Республике» от 17 Октября 1997 г (УП № 285).
5) Указ президента КР «О создании Государственной компьютерной сети» от 3 мая 2001г. (УП №115);
6) Постановление Правительства КР « О мерах по предотвращению негативных последствий в компьютерной технологии» от 1 марта 1999 г. (№117);
7) Постановление Правительства КР « О концепции информационной безопасности Кыргызской Республики» от 22 марта 2005 г. (№143)

Новый уголовный кодекс Кыргызской Республики с главой «Преступление в сфере компьютерной информации» предусматривает следующие преступления: 1) Неправомерный доступ к компьютерной информации (статья 289 УК КР); 2) Создание, использование и распространение вредоносных программ для ЭВМ (статья 290 УК КР); 3) Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (статья 291 УК КР).

Как мы отмечали, статья 289 УК КР предусматривает ответственность за неправомерный доступ к компьютерной информации, т.е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Обычно под компьютерным преступлением понимаются две категории преступлений:

1) Преступления, связанные с вмешательством в работу компьютеров;
2) Преступление, использующие компьютеры как необходимые технические средства.

В данной работе рассмотрим преступление, связанные с вмешательством в работу компьютеров. Владелец компьютерной системы имеет право на неприкосновенность содержащейся в системе информации. Это подтверждается Конституцией КР [5] . Ч.13 ст 14 Конституции КР наделяет каждого правом на неприкосновенность частной жизни, личную и семейную тайну. Поэтому в УК КР принята Статья 135 - нарушение неприкосновенности частной жизни человека.

Владелец компьютерной системы является любое лицо, правомерно и в своих интересах пользующееся услугами по автоматизированной обработке данных: как собственник компьютера, так и лицо, приобретшее право пользования компьютером в обязательственных отношениях.

Неправомерный доступ осуществляется с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, путем хищения носителя информации, установки аппаратуры записи, подключаемой к каналам передачи данных. П 4 ст14 Конституции КР предусматривает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. В ч. 5 этой статьи установлено, что органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечит каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Объективная сторона преступления характеризуется неправомерным доступом, нарушающим чужие права и интересы по поводу использования компьютерной системы,

совершенным во вред имущественным или иным подлежащим правовой охране правом и интересом физических и юридических лиц, общества и государства, преступными последствиями и причиной связью между действиями и наступившими последствиями.

Неправомерным следует считать доступ к компьютерной информации в случае, если лицо действует без разрешения владельца этой системы или сети и другого законного полномочия. Понятие охраняемой законом компьютерной информации включает как программы так и иную информацию в оперативной памяти компьютера, информацию на дисплее, информацию на стационарных дисковых накопителях и иную информацию на машинных носителях, в компьютерной системе и сети.

Субъективная сторона характеризуется умышленной формой вины. Совершая это преступление, лицо осознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления предусмотренных в законе последствий, желает или сознательно допускает наступления этих последствий либо относится к ним безразлично [6,7].

Мотивы и цели этого преступления могут быть разными: корыстный мотив, цель получить какую-либо информацию, желание причинить вред либо желание проверить свои способности владения компьютером. Но мотив и цель не являются признаками состава этого преступления и не влияют на квалификацию. Часть 2 ст. 289 УККР предусматривает в качестве квалифицирующих признаков этого преступления совершение его группой лиц по предварительному сговору или организованной группой (ст. 31 УК КР) либо с использованием своего служебного положения.

Лицом имеющим доступ к ЭВМ, системе ЭВМ или их сети, является как лицо, которому в силу разрешения владельца системы или служебного полномочия позволено получать информацию в компьютерной системе, вводить ее или производить с ней операции, так и лицо, осуществляющее техническое обслуживание компьютерного оборудования и на иных основаниях имеющее доступ к компьютерной системе. Лицо, имеющее доступ к компьютерной системе может совершить это преступление лишь в случаи доступа к информации, допуска к которой оно не имеет. В случае, когда существенный вред причиняется действиями лица, имеющего правомерный доступ к компьютерной информации, ответственность наступает по ст. 291 УК КР.

Закон очень широко определяет круг противоправных действий при неправомерном доступе к компьютерной информации. По этому важно в каждом конкретном случаи установить, что деяние причиняет вред личности, обществу и государству либо создает угрозу причинения вреда. Ст 173 УК КР рассматривает причинение имущественного существенного вреда путем обмана или злоупотребления доверием.

Итак, для решения вопроса о том, является ли данное деяние преступлением, необходимо установить материальный признак преступления, т.е. факт причинения существенного вреда или угрозу причинения такого вреда личности, обществу или государству. Отсутствие посягательства на эти общественные отношения исключает уголовную ответственность в силу ч 2 ст. 8 УК КР.

В заключение данной работы в целях совершенствования уголовного законодательства предлагаем статью 289 УК КР в следующей редакции:

«Статья 289. Неправомерный доступ к компьютерной информации

(1) Неправомерный доступ охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно- вычислительной машине (ЭВМ) , системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации,

-наказывается штрафом в размере от пятидесяти до трехсот минимальных месячных заработанных плат либо лишением свободы на срок до двух лет в колониях общего режима.

(2) То же деяние, повлекшее нарушение работы ЭВМ, системы ЭВМ или их сети, совершенное группой лиц по предварительному сговору или организованной группой

либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ или их сети,

- наказывается штрафом в размере от двухсот до семисот минимальных месячных заработных плат либо лишением свободы на срок до пяти лет в колониях общего режима».

Библиографический список

1. Оконова Р.А. Компьютерные преступления: уголовно-правовые и криминологические проблемы, пути их решения. - Бишкек: Салам,2005. - 300 с.
2. Бекбоев А.З. Уголовно-правовые и криминологические меры противодействия преступности в сфере использования компьютерных технологий // Автореф. ... канд. юрид. наук. - Бишкек: КГЮА, 2007. - 23 с.
3. Уголовный кодекс КР от 1 октября 1997 г. - Бишкек: НАКР, 1997. – 168 с.
4. Крылов В.В. Информационно компьютерные преступления. Квалификация. Методика расследования. Основные нормативные акты- М.: Инфра – М – Норма, 1997. - 285 с.
5. Конституция КР от 5 мая 1993 г. с изменением и дополнением на 1 сентября 2002 г. (Токтом).
6. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. – М.: Право и Закон, 1996. – 182 с.
7. Волеводз А.Г. Противодействие компьютерным преступлениям. – М.: Юрлитинформ, 2002. – 496 с.

T.K. Yuldashev, Z.K. Akmataliev

COUNTERACTION LAW RULES OF COMPUTER CRIMINALITY: WRONGFUL ACCESS TO THE COMPUTER INFORMATION

Problems of a legal substantiation of counteraction of computer criminality, in case of wrongful access to the computer information are considered

Секция 3. «Защита персональных данных в информационных системах»

УДК 004.056

Р.М. Алгулиев, Я.Н. Имамвердиев, Ф.Д. Абдуллаева

ВЕКТОР АТАКИ И ЗАЩИТНЫЕ МЕРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

▪

В работе рассматривается проблема обеспечения безопасности персональных данных. Излагается понятие вектора атаки персональных данных технического, физического и социально-инженерного характера. Понятие «кража данных» описывается как реальная угроза широкого использования персональных данных. На основе методики управления рисками предлагается подход к снижению рисков краж персональных данных.

В настоящее время, несмотря на ускоренное развитие отрасли информационной безопасности в целом, количество инцидентов безопасности продолжает увеличиваться. Причиной увеличения инцидентов безопасности является наличие недостатков в разработанных программных продуктах, нацеленных на решение задач информационной безопасности.

Экспансия информационных технологий в производство и управление современных организаций предопределяют рост информационных инфраструктур организаций, что зачастую приводит к неструктурированному гетерогенному характеру компьютерных сетей и является основой неконтролируемого роста уязвимостей, а также к увеличению возможностей несанкционированного доступа к информации.

Несанкционированный доступ к записям, содержащих персональные данные индивидуума приводит к возникновению брешей данных.

Брешь данных (data breach) – это неавторизованное приобретение электронных данных компрометирующее безопасность, конфиденциальность, целостность персональной информации [1]. Это понятие также известно, как брешь в системе защиты (security breach) или как брешь секретности (privacy breach).

На основе данных центра ITRC (Identity Theft Resource Center, ITRC), уведомление субъектов о наличии брешей были помещены в одну из следующих категорий [2]:

- учебные заведения: все уровни государственных и частных учебных предприятий, включая колледжи, университеты, аффилированные объекты (например, организации выпускников);
- организации здравоохранения: больницы, службы здравоохранения, страховые компании здравоохранения;
- организации по управлению финансами: банки, страховые компании и инвестиционные услуги;
- предприятия общего назначения: коммерческие организации, не имеющие отношения к вышеперечисленным категориям;
- правительственные организации: федеральные, государственные и муниципальные организации.

Бреши в системе защиты классифицируются по причинам их возникновения [2]:

- хакер: нелегальный доступ через Интернет человека, находящегося вне атакованном объекте к данным содержащийся в компьютерной системе;
- физическая кража: кража компьютеров, компьютерных оборудований (включая носители компьютерных данных) или бумажных файлов;
- чужой дисплей: позволяет просмотр персональной информации человеку, который не имеет к нему доступа;
- доступ изнутри: кража служащих и контракторов, предоставление предпринимателем доступа к персональной информации;
- потеря резервных оборудований: кража носителей, содержащих персональные данные;

- не установленные: специфичная причина брешей, которая не была раскрыта субъектом, испытывающим потери данных.

Бреши безопасности, вытекающие от хакеров и внешних доступов, имеют наибольший разрушительный потенциал. Эти бреши завершаются преднамеренными попытками для получения доступа к персональной информации. При наличии перечисленных типов брешей персональная информация приобретается субъектом или передается субъекту, стремящемуся совершать кражу данных (Identity Theft).

Борьба с кражами данных является актуальной и жизненно важной проблемой. С целью составления статистических данных о краже персональных данных в зарубежных странах созданы специальные центры:

- Identity Theft Data Clearinghouse http://www.ftc.gov
- Privacy Rights Clearinghouse http://www.privacyrights.org
- Identity Theft Resource Center (ITRC) http://www.idtheftcenter.org

По данным центра Privacy Rights Clearinghouse 85% организаций, сталкивались с проблемой кражи персональных данных. За период 2005-2009 годы было украдено 260716323 записей СУБД.

Многие толкователи отмечают, что термин «кража данных» (“identity theft”) в общем, используется для выражения термина “подделка данных” (“identity fraud”) в котором "кража" (theft) и "подделка" (fraud) должны разъединяться [3].

- подделка (fraud): обман злоумышленника, которая умышленно осуществляется, чтобы обеспечивать несправедливую и незаконную выгоду.
- кража данных (identity theft): получение персональной или финансовой информации, присущей другому человеку, с целью создания ложной идентификации. Кража данных соответственно охватывает множество действий, включая сбор персональной информации, создание ложных документов личности и использование персональной информации обманным путем.

Злоумышленники часто стараются приобрести следующие персональные данные человека (таблица 1).

Таблица 1

Название	Гендер	Возраст
дата рождения	место рождения	свидетельство о рождении
девичья фамилия матери	семейное положение	этническое происхождение
адрес (текущий и прежний)	телефонный номер	адрес электронной почты
номер социального страхования	лицензионный номер водителя	номер медицинской карточки
номер паспорта	карточка постоянного жительства	мандат счета (имя пользователя, пароль, ПИН, и т.д)
трудовая книжка	информация о семьи	история об образовании
история болезни	число иждивенцев	информация о супруге
личный адрес	номер диска транспортного средства	
регистрационный номер транспортного средства	информация о средствах	
номера кредитной карточки	номер визитной карточки и персональный идентификационный номер (ПИН)	долги
номера платежной карточки и персональный идентификационный номер (ПИН)	идентификационный номер налогоплательщика	фактические или ожидаемые доходы
номера банковского счета	подробности об ипотеки	информация об инвестиции
неуплаченный долг		
отпечатки пальца	отпечатки голоса	изображение сетчатки
высота	вес	цвет глаз и волос

Злоумышленники для приобретения персональных данных пользуются многими методами. Эти методы называются *векторами атаки*, термин который означает маршрут или способ, который используется для вторжения в компьютерные системы [4, 5].

Имеются три различные вида векторов атак:

1. **Технические** – атаки эксплуатируют компьютеры и подключения Интернет:

- Trojan/Keystroke Logger - программы-шпионы/вредоносные программы, помещенные посредством хакерства
- Wireless Intercept - вооруженное нападение (Wardriving), открывает точку доступа, установка фальшивой точки доступа (airsnarfing). Атака “Evil Twin”
- Pharming - DNS спуфинг, отравление кеша DNS, прокси атаки
- Scrape Web site – собирает персональные данные из Веб сайтов, поисковые системы Веб используются как верификатор
- Sniffing – собирает пакеты данных атакуемой сети
- Hacking - получает привилегированный доступ к компьютеру для осуществления дальнейших нападений и/или сбор данных
- Data attacks - SQL Injection, XSS
- Database attacks - Login attacks, inference attacks, SQL сканеры
- Password cracking – приобретает пароли администратора к серверам

2. **Физические** – атаки, связанные с такими устаревшими технологиями как отслеживание мусора:

- Theft – кража портативных компьютеров, бумажников, почты
- Shoulder Surfing – непосредственное наблюдение персональной информации
- Dumpster Diving – приобретают отброшенные документы, аппаратные средства (диски)
- Trusted Insiders – персональная информация, неправильно использованная индивидуумами при доступе
- Breach firewall(s) – присоединение к внутренней сети

3. **Социально-инженерные** - атака, использующая особенности человека в своих интересах, чтобы получить персональную информацию:

- Phishing - соблазнение индивидуумов, чтобы показать конфиденциальные данные
- Family members – персональные данные, ошибочно использованные членами семьи
- Legal Sources of Identity – получать персональные данные от кредитных бюро, правительственных агентств мошенническим путем
- 419 scams – получать деньги или информацию о счете
- Trusted Insiders - получать персональную информацию от провайдеров (от докторов, стоматологов, юристов, администраторов баз данных, служащих, контракторов, индивидуумов и т.д.)
- Gain access – получать доступ в компьютерные залы, коммутационные шкафы, коммутаторы, маршрутизаторы
- Phone requests – получать персональную информацию, чтобы облегчать хакерство.

Отметим, что перечисленные атаки ставят персональные данные под угрозу подвергания риску их краж. Имеются ряд защитных мер, которые могут быть предприняты для минимизации рисков, вытекающих от вышеперечисленных атак. Выбор защитных мер должен осуществляется на основе их эффективности. При этом определение критерия выбора конкретных защитных мер является более сложной задачей. Подходы оценки и управления рисками являются эффективными механизмами в этом процессе отбора.

Оценка рисков подразделяется на три основные этапа: определение серьезности последствия угрозы, определение вероятности возникновения угрозы и проведение на основе этих двух факторах оценки рисков [6].

$$Риск = Вероятность\ возникновения \times Серьезность\ последствия$$

Если предположить, что эти два фактора точно определены, то метод оценки рисков окажет помощь при выборе защитных мер, препятствующих конкретной атаке. Соответствующие защитные меры, избранные с применением метода оценки рисков в контексте персональных данных иллюстрированы в Таблице 2

Таблица 2.

Защитные меры персональных данных

Защитные меры / Инциденты	Многофакторная аутентификация	Антивирусная защита	Шифрование	SSL/TLS	Контроль доступа	Обучение пользователя	Соблюдение политики безопасности	Аудитный контроль
Trojan/Keystroke Logger	√	√						
Wireless Intercept			√					
Pharming				√				
Scrape Web site								
Sniffing				√				
Hacking					√			
Data attacks								
Database attacks	√		√					
Password cracking	√							
Theft			√			√	√	
Shoulder Surfing						√		
Dumpster Diving						√		
Trusted Insiders	√		√		√	√		√
Breach firewall(s)								
Phishing	√							
Family members						√		
Legal Sources of Identity	√							
419 scams						√		
Gain access	√					√		
Phone requests						√		

Библиографический список

1. Romanosky S., l Telang R., Acquisti A. Do Data Breach Disclosure Laws Reduce Identity Theft? / Seventh Workshop on the Economics of Information Security. Hanover, 2008
2. ITRC Breach Meter Reaches 342, to Date 2008 Data Breach count is 69% greater than 2007(Jan 1 through June 27), http://www.idtheftcenter.org/artman2/publish/m_press/Breach_List_2008_Q2.shtml
3. Identity theft and protecting personal information. Plymouth Chamber of Commerce: Brown Bag Lunch Series. 2009
4. Techniques of Identity Theft. Canadian Internet Policy and Public Interest Clinic, CIPPIC Working Paper No. 2 (ID Theft Series), 2007
5. Liberty Alliance Whitepaper: Identity Theft Primer, Liberty Alliance Project, 2005, http://www.projectliberty.org/resources/id_Theft_Primer_Final
6. General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD, 1999.

R.M. Alguliev, Y.N. Imamverdiev, F.D. Abdullayeva
ATTACK VECTORS AND DEFENSIVE MEASURES OF PERSONAL DATA

In this paper the problem of security of the personal data is considered. Concept of attack vectors of the personal data in technical, physical and social - engineering character is described. The «Identity Theft» concept is described as a real threat of the wide implementation of personal data. On the basis of risk management technique is offered the approach reducing risks of personal data thefts.

УДК 004.8.032.26

О. О. Варламов
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И АНАЛИЗ ДЕВЯТИ ВИДОВ ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Рассмотрены девять видов технической компьютерной разведки и особенности защиты персональных данных от них.

Выделяют агентурную и техническую разведки. В отличие от агентурной разведки, техническая разведка непосредственно с людьми не работает. Образно говоря, при создании, передаче, хранении или обработке информации всегда можно выделить некий "материальный носитель" информации и ее "содержание" (смысл, семантика), между которыми всегда есть четкое взаимоотношение. Тогда, информация - это "двойка", т.е. вектор, включающий два параметра: 1) носитель информации и 2) «содержание» (смысл) информации. Причем, «содержание» появляется только в голове у человека, а вот носитель может иметь разную "физическую природу". С развитием науки и техники, расширяются возможности технических разведок, следовательно, необходимо защищать персональные данные постоянно учитывая новые угрозы и своевременно внедряя сертифицированные средства защиты информации. Исходя из разнообразия физического мира и взаимосвязи всех его сущностей, становится понятно, что носители информации могут проявляться совершенно в неожиданных формах: акустика, оптика, ПЭМИН и т.п.

Конечно, для разведки интерес представляет, прежде всего, информация ограниченного доступа. Такая информация может быть не только в виде слов, но может записываться на технические устройства, реализовываться в виде устройств, способов и т.п. Возможности современной науки и техники огромны, ну а техническая разведка (ТР) никогда от них не отставала [1]. Техническая разведка всегда использовала достижения науки и технического прогресса и порождала "отрицательные" последствия успехов науки. В настоящее время выделено более 30 видов технической разведки [1, 2]. Кроме того, разработана модель универсального описания хранения и передачи информации. Выделяют отправителя информации, время передачи и получателя. Если отправитель и получатель различны, а время передачи мало, то это передача информации. Если отправитель и получатель одинаковы, а время передачи велико, то - это хранение информации. Возможны различные варианты, но данная модель очень полезна и удобна для анализа технической разведки.

Известен классический подход к определению "канала" технической разведки, когда выделяют (вектор-"тройку"): 1) источник информации (объект защиты), 2) среда передачи данных (материального носителя информации) и 3) средства добывания информации (приемник материального носителя информации), который и является инструментом ТР. Наборы таких "троек" образуют различные "технические каналы распространения (утечки) информации". Для "классических" видов технической разведки, например: радио, видео, акустической и т.п., с "каналами ТР" все известно. С появлением компьютеров

появилась и техническая компьютерная разведка (ТКР). В связи с небольшим временем существования (относительно других видов ТР), а также с учетом стремительного развития ИТ-технологий, ТКР пока не является классической и является предметом споров и дискуссий. Исходя из сущности понятия "канал технической разведки", еще в 2003 году были выделены 9 видов ТКР. Не вдаваясь в "юридические" споры и исходя из технического смысла, получаем, что персональные данные - это некая информация о человеке, проявляющаяся в различных физических средах и которую надо защищать. Под защитой понимают: конфиденциальность, целостность и доступность. При защите ПДн необходимо учитывать возможности технических разведок: побочные электромагнитные излучения и наводки (ПЭМИН), видовой и акустической, которые ранее для защиты конфиденциальной информации не учитывались. Существует три источника для ТКР [2]:

1) данные, сведения и информация, обрабатываемые, в т.ч. передаваемые и хранимые, в компьютерных системах и сетях;
2) характеристики программных, аппаратных и программно-аппаратных комплексов;
3) характеристики пользователей компьютерных систем и сетей.

Принципиально важно, что компьютерные системы являются многоуровневыми. На одинаковых компьютерах можно устанавливать совершенно различные программные комплексы для выполнения разнообразных задач. И, наоборот, на аппаратно разных компьютерах можно устанавливать одинаковые программные среды и комплексы для решения однотипных задач. Многоуровневое построение обуславливает наличие на одной физической среде нескольких различных: объектов защиты, сред передачи данных и средств добывания информации, т.е. различных "виртуальных" каналов ТКР.

Техническая компьютерная разведка

По принципам построения программно-аппаратных комплексов, каналам распространения информации и функциональному предназначению выделяют [2-3]: **техническую компьютерную разведку**, обеспечивающую добывание информации из компьютерных систем и сетей; характеристик их программно-аппаратных средств и пользователей, которая, включает:

1) **семантическую**, обеспечивающую добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов;
2) **алгоритмическую**, использующую программно-аппаратные закладки и недекларированные возможности для добывания данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и недекларированных возможностей (НДВ) компьютерных систем и сетей;
3) **вирусную**, обеспечивающую добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами;
4) **разграничительную**, обеспечивающую добывание информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе несанкционированного доступа (НСД) к информации, а также реализации несанкционированного доступа при физическом доступе к похищенным компьютерам или машинным носителям информации (МНИ);
5) **сетевую**, обеспечивающую добывание данных из компьютерных сетей, путем реализации зондирования сети, инвентаризации и анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств

сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ресурсам, модификацию ресурсов, перехват управления ресурсами либо маскирование своих действий;

6) **потоковую**, обеспечивающую добывание информации и данных путем перехвата, обработки и анализа сетевого трафика (систем связи) и выявления структур компьютерных сетей и их технических параметров;

7) **аппаратную**, обеспечивающую добывание информации путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими типами ТКР;

8) **форматную**, обеспечивающую добывание информации и сведений путем "вертикальной" обработки, фильтрации, декодирования и других преобразований форматов представления, передачи и хранения добытых данных; преобразования добытых данных в сведения, а затем в информацию для последующего ее представления оператору ПДн;

9) **пользовательскую**, обеспечивающую добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной информационной инфраструктуре (приманка).

Анализ возможностей защиты ПДн от ТКР

Семантическая разведка занимается анализом фактографической информации и представляет собой угрозу для ПДн. В Руководящих документах ФСТЭК России (далее - РД) данная угроза пока не прописана. Следовательно, необходимо самостоятельно предусмотреть защиту от этой разведки - по решению оператора ПДн.

Алгоритмическая разведка на уровне программных закладок (НДВ) является угрозой для ПДн. Средством защиты от этого является сертификация на НДВ. Для защиты ПДн достаточно провести сертификацию на «НДВ-4». Защита от алгоритмической разведки на уровне аппаратуры ("железа") реализуется в рамках проведения специальных проверок компьютерного оборудования, что актуально только для ИСПДн высшего класса защиты К1.

Вирусная разведка может реализовать угрозу для ИСПДн. В РД есть подробные требования по подсистеме антивирусной защиты ПДн.

Разграничительная разведка реализуется в виде несанкционированного доступа – НСД. Защита от НСД подробно прописана в РД. Кроме того, для противодействия этой разведке необходимо проводить сертификацию программных средств защиты информации по "СВТ". Рекомендуют также встраивать внешние средства противодействия разграничительной разведке и недопущения несанкционированного доступа к конфиденциальной информации.

Сетевая разведка также представляет собой большую угрозу для ПДн, и средства защиты от нее должны располагаться на сетевом уровне взаимодействия, где разработаны специальные аппаратные, программные и программно-аппаратные средства. Прежде всего, это межсетевые экраны (МЭ), которые обязательно должны пройти сертификацию по "МЭ". Кроме того, по РД необходимо создавать подсистему обнаружения вторжений, требования к которой разработаны ФСБ.

Потоковая разведка работает на том же уровне, что и сетевая. В явном виде она не представляет угрозу для ПДн, но в отдельных сложных случаях необходимо защищаться и от нее. Для этого должны применяться специальные программно-аппаратные комплексы. Впрочем, отдельного исследования требует оценка необходимости защиты от потоковой

разведки персональных данных. С учетом критерия стоимости самой подсистемы защиты информации, достаточно низких рисков и отсутствия явно сформулированных требований, целесообразно оставить это на усмотрение операторов ПДн.

Аппаратная разведка направлена для получения информации об аппаратуре ("железе"). Следовательно, эта разведка непосредственно для ПДн не представляет угрозы, требований РД не предъявлено, значит - на усмотрение операторов ПДн.

Форматная разведка представляет угрозу для ПДн. Однако, специальных явно сформулированных требований руководящих документов, за исключением криптографических средств, не существует. При необходимости, оператор ПДн может применять различные средства защиты информации, вплоть до сертифицированных российских криптографических средств защиты информации.

Пользовательская разведка угрожает безопасности ПДн, но требований в РД к ней нет. Оператор ПДн сам вправе определить, как защищать свою конфиденциальную информацию и персональные данные от пользовательской разведки. Например, можно применять методы "избыточного трафика", "разбиения на несколько пользователей", защищенные вычислительные устройства и т.п.

Для аттестации ИСПДн выдвигается довольно много требований, которые напрямую не относятся к программному обеспечению, но должны быть выполнены оператором ПДн. Прежде всего, это организационные и технические меры, подробно расписанные в РД ФСТЭК России для каждого класса защиты ИСПДн. Вплоть до обязательного введения администраторов информационной безопасности для защиты ПДн в ИСПДн К1. Важно подчеркнуть, что при создании ИСПДн сразу же необходимо продумывать и создавать все требуемые подсистемы защиты ПДн, использовать сертифицированное оборудование и программное обеспечение.

Выводы

С развитием науки и техники, расширяются возможности технических разведок, следовательно, необходимо защищать персональные данные постоянно учитывая новые угрозы и своевременно внедряя сертифицированные средства защиты информации. К сожалению, гарантировать полную безопасность ПДн никто не может. Однако, соблюдение требований РД и проведение аттестации ИСПДн обеспечивают юридическую защиту оператору ПДн, даже в случаях нарушения безопасности ПДн, если были соблюдены все предписания и мероприятия, указанные в аттестате на ИСПДн.

Библиографический список

1. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. М.: Российский гос. гуманитарный ун-т, 2002. 399с.
2. Варламов О.О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ТРТУ, Тематический выпуск "Информационная безопасность", Таганрог: Изд-во ТРТУ, 2006, № 7 (62). С. 216-223.
3. Материалы сайта "дтн Варламов О.О." www.ovar.narod.ru.

O. O. Varlamov

PROTECTION OF THE PERSONAL DATA AND THE ANALYSIS OF NINE KINDS OF TECHNICAL COMPUTER INVESTIGATION

As is known, investigation may be secret-service and technical. Unlike secret-service investigation, technical investigation does not work directly with people. Figuratively speaking, at creation, transmission, storage or processing of the information it is always possible to

allocate certain "the material exponent" of information and its "contents" (sense, semantics) between which always there is a precise mutual relation. Then, the information is "two", i.e. a vector including two parameters: 1) a data carrier (exponent) and 2) "contents" (sense) of the information. And, "contents" appears only in a head of the person, and the carrier (exponent) can have different "physical nature ". With development of a science and engineering, opportunities of technical investigations are extended, hence, it is necessary to protect personal data constantly taking into account new threats and introducing in due time the certificated means of protection of information. Unfortunately, nobody can guarantee full safety of the personal data. However, observance of requirements of managing documents (RD) and realization of certification of information systems of personal data (ИСПДн) provides legal protection to the operator of personal data, even in case of infringement of safety personal data if all instructions and the actions specified in the certificate on of information systems of personal data were observed.

УДК 004.8.032.26

О. О. Варламов, Е. Г. Колупаева

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СЕРТИФИКАЦИИ ПРОГРАММ, КЛАССИФИКАЦИИ И АТТЕСТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассмотрены основные понятия в области защиты персональных данных, обоснована необходимость сертификации программ и приведена модифицированная таблица описания классов информационных систем персональных данных.

Персональные данные (ПДн) – это, по существу, информация, которая позволяет однозначно определять конкретного человека (субъекта). Во многих случаях данное соотнесение "информации" и конкретного человека объективно необходимы: при покупке билета на самолет или поезд, в банках при проведении платежей, на работе в отделе кадров и т.д. Более того, такое "соотнесение" проводится уже многие десятилетия. Почему же безопасность "персональных данных" стала актуальна именно в нашем 21 веке? Разве раньше не защищали "личные сведения"? Напомним основные понятия в области ПДн.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и др.

Информационная система персональных данных (ИСПДн) - представляет собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Внесем уточнение: не все персональные данные необходимо защищать. В законодательстве указано, какие ПДн подлежат защите, а какие нет. Каждый человек имеет право открыто опубликовать любую информацию о себе, при этом сам определяет необходимость защиты своих персональных данных. Как только речь заходит о персональных данных других людей, сразу возникает проблема "права каждого человека на личную жизнь и защиту своих персональных данных". С другой стороны, есть некоторые персональные данные, которые по закону должны быть "общеизвестными". Например, сведения об имуществе кандидатов в депутаты и т.п. сведения. Возможны и другие случаи.

Следовательно, существуют разные персональные данные, часть из которых необходимо защищать. Согласно нашему законодательству, которое "идет в русле Европейского опыта", государство обязано обеспечить защиту прав граждан при обработке персональных данных. В отличие от того, что собственник конфиденциальной информации самостоятельно определял меры ее защиты, обеспечение безопасности любых персональных данных должно выполняться по государственным требованиям.

Актуальность защиты информации

Вернемся к вопросу об актуальности защиты информации в 21 веке. Как всем нам хорошо известно, именно с начала 21 века в России информатизация достигла огромных успехов и стала играть важную роль в жизни нашего общества. В данном случае нет необходимости говорить о преимуществах информатизации, покажем ее "обратную сторону". Информатизация связана с переводом в электронный и/или машиночитаемый вид огромных массивов информации.

Информатизация– это материализация человеческих (идеальных) мыслей в виде алгоритмов и программ обработки информации, реализуемых на компьютерах.

Вместе с тем, возможности современных информационных технологий позволяют хранить на физически маленьких устройствах (CD, DVD диски, флэш накопители и т.п.) огромные объемы информации. Как только мы переводим персональные данные в электронный вид, сразу же возникают угрозы того, что кто-то получит к ним доступ и будет использовать их во вред "субъекту". Каждый может сам оценить опасность разглашения своих персональных данных. Возможно нанесение морального и физического ущерба и финансовые потери. Например: политики могут лишиться своей должности; работодатель, получив сведения о здоровье или знакомствах, может отказать в приеме на работу; квартиру могут ограбить по "наводке" и т.п.

Таким образом, необходимо объективно согласиться с тем, что наравне с преимуществами, информатизация имеет и существенные недостатки. К этим недостаткам относится и "несанкционированный доступ", и возможность блокирования, уничтожения или других воздействий на важную информацию. Эти новые угрозы – угрозы 21 века, непосредственное порождение достижений и преимуществ информатизации.

Краткая история защиты информации

Однако с подобными угрозами по отношению к гражданам и их персональным данным, Россия сталкивалась и раньше, но в гораздо меньших объемах. С самого начала появления компьютеров (ЭВМ) на них обрабатывались и защищались конфиденциальная информация и сведения, составляющие государственную тайну. Например, Федеральной службе по техническому и экспортному контролю (ФСТЭК России, ранее Гостехкомиссии России и СССР), в прошлом году исполнилось 35 лет. По нашему законодательству, именно эта организация занимается "противодействием техническим разведкам и технической защитой информации". Если же вспомнить криптографию, за которую сейчас отвечает ФСБ России, то тут счет может идти уже на десятки и сотни лет. Главное отличие в том, что ранее эти организации занимались защитой гос. тайны, а теперь им поручено организовать обеспечение безопасности персональных данных. На наш взгляд, это объективно обусловленное решение и расширение сферы "технической защиты информации".

Исходя из этой объективной реальности, ФСТЭК России и ФСБ России подготовили требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. В основу был положен накопленный ранее опыт по защите гос. тайны и конфиденциальной информации. Напомним термины.

Лицензирование – разрешение на определенный вид деятельности.

Сертификация – процедура подтверждения соответствия, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация удостоверяет в письменной форме (сертификат), что продукция соответствует установленным требованиям.

Аттестация – комплексная проверка защищаемого объекта информатизации в реальных условиях эксплуатации. По результатам аттестации выдается «Аттестат соответствия», подтверждающий, что объект удовлетворяет требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Классификация информационных систем персональных данных

Все ИСПДн разбиты на 4 класса, модифицированное описание которых приведено подробно в Таблице 1.

Класс ИСПДн К1. Наиболее защищаемым является первый класс - К1, к которому предъявлены требования, в определенном смысле, аналогичные требованиям по защите государственной тайны, но самому "низкому" ее значению. Подобные системы существуют и успешно работают в государственных структурах и на предприятиях, выполняющих госзаказы с требованиями "защиты гос. тайны". "Жесткие" требования по защите гос. тайны направлены на защиту самого важного класса персональных данных. Таких систем персональных данных по К1 объективно не должно быть много, поэтому не будем останавливаться на них подробнее.

Класс ИСПДн К2. Наиболее распространенным считается следующий класс защиты: К2. К этому классу защиты предъявлены требования, в определенном смысле, аналогичные известному специалистам классу защиты "АС 1Г", т.е. по защите конфиденциальной информации. Еще в прошлом веке было создано достаточно много систем с такой защитой. Конечно, современные средства и технологии налагают новые требования по защите и по возможностям информационных систем персональных данных. Защитить информационные системы персональных данных по классу К2 можно, и подобные примеры известны. Особенно подчеркнем, что "первопроходцам" по защите персональных данных активно помогают сотрудники и ФСТЭК России, и ФСБ России - консультируют, согласовывают различные документы, хотя это не входит в их непосредственные обязанности. Сейчас все сотрудники этих организаций активно помогают и разъясняют требования документов по защите персональных данных. Кроме того, общеизвестна практика ФСТЭК России по регулярному внесению, при необходимости, изменений и дополнений в документы (РД).

Необходимость сертификации

Отметим, что одним из наиболее важных требований по защите К1 и К2 является сертификация программного обеспечения (ПО), которая требует существенных затрат от производителя и/или поставщика подобного ПО. По существу, такая сертификация - это тестирование ПО на соответствие требованиям по информационной безопасности. Такое тестирование объективно необходимо и не зависит от страны происхождения ПО. Понимая важность санитарных норм и соответствующих сертификатов на продукты питания, необходима "аналогичная" сертификация всего ПО, которое будет использовано в ИСПДн. Это требует дополнительных затрат, но и предоставляет необходимые гарантии, что такое "ПО с сертификатом" будет выполнять все заявленные функции, не делать ничего "лишнего" и не "быть дырявым решетом при защите ПДн". Отдельной проблемой является сертификация оборудования, подготовка помещения и аттестация ИСПДн.

На сегодняшний день подобных систем не так много. В качестве примера можно привести программное обеспечение "ЭЛАР САПЕРИОН", которое внесено в

Государственный реестр сертифицированных средств защиты информации. Анализ обеспечения безопасности персональных данных и защищенности информации в электронных информационных ресурсах, созданных на основе "ЭЛАР САПЕРИОН", показал, что возможно создание ИСПДн и их аттестация по требованиям ФСТЭК России до класса К1.

Класс ИСПДн К3. При защите по третьему классу К3 тоже есть определенные требования, но они значительно менее строгие, а соответственно и более легко реализуемые. Это объективно объясняется меньшими негативными последствиями от их разглашения.

Класс ИСПДн К4. Оценка соответствия проводится по решению Заказчика.

Таблица 1.

Модернизированное описание классов ИСПДн

Класс К1 ИСПДн 1) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни (ПДн категории 1), вне зависимости от количества субъектов ПДн. 2) Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (ПДн категории 2), при одновременной обработке в ИСПДн более чем 100 000 субъектов ПДн или ПДн субъектов персональных данных в пределах субъекта РФ или Российской Федерации в целом.
Класс К2 ИСПДн 1) Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных категории 1 (ПДн категории 2), при этом в ИСПДн одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн или ПДн субъектов персональных данных, работающих в отрасли экономики РФ, в органе гос. власти или проживающих в пределах муниципального образования. 2) Персональные данные, позволяющие идентифицировать субъекта ПДн (ПДн категории 3), при этом в ИСПДн одновременно обрабатываются персональные данные более чем 100 000 субъектов ПДн или ПДн субъектов персональных данных в пределах субъекта РФ или Российской Федерации в целом.
Класс К3 ИСПДн 1) Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (ПДн категории 2), при этом в ИСПДн одновременно обрабатываются данные менее чем 1000 субъектов ПДн или ПДн субъектов персональных данных в пределах конкретной организации. 2) Персональные данные, позволяющие идентифицировать субъекта ПДн (ПДн категории 3), при этом в ИСПДн одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн или ПДн субъектов ПДн, работающих в отрасли экономики РФ, в органе гос. власти, проживающих в пределах муниципального образования. 3) Персональные данные, позволяющие идентифицировать субъекта ПДн (ПДн категории 3), при этом в ИСПДн одновременно обрабатываются данные менее чем 1000 субъектов ПДн или ПДн субъектов персональных данных в пределах конкретной организации.
Класс К4 ИСПДн Обезличенные и (или) общедоступные ПДн, вне зависимости от количества субъектов ПДн.

Вывод

Персональные данные необходимо защищать и государство выполняет свои функции по формированию принципов и условий обеспечения безопасности персональных данных,

а также осуществлению контроля и надзора за их обработкой. На данном этапе для многих организаций требования по обеспечению безопасности ИСПДн являются новыми и, даже, "пугающими". Любая защита требует дополнительных гарантий (сертификатов и аттестации), а, следовательно – расходов, но это необходимая плата за соблюдение прав граждан и обеспечение безопасности их персональных данных.

O. O. Varlamov, E. G. Kolupaeva

ACTUAL PROBLEMS OF CERTIFICATION OF PROGRAMS, CLASSIFICATIONS AND ATTESTATIONS OF INFORMATION SYSTEMS OF THE PERSONAL DATA

The basic concepts are considered in the field of protection of the personal data, necessity of certification of programs is proved and the modified table of the description of classes of information systems of the personal data is given. The personal data are necessary for protecting and the state carries out its functions on formation of principles and conditions of a safety of the personal data, and also realization control and supervision of their processing. At the given stage the requirement on safety information systems of the personal data are new for many organizations and, even, "frightening". Any protection demands additional guarantees (certificates and certifications attestations), and, hence - charges, but it is a necessary payment for observance of rights of citizens and a safety of their personal data.

УДК 004.8.032.26

А. Н. Владимиров, О. О. Варламов, Е. Г. Колупаева, А. В. Носов

ОБ ОДНОМ ПОДХОДЕ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В БАЗАХ ДАННЫХ И ЭЛЕКТРОННЫХ АРХИВАХ

Рассмотрен подход к обеспечению безопасности персональных данных при их обработке в базах данных и электронных архивах.

Проблема обеспечения безопасности персональных данных (ПДн) регулируется федеральными законами: №152-ФЗ «О персональных данных» от 27 июля 2006 г. и №149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. Актуальность тематике придает то, что ИСПДн должны быть приведены в соответствие с требованиями закона не позднее 1 января 2010 года.

Проанализируем классификацию ИСПДн, которая имеет "многомерный характер", т.к. учитываются следующие исходные данные: категория данных, обрабатываемых в ИСПДн – Хпд; объем обрабатываемых ПДн (количество субъектов ПДн, персональные данные которых обрабатываются в информационной системе) - Хнпд; заданные оператором характеристики безопасности ПДн, обрабатываемых в информационной системе; структура информационной системы; наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена; режим обработки ПДн; режим разграничения прав доступа пользователей информационной системы; местонахождение технических средств информационной системы.

Необходимо упомянуть, что вводятся типовые и специальные ИСПДн. В типовых требуется обеспечение только конфиденциальности ПДн, а в специальных дополнительно требуется обеспечить хотя бы одну из характеристик безопасности ПДн: защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий. Существуют следующие классы типовых ИСПДн: К1, К2, К3, К4.

Класс К1 ИСПДн (значительные негативные последствия).

1) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни (ПДн категории 1), вне зависимости от количества субъектов ПДн.

2) Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (ПДн категории 2), при одновременной обработке в ИСПДн более чем 100 000 субъектов ПДн или ПДн субъектов персональных данных в пределах субъекта РФ или Российской Федерации в целом.

Класс К2 ИСПДн(негативные последствия).

1) Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (ПДн категории 2), при этом в ИСПДн одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн или ПДн субъектов персональных данных, работающих в отрасли экономики РФ, в органе гос. власти или проживающих в пределах муниципального образования.

2) Персональные данные, позволяющие идентифицировать субъекта ПДн (ПДн категории 3), при этом в ИСПДн одновременно обрабатываются персональные данные более чем 100 000 субъектов ПДн или ПДн субъектов персональных данных в пределах субъекта РФ или Российской Федерации в целом.

Класс К3 ИСПДн (незначительные негативные последствия).

1) Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (ПДн категории 2), при этом в ИСПДн одновременно обрабатываются данные менее чем 1000 субъектов ПДн или ПДн субъектов персональных данных в пределах конкретной организации.

2) Персональные данные, позволяющие идентифицировать субъекта ПДн (ПДн категории 3), при этом в ИСПДн одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн или ПДн субъектов ПДн, работающих в отрасли экономики РФ, в органе гос. власти, проживающих в пределах муниципального образования.

3) Персональные данные, позволяющие идентифицировать субъекта ПДн (ПДн категории 3), при этом в ИСПДн одновременно обрабатываются данные менее чем 1000 субъектов ПДн или ПДн субъектов персональных данных в пределах конкретной организации.

Класс К4 ИСПДн (не приводит к негативным последствиям)**.** Обезличенные и (или) общедоступные ПДн, вне зависимости от количества субъектов ПДн.

Мероприятия по защите ПДн

Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства. В общем случае, необходимо следующее: проведение мероприятий по предотвращению НСД к ПДн; своевременное обнаружение фактов НСД к ПДн; недопущение воздействия на технические средства ИСПДн, в результате которых может быть нарушено их функционирование; обеспечение возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД; реализация постоянного контроля за обеспечением уровня защищенности ПДн.

Отметим, что все мероприятия по защите ПДн можно разделить на:

1) организационные (по организации обеспечения безопасности);

2) технические (по техническому обеспечению безопасности).

В свою очередь, в рамках технического обеспечения безопасности ПДн реализуют следующие мероприятия:

2.1) по защите от НСД к ПДн при их обработке в ИСПДн;

2.2) по защите информации от распространения по техническим каналам (ПЭМИН, акустика и т.п.).

Известен классический подход к технической защите информации, который реализован и для ИСПДн: 1) выявляют угрозы, 2) создают систему защиту от этих угроз и 3) контролируют защищенность ПДн. Для защиты ИСПДн прежде всего разрабатывается "Модель угроз" по методике определения актуальных угроз безопасности ПДн и на основе "Базовой модели угроз". Это обусловлено тем, что выявление и учет угроз в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных обеспечение безопасности ПДн при их обработке в ИСПДн. Подчеркнем, что именно на этом этапе определяется основная стоимость проектируемой системы защиты ПДн. Если обосновать исключение отдельных угроз, то можно будет сэкономить.

В состав мероприятий по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий входят: защита от НСД при однопользовательском режиме обработки ПДн; защита от НСД при многопользовательском режиме обработки ПДн и равных правах доступа к ним субъектов доступа; защита от НСД при многопользовательском режиме обработки ПДн и разных правах доступа к ним субъектов доступа; защита информации при межсетевом взаимодействии ИСПДн; антивирусная защита; обнаружение вторжений.

Подсистемы обеспечения безопасности ПДн

Мероприятия по защите ПДн реализуются в рамках 6 подсистем, среди которых первые 4 хорошо известны по защите конфиденциальной информации, а последние 2 официально добавлены впервые, хотя также применялись и ранее:

1) управления доступом;
2) регистрации и учета;
3) обеспечения целостности;
4) криптографической защиты;
5) антивирусной защиты;
6) обнаружения вторжений (по требованиям ФСБ).

Отметим, что в РД ФСТЭК России в явном виде неоднократно подчеркнуто, что должна проводиться сертификация ПО ИСПДн на НДВ, а также анализ защищенности системного и прикладного ПО в ходе периодического инспекционного контроля. Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется оператором в зависимости от ущерба. Для остальных классов эти мероприятия определены в документах ограниченного доступа. Можно только привести некоторые требования.

Например, для ИСПДн К1 и К2: обязательная сертификация и аттестация, а также надо реализовать мероприятия по защите ПДн от ПЭМИН. В ИСПДн К1 рекомендуется использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств. Если есть голосовой ввод или подобное, то должны быть реализованы мероприятия по защите акустической (речевой) информации.

В ИСПДн К2 для обработки информации рекомендуется использовать СВТ, удовлетворяющие требованиям стандартов РФ по электромагнитной совместимости, по безопасности и эргономике средств отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ.

Общие требования по защите ИСПДн

Можно привести следующие общие требования для ИСПДн. Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации – СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение – ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ (по мнению специалистов – это "НДВ-4"). Анализ защищенности должен проводиться путем использования в составе ИСПДн программных

или программно-аппаратных средств (систем) анализа защищенности (САЗ). Для исключения просмотра текстовой и графической видовой информации рекомендуется оборудовать помещения шторами (жалюзи). Специалистами предложено следующее соотношение требований по защите автоматизированных систем (АС) и ИСПДн:

К3 - "1Д";
К2 - "1Г";
К1 - "1В".

Как видим, защита ИСПДн К1 аналогична защите гос. тайны, а защита ИСПДн К2 аналогична защите конфиденциальной информации.

Создание защищенных электронных архивов и баз данных

Рассмотрим конкретные научно-практические аспекты создания защищенных электронных архивов (ЭА) и традиционных баз данных (БД) на основе системы управления электронными информационными ресурсами ЭЛАР САПЕРИОН. Изначальная ориентация системы на гарантированное долгосрочное архивное хранение электронных документов, включая отсканированные образы бумажных документов, обусловила те функциональные возможности, которыми с точки зрения обеспечения безопасности информации не обладают представленные на российском рынке системы управления документами. ЭЛАР САПЕРИОН имеет мощные средства разграничения и контроля доступа к документам на уровне пользователей и групп пользователей, осуществляет мониторинг и ведет журнал всех действий пользователей в соответствии с их правами, всех изменений, произведенных с документами.

Для аттестации ИСПДн выдвигается довольно много требований, которые напрямую не относятся к программному обеспечению, но должны быть выполнены Оператором независимо от специфики АС. Отметим, что для наиболее распространенных (из требующих обязательной аттестации) ИСПДн К2 аттестация по сути аналогична хорошо известной "аттестации АС 1Г", т.е. для систем обработки конфиденциальной информации. С точки зрения поставщика программного обеспечения "ЭЛАР САПЕРИОН" невозможно реализовать защиту от многих угроз. Это обусловлено тем, что такие угрозы не распространяются непосредственно на "ЭЛАР САПЕРИОН", хотя могут воздействовать опосредованно, например, вирусы через операционную систему.

Действия поставщика программного обеспечения для аттестации ИСПДн

Проанализируем, какие действия может выполнить поставщик программного обеспечения для аттестации ИСПДн. До любой аттестации необходимо провести сертификацию или использовать ранее сертифицированные компоненты программного обеспечения (операционные системы - ОС, системы управления базами данных - СУБД, и т.п.).

Таким образом, поставщик программного обеспечения должен:

1) провести необходимую обязательную сертификацию по НДВ;
2) для сложного программного обеспечения, в котором есть встроенные средства защиты информации (операционные системы, СУБД и т.п.), провести сертификацию по СВТ;
3) показать работоспособность на необходимом Оператору аппаратном обеспечении ("железо"), которое при необходимости проходит специальные проверки и исследования;
4) обеспечить взаимодействие своего программного обеспечения с необходимым Оператору сертифицированным программным обеспечением (ОС, СУБД и т.п.);
5) обеспечить совместимость с другими внешними средствами защиты информации (криптография и ЭЦП).

Вывод

Защита ИСПДн К1 аналогична защите гос. тайны, а защита ИСПДн К2 аналогична защите конфиденциальной информации. Таким образом, для ИСПДн К2 аттестация по сути аналогична хорошо известной "аттестации АС 1Г". Анализ обеспечения безопасности персональных данных и защищенности информации в электронных архивах, созданных на основе сертифицированного "ЭЛАР САПЕРИОН", показал, что возможно создание ИСПДн и их аттестация по требованиям ФСТЭК России до класса К1 (сертификат соответствия №1638).

A.N. Vladimirov, O. O. Varlamov, E. G. Kolupaeva, A.V. Nosov

ABOUT ONE APPROACH TO THE SAFETY OF THE PERSONAL DATA AT THEIR PROCESSING IN DATABASES AND ELECTRONIC ARCHIVES

The base of a safety of personal data are federal laws: № 152-FZ «About the personal data » from July, 27, 2006 and № 149-FZ «About the information, information technologies and about protection of the information » from July, 27, 2006. It is known the classical approach to technical protection of the information which is realized and for personal data: 1) reveal threats, 2) create system protection against these threats and 3) supervise security personal data. "The Model of threats" first of all is developed for protection personal data by a technique of definition of actual threats of safety personal data and on a basis of "Base model of threats". It is caused that revealing and the account of threats in concrete conditions make a basis for planning and realization of the actions, directed for safety personal data at their processing in information system personal data. The analysis of a safety of the personal data and securities of the information in the electronic archives created on the basis of certificated "ELAR SAPERION", has shown, that it is possible to create of in information system personal data and their certification for requirements FSTECof Russia up to class K1.

УДК 004.056

С.И. Ивашутин

ПОРЯДОК РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

В статье делается краткий обзор законодательства и актуальных требований в области обработки и защиты персональных данных, а также выдвигаются практические рекомендации по защите таких данных.

Обрабатывая персональные данные, организация (оператор ПДн) должна придерживаться требований ФЗ № 152 «О персональных данных», в котором сказано, что «оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных». Статья 25 того же закона говорит о том, что информационные системы предприятий и организаций, обрабатывающие персональные данные должны быть приведены в соответствие не позднее 1 января 2010 г. В связи с этим у оператора персональных данных возникает проблема реализации требований на своей информационной системе персональных данных. В данной статье будет проведен обзор актуальных требований по защите и обработке персональных данных, а также предложена практическая реализация требований.

Ряд требований выдвигает положение правительства «об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК также накладывает свои требования на защиту персональных данных в

виде четырех нормативно-методических документов. Данные НМД регламентируют порядок классификации информационных систем персональных данных, анализа угроз и создания системы защиты персональных данных.

Предварительные действия оператора

Прежде чем приступить к обработке персональных данных, необходимо уведомить Уполномоченный орган по защите прав субъектов ПДн (Управление Россвязькомнадзора) о своем намерении. То есть зарегистрировать свою организацию, как оператора персональных данных в государственном реестре. Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных.

Классификация информационных систем ПДн

С целью дифференцированного подхода к защите персональных данных, необходима классификация информационных систем. Классифицируя информационные системы персональных данных, необходимо учитывать следующие данные:

- категория обрабатываемых в информационной системе персональных данных.
- количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе
- структура информационной системы
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена
- режим обработки персональных данных
- режим разграничения прав доступа пользователей информационной системы
- местонахождение технических средств информационной системы

Персональные данные подразделяются на категории:

- категория 1 — ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 — ПД, позволяющие идентифицировать субъекта персональных данных и получить о нём дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 — персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 — обезличенные и (или) общедоступные ПД.

Например, отдельно фамилия является данными 4-й категории, сочетание фамилии и адреса — третьей, фамилия, адрес, номера страховок и карт — второй, а если к этим данным добавлена электронная медкарта, то получившиеся персональные данные относятся исключительно к первой категории.

В зависимости от объема обрабатываемых данных информационные системы персональных данных (ИСПДн) делятся:

1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

ИСПДн по характеристикам безопасности подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам относят:

- информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;
- информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Далее информационной системе присваивается один из следующих классов:

- класс 1 (К1) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Порядок защиты персональных данных

Как известно, любая система защиты начинается с предварительного анализа, который включает в себя:

1. Анализ информационных ресурсов:

- определение состава, содержания и местонахождения ПДн, подлежащих защите;
- категорирование ПДн;
- оценка выполнения обязанностей по обеспечению безопасности ПДн оператором.

2. Анализ уязвимых звеньев и возможных угроз безопасности ПДн:

- оценка возможности фактического доступа;
- выявление возможных технических каналов утечки информации;
- анализ возможностей программно-математического воздействия на ИСПДн;
- анализ возможностей электромагнитного воздействия на ПДн, обрабатываемых в ИСПДн.

3. Оценка ущерба от реализации угроз (оценка непосредственного и опосредованного ущерба от реализации угроз безопасности ПДн).

4. Анализ имеющихся в распоряжении мер и средств защиты ПДн:

- от физического доступа;
- от утечки по техническим каналам;
- от несанкционированного доступа;
- от программно-математических воздействий;
- от электромагнитных воздействий.

Также необходимо проанализировать необходимость обеспечения безопасности ПДн от угроз:

- уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;
- утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН);
- перехвата при передаче по проводным (кабельным) линиям связи;
- хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- воспрепятствования функционированию ИСПДн путем преднамеренного электромагнитного воздействия на ее элементы;
- непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неатропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

Далее выбирается политика защиты персональных данных. Сюда входит:

1) Определение основных направлений по защите ПДн:

- по подразделениям;
- по указанным звеньям, направлениям защиты;
- по категориям ПДн.

2) Выбор способов защиты по направлениям защиты:

- по актуальным угрозам;
- по возможности реализации с учетом затрат.

3) Решение основных вопросов управления защитой ПДн:

- организация охраны;
- организация служебной связи и сигнализации;
- организация взаимодействия;
- организация резервного копирования программного и аппаратного обеспечения;
- организация управления администрированием.

4) Решение основных вопросов обеспечения защиты ПДн:

- финансового;
- технического и программного;

- информационного;
- кадрового.

В рамках политики защиты персональных данных необходимо решить следующие вопросы:

- распределить функции управления доступом к данным и их обработки между должностными лицами;
- определить порядок изменения правил доступа к защищаемой информации;
- определить порядок изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
- определить порядок действий должностных лиц в случае возникновения нештатных ситуаций;
- определить порядок проведения контрольных мероприятий и действий по его результатам.

Затем оператором персональных данных проводится организация работ по созданию системы защиты ПДн (СЗПДн). СЗПДн приводится в соответствие требованиям изложенных в НМД ФСТЭК «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных».

Требования предъявляются к следующим элементам:

- системе управления доступом;
- системе регистрации и учета;
- обеспечения целостности;
- криптографической защиты;
- антивирусной защиты;
- межсетевому экранированию;
- обнаружению вторжений.

Также оператору ПДн следует разработать некоторую документацию. В обязательном порядке разрабатываются:

- положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- требования по обеспечению безопасности ПДн при обработке в ИСПДн;
- должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

В процессе развертывания и ввода опытную эксплуатацию ИСПДн в соответствии с частным техническим заданием проводятся испытания СЗПДн. Заключение по результатам испытаний должно содержать вывод о степени соответствия СЗПДн заданным требованиям по обеспечению безопасности ПДн. Далее возможна доработка СЗПДн.

Как отмечают эксперты, к 1 января 2010 г. вряд ли будут зарегистрированы все операторы персональных данных. Главными препятствиями являются высокая стоимость реализации технической защиты; нежелание оказаться под контролем со стороны еще нескольких органов исполнительной власти; неясные последствия отказа от выполнения требований закона для органов власти, бизнеса и руководителей. Иногда дешевле будет заплатить штраф, но не усложнять информационную систему и не вкладывать деньги в ее защиту; отсутствие в нашей стране примеров реальной потери репутации компании в результате утечки персональных данных; отсутствие четкого понимания процедуры государственного контроля и надзора за безопасностью ПД, влияние этого контроля на деятельность предприятий и организаций.

S.I. Ivashutin

PERSONAL DATA PROCESSING TECHNOLOGY

In article the short review of the legislation and actual requirements in the field of processing and protection of personal data becomes, and also practical recommendations about protection of such data are put forward

РЕШЕНИЕ КОНФЕРЕНЦИИ

Оргкомитет выражает благодарность всем участникам, предоставившим свои доклады для публикации.

Участники конференции, представляющие Россию и ближнее зарубежье, показали достаточно высокий уровень работ в предметной области. Оргкомитет выражает надежду на дальнейшее сотрудничество и напоминает, что конференция «Актуальные проблемы безопасности информационных технологий», призванная стать одним из центров научного сотрудничества в Сибири, будет проводиться регулярно, в сентябре-октябре, причем возможно как очное, так и заочное участие студентов, аспирантов, сотрудников и специалистов организаций России и других государств в работе конференции.

Результаты, полученные в научных и научно-практических исследованиях, опубликованные в сборнике, представляют особый интерес, поскольку дают возможность связать науку, в том числе и студенческую, с реальными практическими задачами.

Оргкомитет

ИНФОРМАЦИЯ ОБ УЧАСТНИКАХ КОНФЕРЕНЦИИ

Секция 1. «Криптографические методы и средства защиты информации»

А.Т. Алиев, А.Н. Щербакова
СТЕГАНОГРАФИЧЕСКИЙ МЕТОД СИНОНИМИЧНЫХ ПРЕОБРАЗОВАНИЙ ОТКРЫТОГО ТЕКСТА С УЧЕТОМ КОНТЕКСТА
Донской государственный технический университет
Россия, Ростов-на-Дону
stego@inbox.ru, lilo-neil@ya.ru

С.С. Барильник, И.В. Минин, О.В. Минин
ПРИМЕНЕНИЕ АЛГОРИТМОВ СТЕГАНОГРАФИИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ
Новосибирский государственный технический университет
Россия, Новосибирск
krutoystas@mail.ru, igor.minin@ngs.ru

Р. Г. Бияшев, Н. А. Капалова, С. Е. Нысанбаева
РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДИФИЦИРОВАННОГО АЛГОРИТМА ДИФФИ–ХЕЛЛМАНА НА БАЗЕ МОДУЛЯРНОЙ АРИФМЕТИКИ
Институт проблем информатики и управления
Казахстан, Алматы
brg@ipic.kz, Kapalova@ipic.kz, nyssanbayeva@ipic.kz

Д.В. Малухин
ПРОТОКОЛ СМЕНЫ КЛЮЧЕВОЙ ИНФОРМАЦИИ ДЛЯ ПРОЗРАЧНОГО ШИФРОВАНИЯ СИГНАЛА УПРАВЛЕНИЯ КОСМИЧЕСКИМ АППАРАТОМ
Сибирский государственный аэрокосмический университет
Россия, Красноярск
khvkh@mail.ru

К.В. Мушовец
МОДИФИКАЦИЯ ПРОТОКОЛА АУТЕНТИФИКАЦИИ СНАР ДЛЯ ПРОТИВОДЕЙСТВИЯ НЕКОТОРЫМ ТИПОВЫМ АТАКАМ
Сибирский государственный аэрокосмический университет
Россия, Красноярск
amida@land.ru

Подколзин В.В., Осипян В.О.
ВЕРХНЯЯ ГРАНИЦА ЧИСЛА РЕШЕНИЙ ОБОБЩЕННОЙ ЗАДАЧИ О РЮКЗАКЕ НА ЗАДАННОМ ВХОДЕ
Кубанский государственный университет
Россия, Краснодар
rrwo@mail.ru, vvp_35@mail.ru

Т. А. Чалкин, К. М. Волощук
АЛГОРИТМ ПОСТРОЕНИЯ УЗЛОВ ЗАМЕН АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147-89
Сибирский государственный аэрокосмический университет
Россия, Красноярск
booroo@rambler.ru

А. Н. Шниперов
СИНТЕЗ ХЭШ-ФУНКЦИЙ НА ОСНОВЕ БЛОЧНЫХ ПРЕОБРАЗОВАНИЙ С ИСПОЛЬЗОВАНИЕМ УПРАВЛЯЕМЫХ ОПЕРАЦИЙ
Сибирский федеральный университет,
Россия, Красноярск
stekmain@mail.ru

Секция 2. «Оптимизация, моделирование и разработка систем защиты информации. Подготовка специалистов в области безопасности информационных технологий. Информационные технологии: теоретические и прикладные аспекты»

С. В. Белим, Н. Ф. Богаченко
ИЕРАРХИЧЕСКИЕ СТРУКТУРЫ РОЛЕВОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА
Омский государственный университет
Россия, Омск
sbelim@mail.ru, nfbogachenko@mail.ru

С.С. Валеев, М.Ю. Дьяконов
ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ МИКРОЯДЕРНОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
Уфимский государственный авиационный технический университет
Россия, Уфа
dyakonov_maksim@mail.ru

Е.В. Горковенко
РАЗРАБОТКА МОДУЛЬНОЙ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ ОБЩЕГО И ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ
Институт космических исследований
Казахстан, Алматы
gev@ipic.kz

В. Г. Жуков, М. Н. Жукова, А. П. Стефаров
ПОСТРОЕНИЕ МОДЕЛИ СИСТЕМЫ РЕАГИРОВАНИЯ ДЛЯ СЕТЕВЫХ СИСТЕМ ОБНАРУЖЕНИЯ АТАК
Сибирский государственный аэрокосмический университет
Россия, Красноярск
vadimzhukov@mail.ru

В. Г. Жуков, Н. Ю. Паротькин
ПРИМЕНЕНИЕ МОДИФИЦИРОВАННОГО ГЕНЕТИЧЕСКОГО АЛГОРИТМА ДЛЯ ОПТИМИЗАЦИИ СТРУКТУРЫ СЕТИ WI-FI
Сибирский государственный аэрокосмический университет
Россия, Красноярск
vadimzhukov@mail.ru

В. В. Золотарев, Н.С. Заблоцкая
ПРИМЕНЕНИЕ ФАКТОРНОГО АНАЛИЗА ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
Сибирский государственный аэрокосмический университет

Россия, Красноярск
amida@land.ru

А. А. Калинин
СЛОГОВОЙ МЕТОД ГЕНЕРАЦИИ ПАРОЛЕЙ
Сибирский государственный аэрокосмический университет
Россия, Красноярск
verbalab@yandex.ru

Ф.Ю. Кулишов
АЛГОРИТМЫ СИГНАТУРНОГО АНТИВИРУСНОГО ПОИСКА ДЛЯ СОВМЕРЕННЫХ SIMD-ПРОЦЕССОРОВ
Московский инженерно-физический институт (Национальный исследовательский ядерный университет)
Россия, Москва
feodor.kulishov@gmail.com

И. А. Лубкин, К. В. Якименко
ОБЗОР МЕТОДОВ ЗАЩИТЫ ПРОГРАММ И ИХ ПРЕОДОЛЕНИЯ
Сибирский государственный аэрокосмический университет
Россия, Красноярск
lubkin@rambler.ru

А.Н. Мироненко, С.В. Белим
ВЫЯВЛЕНИЕ СПАМ-СООБЩЕНИЙ В ПОТОКЕ ЭЛЕКТРОННОЙ ПОЧТЫ
Омский государственный университет
Россия, Омск
mironim84@mail.ru

А.П. Никитин, С.С. Валеев, В.В. Озеров
СИСТЕМА ОГРАНИЧЕНИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНТЕРНЕТ-САЙТАМ
Уфимский государственный авиационный технический университет
Россия, Уфа
ciso.ru@gmail.com, vss2000@mail.ru

А.П. Никитин, В.В. Озеров
ИЕРАРХИЧЕСКОЕ ФОРМИРОВАНИЕ БАЗ ЗНАНИЙ СИСТЕМЫ СПАМ-ФИЛЬТРАЦИИ
Уфимский государственный авиационный технический университет
Россия, Уфа
ciso.ru@gmail.com

Ракицкий Ю.С., Белим С.В.
МОДЕЛИРОВАНИЕ РОЛЕВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ СО СТАНДАРТОМ СТО БР ИББС-1.0-2008
Омский государственный университет
Россия, Омск
sbelim@mail.ru

Е. Ю. Федорова, Т. А. Чалкин
РАЗРАБОТКА АЛГОРИТМА АВТОМАТИЧЕСКОЙ КЛАССИФИКАЦИИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Сибирский государственный аэрокосмический университет
Россия, Красноярск
booroo@rambler.ru

Т.К. Юлдашев
НЕЯВНОЕ ЭВОЛЮЦИОННОЕ ИНТЕГРАЛЬНОЕ УРАВНЕНИЕ ВОЛЬТЕРРА ПЕРВОГО РОДА
Ошский государственный юридический институт
Кыргызстан,Ош
tursunbay@rambler.ru

Т.К. Юлдашев, Ж.К. Акматалиев
ПРАВОВЫЕ НОРМЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ: НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ
Ошский государственный юридический институт
Кыргызстан,Ош
tursunbay@rambler.ru

Секция 3. «Защита персональных данных в информационных системах»

Р.М. Алгулиев, Я.Н. Имамвердиев, Ф.Д. Абдуллаева
ВЕКТОР АТАКИ И ЗАЩИТНЫЕ МЕРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
Институт Информационных Технологий, Национальная академия наук Азербайджана
Азербайджан, Баку
secretary@iit.ab.az, yadigar@lan.ab.az, farqana@iit.ab.az

О.О. Варламов
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И АНАЛИЗ ДЕВЯТИ ВИДОВ ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ РАЗВЕДКИ
ООО "МИВАР"
Россия, Москва
ovar@narod.ru, ovarlamov@elar.ru

О. О. Варламов, Е. Г. Колупаева
АКТУАЛЬНЫЕ ПРОБЛЕМЫ СЕРТИФИКАЦИИ ПРОГРАММ, КЛАССИФИКАЦИИ И АТТЕСТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ
ЗАО "Электронный архив"
Россия, Москва
ekolupaeva@elar.ru; ovar@narod.ru

А.Н. Владимиров, О.О. Варламов, Е.Г. Колупаева, А.В. Носов
ОБ ОДНОМ ПОДХОДЕ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В БАЗАХ ДАННЫХ И ЭЛЕКТРОННЫХ АРХИВАХ
ООО "МИВАР"
Россия, Москва
ovar@narod.ru, ovarlamov@elar.ru

С. И. Ивашутин
ПОРЯДОК РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ
Сибирский государственный аэрокосмический университет
Россия, Красноярск
_fluffy_07@mail.ru

ПРИЛОЖЕНИЯ

Приложение 1

Федеральное агентство по образованию Российской Федерации
Сибирский государственный аэрокосмический университет

ИНФОРМАЦИОННОЕ ПИСЬМО

IV научно-техническая конференция
«Актуальные проблемы безопасности информационных технологий»
(АПроБИТ-2010)

10-12 ноября 2010 г.

ПРЕДПОЛАГАЕМАЯ ПРОГРАММА КОНФЕРЕНЦИИ

Секция 1. **Криптографические методы и средства защиты информации** (председатель секции О.Н. Жданов)

Секция 2. **Оптимизация, моделирование и разработка систем защиты информации** (председатель секции В.В. Золотарев)

Секция 3. **Подготовка специалистов в области безопасности информационных технологий. Информационные технологии: теоретические и прикладные аспекты** (председатель секции В.Х. Ханов)

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Вейсов Е.А. – к.т.н., проф., проректор по информатизации Сибирского государственного аэрокосмического университета (председатель)
Маковецкий А.А. – зам. начальника Центра специальной связи и информации Федеральной службы охраны РФ по Красноярскому краю (зам. председателя) – по согласованию
Попов А.М. – д.ф.-м..н., проф., директор института информатики и телекоммуникаций Сибирского государственного аэрокосмического университета (зам. председателя)
Золотарев В.В. – к.т.н., заместитель директора Института информатики и телекоммуникаций Сибирского государственного аэрокосмического университета (ответственный секретарь конференции)
Ханов В.Х. – к.т.н., доцент, зав. каф. безопасности информационных технологий Сибирского государственного аэрокосмического университета
Жданов О.Н. – к.ф.-м.н., доцент Сибирского государственного аэрокосмического университета
Жуков В.Г. – к.т.н., доцент Сибирского государственного аэрокосмического университета
Лубкин И.А. – ассистент каф. безопасности информационных технологий Сибирского государственного аэрокосмического университета
Буторов В.В. – инженер каф. безопасности информационных технологий Сибирского государственного аэрокосмического университета

ОБЩАЯ ИНФОРМАЦИЯ

Рабочие языки конференции – русский и английский. При подаче материалов на английском языке порядок публикации согласуется с оргкомитетом по электронной почте.

Статьи рецензируются. По результатам закрытого рецензирования (результаты не обсуждаются и не высылаются авторам) будут разосланы приглашения и реквизиты для оплаты оргвзноса. При отклонении доклада из-за несоответствия тематике, нарушения сроков или требований оформления доклады не публикуются.

Заявкой для участия в конференции являются: заполненная регистрационная форма (прилагается ниже), текст доклада и экспертное заключение о возможности опубликования в открытой печати. Регистрационная форма и доклады высылаются в адрес оргкомитета в электронном виде по электронной почте; экспертное заключение высылается обязательно в печатном виде на почтовый адрес оргкомитета.

Объем докладов не более 4 страниц в формате Microsoft Word. Доклады объемом более 4 страниц представляются по согласованию с оргкомитетом.

Материалы должны быть отправлены по электронной почте до **06 мая 2010 года** по адресу: Золотареву В.В., amida@land.ru; продублировать по адресу: Жданову О.Н., ONZhdanov@mail.ru. Экспертные заключения в печатном виде должны поступить до конца мая.

Сборник трудов конференции будет издан к началу работы конференции. При заочном участии сборник высылается почтой.

КОНТРОЛЬНЫЕ ДАТЫ

6 мая 2010 г. заканчивается прием материалов от участников конференции;

11 мая 2010 г. заканчивается предварительная экспертиза и высылаются по электронной почте ее результаты;

31 мая 2010 г. заканчивается прием платежей от получивших положительные рецензии участников конференции;

Сентябрь 2010 г. издание сборника трудов конференции.

Адрес оргкомитета конференции:

660014, Красноярск, пр. им. газ. «Красноярский рабочий», 31, СибГАУ, ФИСУ, кафедра БИТ.

Сайт конференции: www.fisu.ru/aprobit

Контактные телефоны и электронная почта:

Тел. (391) 2-919-148 – ответственный секретарь оргкомитета Золотарев Вячеслав Владимирович**,** amida@land.ru

Тел. (391) 2-621-847 – Жданов Олег Николаевич**,** ONZhdanov@mail.ru

Тел. (391) 2-645-517 – Ханов Владислав Ханифович, khvkh@mail.ru

ОРГАНИЗАЦИОННЫЙ ВЗНОС

Организационный взнос за каждую публикацию составляет 150 рублей за страницу доклада. Организационный взнос оплачивается только после получения положительной рецензии на текст доклада. Сумма организационного взноса включает оплату рассылки информационных материалов, рецензирование, оплату сборника докладов конференции, НДС.

Приложение 2

РЕГИСТРАЦИОННАЯ ФОРМА[*]

на участие в IV научно-технической конференции
«Актуальные проблемы безопасности информационных технологий»
(АПроБИТ-2010)

1. Фамилия, имя, отчество
2. Организация
3. Должность (с указанием ученой степени, звания)
4. Город, страна, индекс
5. Почтовый адрес (домашний, для рассылки сборника трудов)
6. E-mail

[*)] Регистрационная форма высылается в адрес секретаря оргкомитета Конференции только **по электронной почте**.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ДОКЛАДОВ

Общие требования. Тексты представляются в электронном виде.

Количество авторов одной статьи не более 5-ти. Автор имеет право публиковаться в сборнике один раз, второй в соавторстве.

Индекс УДК предшествует названию статьи, соответствует заявленной теме и проставляется в верхнем левом углу листа.

Текст доклада набирается в программе Microsoft Word.

Содержание. В тексте необходимо сформулировать проблемы, отразить объект исследования, достигнутый уровень процесса исследования, новизну результатов, область их применения, перспективы.

Доклад должен заканчиваться выводом. Текст вывода набирается отдельным абзацем (абзацами), акцентируется новизна результатов, эффективность использования и др.

Объем текста доклада: не более 4 страниц (включая рисунки, таблицы и библиографический список).

Параметры страницы. Формат А4 (210х297). Поля: правое и левое - 2 см., верхнее и нижнее - 2,5 см.

Текст. Шрифт - Times New Roman, размер 12 пт. По центру набираются инициалы, фамилия автора(ов). Ниже по центру шрифтом 12 пт печатается название статьи и через строку (курсивом) - резюме.

Не допускается (!) набирать тексты прописными (заглавными) буквами и жирным шрифтом, а также размещать все указанные элементы в рамках и имитировать оформления набора, выполняемого в журнале.

Основной текст статьи размещается через пробел от резюме. Межстрочный интервал - одинарный, межбуквенный и междусловный интервал - нормальный, перенос слов не допускается. Заголовки глав должны быть центрированы.

Абзацный отступ равен 0,5 см.

Ссылки на литературные или иные источники оформляются числами, заключенными в квадратные скобки, например [1]. Ссылки должны быть последовательно пронумерованы.

Примечания: 1. Смысловые пояснения основного текста или дополнения к нему оформляются в виде внутритекстовых примечаний среди строк основного текста специальной рубрикой, выделенной светлым курсивом: *Примечание:* (одно примечание*), Примечания*: (несколько примечаний). Отделяются от текста *точкой* (если стоят в единственном числе в подбор к тексту примечания).

Примечания должны быть последовательно пронумерованы.

При наличии гранта ссылка на грант помещается внизу полосы под строками основного текста (подстрочное примечание).

Формулы. Простые внутристрочные и однострочные формулы должны быть набраны без использования специальных редакторов - символами (шрифт Symbol). Специальные сложные символы, а также многострочные формулы, которые не могут быть набраны обычным образом, должны быть набраны в редакторе формул Microsoft Equation 3.0. Набор математических формул в пределах всего текста должен быть единообразен:

- русские и греческие символы - прямым шрифтом,
- латинские - курсивом.

Размер обычного символа - 12 пт, крупный индекс - 10 пт, мелкий индекс - 9 пт, крупный символ - 11 пт, мелкий символ - 10 пт.

Формулы, набранные отдельными строками, располагают по центру.

Не допускается (!) набор в основном тексте статьи простых латинских, греческих или специальных символов в редакторе формул.

Таблицы должны быть последовательно пронумерованы. Слово «таблица» набирается светлым курсивом с выравниванием вправо, шрифтом 11, например, *Таблица 1* ниже - заглавие таблицы (набирается жирным шрифтом по центру). Если таблица имеет большой объем, она может быть помещена на отдельной странице, а в том случае, когда она имеет значительную ширину - на странице с альбомной ориентацией.

Иллюстрации оформляются отдельным файлом с расширением tiff. Последовательно пронумеровываются обычным шрифтом без кавычек с выравниванием по центру, например, Рис. 1. Могут содержать подрисуночную подпись, шрифтом 11 пт. Иллюстрации могут быть отсканированы с оригинала (в градациях серого с разрешением 150 dpi) или выполнены средствами компьютерной графики. Не принимаются цветные иллюстрации или с разрешением 300 dpi и более.

Библиографический список составляется в соответствии с действующими требованиями к библиографическому описанию и помещается после основного текста.

Текст на английском языке приводится в конце статьи и содержит в себе перевод заглавия статьи, фамилию автора, название организации и резюме.

ПРИМЕР ОФОРМЛЕНИЯ СТАТЬИ

УДК 621.396.96.001(07)

И. А. Иванов

ДЕЦЕНТРАЛИЗОВАННЫЕ АЛГОРИТМЫ ОБРАБОТКИ ИНФОРМАЦИИ В ДВУХКАНАЛЬНЫХ ИЗМЕРИТЕЛЬНЫХ СИСТЕМАХ[1]

Рассматривается децентрализованная обработка информации в двухканальных измерительных системах при косвенном измерении для различных алгоритмов фильтрации оценки вектора состояния в измерительных пунктах и пункте обработки информации.

Задача обеспечения высокой точности оценивания координат и параметров траектории движения объекта может быть решена за счет применения многоканальных измерительных систем с оптимальной централизованной обработкой.

(Продолжение текста публикуемого материала)

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 00 - 01 - 00912).

Библиографический список

1. Гришин, Б. П. Динамические системы, устойчивые к отказам / Б. П. Гришин, Ю. М. Казаринов. М.: Радио и связь, 1985. – 76 с.

2. Медведев, А. В. О моделировании организационных процессов / А. В. Медведев // Вестник Сибирской аэрокосмической академии имени академика М. Ф. Решетнева : сб. науч. тр. / САА. Вып. 1. Красноярск, 2000. с. 173-191.

I. A. Ivanov

DECENTRALIZED ALGORITHMS OF INFORMATION PROCESSING IN TWO-CHANNEL MEASURE SYSTEMS

It is covered a decentralized algorithms of information processing in two-channel measure systems in case of an indirect measuring for different filtration algorithms of a condition vector estimation at the reception measure station and the station of information processing. Comparative analysis is carried out with a help of imitation modeling of synthesized algorithms.

Научное издание

АКТУАЛЬНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Материалы III Международной научно-практической конференции

Печатается в авторской редакции
Компьютерная верстка

Подп. в печать . .2009. Формат 70×108/8. Бумага офсетная.
Печать плоская. Усл. печ. л. . Уч.-изд. л. .
Тираж 100 экз. Заказ . С 38/7.

Редакционно-издательский отдел Сиб. гос. аэрокосмич. ун-та.
Отпечатано в отделе копировально-множительной техники
Сиб. гос. аэрокосмич. ун-та.
660014, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31